IA MPSVR SR
EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

Prínos blockchainu / krypto-technológií pre podnikateľský a verejný sektor

REPUBLIKOVÁ ÚNIA
RÚZ
ZAMESTNÁVATEĽOV

NÁRODNÝ PROJEKT

Podpora kvality sociálneho dialógu

Typ projektu: Neinvestičný

Termín realizácie projektu: 08/2019 – 12/2019

ITMS projektu: 312031V749

Autorský kolektív

Autorské dielo bolo vypracované v rámci hlavnej aktivity „Posilnenie odborných a analytických kapacít sociálnych partnerov, budovanie infraštruktúry a komunikačnej platformy sociálneho dialógu a rozvoja sociálneho partnerstva na národnej a medzinárodnej úrovni“ v rámci podaktivity 1.1 Posilnenie kapacít sociálnych partnerov prostredníctvom analytickej činnosti Národného projektu Podpora kvality sociálneho dialógu expertným tímom sociálneho partnera Republiková únia zamestnávateľov. Vyjadruje názory a postoje sociálneho partnera na predmetnú tému. Autorské dielo nevyjadruje názory ani postoje prijímateľa projektu a bolo schválené Riadiacim výborom Národného projektu Podpora kvality sociálneho dialógu.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

OBSAH

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ZOZNAM TABULIEK

ZOZNAM ILUSTRÁCIÍ

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ZOZNAM SKRATIEK A ZNAČIEK

CPU – centrálna počítačová jednotka (z angl. Central Processor Unit)

DLT – technológia distribuovanej databázy (z angl. Distributed Ledger Technology)

DPoS – delegovaný dôkaz o podiele na sieti (z angl. Delegated Proof-of-Stake)

EÚ – Európska únia

GPU – grafická karta (z angl. Graphics Processing Unit)

ICO – prvotná emisia mincí (z angl. Initial Coin Offering)

INATBA – International Association for Trusted Blockchain Applications

IoT – Internet of Things

IPO – prvotná ponuka akcií

ISP – poskytovateľ Internetových služieb (z angl. Internet Service Provider)

MAST – Abstraktný syntaxový strom (z angl. Merkelized Abstract Syntax Tree)

NFT – forma unikátnych kryptografických tokenov (z angl. Non-Fungible Tokens)

PoC – prototyp testujúci koncept (z angl. Proof of Concept)

PoI – dôkaz o dôležitosti (z angl. Proof-of-Importance)

P2P – Peer-to-Peer sieť

PoS – dôkaz o podiele na sieti (z angl. Proof-of-Stake)

PoW – dôkaz o vykonanej práci (z angl. Proof-of-Work)

STO – ponuka tokenov reprezentujúcich cenné papiere (z angl. Security Token Offering)

UTXO – transakčný výstup (z angl. Unspent Transaction Output)

ZKP – dôkazy s nulovou znalosťou (z angl. Zero-Knowedlge Proof)

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ÚVOD

História krypto-technológií siaha až do obdobia antického Grécka kedy sa objavili prvé šifry využívané na ochranu komunikácie pred neželanými tretími stranami. Keďže sa táto praktika stala neoddeliteľnou súčasťou nielen súkromnej, ale aj obchodnej či vojenskej komunikácie, stala sa z nej samostatná veda – kryptológia. Kryptológia je veda o utajení obsahu správ a v súčasnosti sa považuje za pridruženú časť matematiky a informatiky. Kryptológia sa taktiež ďalej delí na pridružené oblasti ako kryptografia či steganografia. Pre účel tejto štúdie je najrelevantnejšou oblasťou kryptografia, ktorá sa zaoberá skúmaním a navrhovaním šifrovacích systémov. Tieto systémy typicky musia spĺňať určité atribúty ako autenticita, dôvernosť, dostupnosť či integrita dát.

Pojem krypto-systémy môže teda zahŕňať akékoľvek systémy a aplikácie, ktoré nejakým spôsobom využívajú šifrovanie alebo niektoré z kryptografických techník.

Typickým príkladom snáď najrozšírenejších aplikácií tohto druhu sú chatovacie aplikácie slúžiace na komunikáciu. V dnešnej dobe už všetky aplikácie tohto druhu ako Facebook Messenger, Threema, Signal alebo WhatsApp využívajú nejakú mieru šifrovania, aby bola komunikácia prístupná len dvom komunikujúcim stranám. Ďalším, pre túto štúdiu relevantnejším príkladom, sú anonymizačné siete ako Tor[1], I2P[2] alebo Freenet[3], ktoré poskytujú oveľa vyššiu mieru anonymity pre ich užívateľov hlavne tým, že maskujú IP adresu zariadení, a teda výrazne zvyšujú náročnosť lokalizovania pripojených zariadení. Tieto siete svojim spôsobom vytvárajú paralelný ekosystém stránok, služieb a užívateľov, ktorý býva často nazývaný „Darknet“ alebo „Deep Web“. Naopak, bežný internet, v ktorom interaguje väčšina

---

[1] Viac informácií na: https://www.torproject.org/

[2] Viac informácií na: https://geti2p.net/en/

[3] Viac informácií na: https://freenetproject.org/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

užívateľov, sa často označuje ako „Clearnet“. Najrozšírenejším nástrojom na prístup k Darknetu je webový prehliadač Tor.

Tor browser maskuje IP adresu užívateľa tým, že prenáša spojenie vez viacero uzlov v sieti prostredníctvom tzv. Onion routingu, čím vytvára niekoľko vrstiev ochrany. Uzle v sieti vedia len to odkiaľ spojenie prišlo a kam ho majú ďalej poslať, bez toho aby mali vedomosť o obsahu dát, ktoré prenášajú. Sieť Toru sa skladá z niekoľko tisícov takýchto uzlov po celom svete. Tor navyše aj blokuje všetky sledovacie nástroje (z angl. trackers), ktoré využívajú webové stránky na sledovanie a identifikáciu užívateľov. Cieľom Toru je aby všetci užívatelia vyzerali rovnako a aby sa nedala rozpoznať ich identita.

Väčšina týchto technológií využíva tzv. asymetrické šifrovanie, ktorého objavenie koncom sedemdesiatych rokov znamenalo revolúciu v kryptografii. Bolo to hlavne preto, že dovtedy si komunikujúce strany museli medzi sebou zdieľať kľúč, ktorým šifrovali svoju komunikáciu. Tento fakt sám osebe reprezentoval potenciálny vektor útoku, kedy hrozilo, že sa kľúč dostane do rúk neželanej tretej strany, ktorá tým pádom mohla efektívne odpočúvať prebiehajúcu komunikáciu. Objavenie asymetrického šifrovania znamenalo prelom práve z toho dôvodu, že eliminovalo nevyhnutnosť existencie šifrovacieho kľúča, ktorý si komunikujúce strany museli vymeniť. Asymetrická kryptografia, alebo aj kryptografia s verejným kľúčom, je postavená na tzv. Public Key Infrastructure (PKI). PKI zabezpečuje šifrovanie komunikácie vďaka existencii kľúčových párov. Každá komunikujúca strana má verejný a privátny kľúč. Verejný kľúč je voľne šíriteľný a analogicky by sa dal prirovnať k emailovej adrese, na ktorú je možno prijímať šifrované správy. Tieto správy sa však dajú odšifrovať len využitím korešpondujúceho privátneho kľúča. Celá mechanika takýchto šifier je postavená na náročnosti faktorizácie prvočísiel. Prvú takúto schému popísali koncom sedemdesiatych rokov výskumníci počítačových vied Whitfield Diffie, Martin Hellman a Ralph Merkle. Krátko nato bol ich koncept daný do praxe prostredníctvom RSA algoritmu, za ktorým stála ďalšia trojica legendárnych výskumníkov z MIT – Ronald Rivest, Adi Shamir a Leonard Adleman.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Práve kryptografia verejných kľúčov bola esenciálnym prvkom pri zrode súčasných krypto-systémov vrátane kryptomien ako Bitcoin. Bitcoin ako aj ďalšie kryptomeny však zďaleka neboli prvými pokusmi o digitálne meny. História digitálnych mien sa začala písať začiatkom deväťdesiatych rokov, kedy vznikol Digicash[4]. Digicash bola súkromná spoločnosť, ktorá bola založená svetoznámym vedcom a kryptografom Davidom Chaumom v roku 1990 v Holandsku. Digicash bola prvá digitálna mena, ktorá umožnila anonymné platby jej užívateľom. Hlavný produkt firmy sa volal „e-cash". E-cash umožňoval anonymné platby napriek tomu, že využíval vtedajšiu bankovú infraštruktúru. Anonymita bola dosiahnutá využitím kryptografickej metódy tzv. „blind signatures". Firma ako aj produkt boli populárne v polovici deväťdesiatych rokov, keď nadviazali spoluprácu s viacerými bankami v USA a aj v Európe. Produkt bol taktiež predmetom diskusie o akvizícii firmou Microsoft. V roku 1998 však firma skrachovala. Nasledujúce roky priniesli niekoľko viac či menej decentralizovaných konceptov a produktov, ktoré sa snažili oživiť myšlienku digitálnych mien. Koncom deväťdesiatych rokov vzniklo niekoľko digitálnych mien krytých zlatom. Najznámejšou takou firmou bola E-gold[5], ktorá vznikla v roku 1998 a v priebehu pár rokov získala viac než milión zákazníkov. E-gold sa stal obľúbeným nástrojom kriminálnikov, bol často využívaný v rôznych podvodných kartových schémach a pri praní špinavých peňazí. Z toho dôvodu sa firma stala predmetom vyšetrovania policajných orgánov v USA a jej zakladateľ bol nakoniec odsúdený. V rovnakom období sa objavilo aj niekoľko ďalších technologicky inovatívnych pokusov o krypto-systémy snažiace sa o dizajn nezávislej digitálnej meny.

Projekt nazvaný Hashcash[6] bol prvým z pokusov o vytvorenie digitálneho tokenu, ktorý by reprezentoval kryptografický dôkaz o vykonaní náročných matematických výpočtov. Tento

---

[4] Viac informácií na: https://en.wikipedia.org/wiki/DigiCash

[5] Viac informácií na: https://en.wikipedia.org/wiki/E-gold

[6] Viac informácií na: https://nakamotoinstitute.org/static/docs/hashcash.pdf

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

koncept bol pôvodne navrhnutý ako nástroj na ochranu proti spamu v emailovej komunikácii, kedy emailový klient odosielateľa správy musel pred odoslaním správy vypočítať hash určitej obtiažnosti, ktorý bol zahrnutý do hlavičky emailu a tak signalizoval prijímaciemu serveru dôveryhodnosť. Logika za týmto systémom spočívala v náročnosti výpočtu hašu. Zatiaľ čo pre bežného užívateľa by takáto „práca“ nepredstavovala žiadnu prekážku, pre niekoho, kto posiela tisícky spam emailov to už môže znamenať nárast nákladov na elektrinu kvôli náročnosti a množstvu výpočtov. Hashcash bol kľúčový koncept, ktorý bol následne rozpracovaný v rámci viacerých projektov. Jedným z jeho slabín však bola neprenositeľnosť, to znamená, že vytvorený token nemohol byť používaný ako digitálna hotovosť a cirkulovať v obehu a meniť vlastníkov. Projekty ako Bitgold[7] a B-money[8] ďalej rozpracovali tento koncept a vylepšili ho o niekoľko technologických detailov. Oba taktiež skombinovali Hashcash s myšlienkou distribuovanej databázy, resp. účtovnej knihy, do ktorej by sa zapisovali transakcie prebiehajúce v sieti. Oba projekty ostali len v teoretickej rovine a neboli rozvinuté ďalej do funkčného prototypu. Jeden z dôvodov bol aj ten, že samotní autori si boli vedomí slabín týchto systémov, ktoré spočívali v koordinácii veľkého množstva počítačov, ktoré sa navzájom nepoznajú. Toto malo za následok, že oba systémy boli náchylné na tzv. problém dvojitej útraty (z angl. double-spending), kedy by účastník siete teoreticky mohol zaplatiť tou istou peňažnou jednotkou dvakrát (a viac). Takzvané konsenzuálne algoritmy, ktoré tento problém riešili v korporátnom prostredí a ktoré boli predmetom výskumu od začiatku osemdesiatych rokov, boli navrhnuté tak, aby fungovali v prostredí v ktorom sa servery v distribuovanej sieti navzájom vedeli identifikovať. Skoordinovať stovky či potenciálne tisícky anonymných serverov, tak aby každý z nich súhlasil so stavom siete ako aj stavom jednotlivých účtov, bola veľká výzva.

[7] Viac informácií na: https://nakamotoinstitute.org/bit-gold/

[8] Viac informácií na: https://nakamotoinstitute.org/static/docs/hashcash.pdf

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Snáď posledný z najvýznamnejších predchodcov Bitcoinu bol projekt označený ako „RPOW“[9] (Reusable Proof-of-Work). RPOW bol zverejnený v roku 2004 a vyriešil problém koordinácie počítačov v rámci siete centralizovaným riešením. Centrálny server využíval špeciálny druh procesorov od IBM, ktorý umožňoval užívateľom siete overiť, že vlastník servera nemanipuloval so softvérom, resp. jeho zdrojovým kódom, ktorý na serveri beží a teda celý koncept nevyžadoval dôveru vo vlastníka alebo administrátora systému. Slabinou systému bolo však, že ho vlastník mohol skrátka vypnúť a takáto vlastnosť by bola ťažko akceptovateľná pre akýkoľvek systém finančnej povahy.

Hoci RPOW systém fungoval určitú dobu v testovacej fáze, nakoniec sa neuchytil a nebol ďalej rozvíjaný.

V nasledujúcom období sa stali populárnymi aj nové platobné systémy ako Paypal či Liberty Reserve. Žiadne z nich, kvôli reguláciám finančného sektoru, však neumožňovali anonymitu pri finančných transakciách, aj keď Liberty Reserve sa to určitú dobu darilo, no neskôr bola firma kvôli tomu zavretá a jej majitelia vyšetrovaní.

Bitcoin[10] ako aj ďalšie decentralizované kryptomeny vznikli ako evolučný krok a zároveň aj odpoveď na neúspešné pokusy o dosiahnutie finančnej slobody a anonymity prostredníctvom klasickej paradigmy centralizovaných finančných inštitúcií, ktoré musia plniť striktné regulácie súvisiace so zisťovaním identity klientov a praním špinavých peňazí.

Kryptomeny však tieto regulácie typicky nedodržiavajú nakoľko fungujú len ako „open-source“ protokoly (s verejne dostupným zdrojovým kódom) bežiace na kompletne decentralizovanej infraštruktúre skladajúcej sa z tisícok serverov. Táto infraštruktúra je navyše otvorená

[9] Viac informácií na: https://nakamotoinstitute.org/literature/rpow/

[10] Viac informácií na: https://nakamotoinstitute.org/bitcoin/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

komukoľvek, kto má záujem participovať na sieti. Vďaka tomu je pre vlády veľmi náročné, takmer až nemožné, vynútiť dodržiavanie takýchto regulácií, pretože neexistuje jedna konkrétna zodpovedná entita či inštitúcia.

Práve technológia blockchain bola kľúčovým aspektom, ktorý umožnil vznik decentralizovaných kryptomien. Blockchain sa dá najjednoduchšie opísať ako distribuovaná databáza či účtovná kniha, ktorej aktuálna kópia je replikovaná na tisícky počítačov, nazývaných aj uzle (z angl. nodes), po celom svete. Synchronizácia tejto účtovnej knihy prebieha v aktuálnom čase naprieč všetkými uzlami v sieti. V sieti neexistuje žiadna centrálna alebo nadriadená autorita, ktorá by mala nadriadené práva a všetci účastníci siete, ktorí majú softvér na svojom počítači sú si rovní a každý z uzlov v sieti nezávisle verifikuje transakcie podľa pred-definovaných kritérií daného protokolu. O tom, či sa daná transakcia resp. blok v ktorom sa nachádza, dostane do blockchainu, rozhodne väčšina v sieti. Táto väčšina môže byť meraná rôznymi spôsobmi. Bitcoin využíva tzv. Proof-of-Work (PoW) konsenzuálny algoritmus, ktorý sa používa taktiež v mnohých iných kryptomenách, a v ktorom sa relatívny vplyv v sieti meria prostredníctvom množstva výpočtového výkonu tzv. hashrate-u, t. j. množstvo vypočítaných hašov za sekundu. Práve využitie tohto druhu algoritmu ako nástroja na dosiahnutie konsenzu v prostredí peer-to-peer (P2P) sieti bolo kľúčovou inováciou Bitcoinu.

Proof-of-Work však zďaleka nie je jediný konsenzuálny mechanizmus. Spustenie Bitcoinu naštartovalo obrovský záujem vo vedeckej komunite o výskum v tejto oblasti. Snáď najpopulárnejšou alternatívou ku PoW je Proof-of-Stake (PoS), ktorý je implementovaný v mnohých kryptomenových sieťach a stal sa populárnou voľbou hlavne pre omnoho menšie energetické nároky na počítače participujúce v sieti. Pri PoS systéme sa meria vplyv v sieti cez mieru podielu (z angl. slova stake) v danej sieti, t. j. množstva vlastnených mincí. Takže, ak má entita napr. 10 miliónov mincí zo 100 miliónov mincí, ktoré sú v obehu, štatisticky vyťaží v priemere každý 10. blok v sieti. V poslednej dobe sa na tento systém snaží prejsť viacero kryptomenových sietí, ktoré využívali doposiaľ PoW. Medzi takéto projekty patrí aj

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Ethereum[11], druhá najväčšia kryptomenová platforma po Bitcoine, na základe trhovej kapitalizácie.

Výber konsenzuálneho algoritmu má však často implikácie na vlastnosti danej siete. Kým siete využívajúce PoW sú pomalšie a spotrebúvajú obrovské množstvo energie na ich ťažbu, čo je často predmetom kritiky rôznych environmentálnych skupín, faktom je, že poskytujú aj omnoho vyššiu mieru bezpečia, súvisiacu s nemeniteľnosťou transakcií. Pri diskusii o blockchaine a jeho využití sa často abstrahuje od predpokladov, na ktorých účastníci diskusie stavajú, čo veľakrát spôsobuje nedorozumenia a mylné očakávania od tejto technológie. Preto aj v tejto štúdii ak vravíme o blockchaine, pokiaľ nie je definované inak, máme na mysli blockchainovú sieť podobnú Bitcoinu a založenú na PoW systéme.

Pod pojmom kryptosystémy sa preto môže skrývať obrovské množstvo technológií a aplikácií. V rámci tejto štúdie sa budeme zameriavať hlavne na tie, ktoré súvisia s kryptomenami a technológiou blockchain. Samotný pojem kryptomeny sa dá považovať za zavádzajúci, keďže implikuje využitie týchto technológií hlavne v monetárnej oblasti. No faktom je, že väčšina technológií, ktoré spadajú pod pojem kryptomeny, nemá za cieľ byť platidlom v klasickom zmysle slova. Zatiaľ čo Bitcoin vznikol a aj je využívaný často ako platidlo či alternatíva k národným menám, má okrem toho aj iné využitia. Bitcoin sa sám o sebe dá považovať za globálnu databázu, ktorá je otvorená komukoľvek. Ktokoľvek môže vlastniť a stiahnuť si celú kópiu tejto databázy, a ktokoľvek môže zároveň do nej aj zapisovať údaje, resp. transakcie. Tieto údaje nemusia nevyhnutne súvisieť s transakciami a transferom Bitcoinov. Skladba Bitcoinových transakcií umožňuje zápis akýchkoľvek údajov, aj keď v obmedzenej dátovej veľkosti. Zatiaľ čo Bitcoin a jeho skriptovací jazyk majú pomerne obmedzenú funkcionalitu,

[11] Viac informácií na: https://ethereum.org/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

existuje mnoho kryptomien, ktoré sú tzv. Turing-complete a teda umožňujú bežať akýkoľvek softvér či program za predpokladu dostatku výpočtovej sily.

Snáď najznámejšou takou kryptomenou je Ethereum. Ethereum ako projekt bol od začiatku zamýšľaný ako svetový počítač, na ktorom by bežali decentralizované aplikácie, a nie ako platobný systém na platenie v obchodoch za služby či tovar. Ethereum má natívnu platobnú jednotku – ether, ktorá sa využíva v rámci systému na platbu za výpočtový výkon. Ethereum sa ako sieť dá teda využiť v princípe na čokoľvek, keďže umožňuje tzv. smart kontrakty. Zároveň je nutné dodať, že blockchainy ako také nie sú vhodné na ukladanie veľkého množstva dát a preto sa často kombinujú pre tento účel s ďalšími technológiami ako IPFS[12], ktoré slúži ako decentralizované cloudové úložisko, do ktorého sa ukladajú dáta, a do blockchainu Etherea sa ukladá len záznam o uložení dát ako aj ich lokácia. Ethereum sa pre svoju funkcionalitu stalo populárnou platformou pre decentralizované aplikácie. Rad z nich, ako napríklad aj významná odnož týchto aplikácií často označovaná ako „DeFi“ (z angl. Decentralised Finance), bude taktiež predmetom tejto analýzy.

Rovnako budú predmetom tejto analýzy aj nefinančné využitia blockchainu ako technológie. Zároveň je dôležité podotknúť, že samotný termín „blockchain“ je diskutabilný a nemá jasne definovaný obsah. Blockchain sa často prekladá ako distribuovaná účtovná kniha, ktorá má formu určitej dátovej štruktúry, ktorá sa podobá na reťaz matematicky prepojených blokov. Avšak, existujú podobné systémy, ktoré implementujú inú dátovú štruktúru, populárny je napr. DAG (Directed Acyclic Graph), a nie sú považované technicky za blockchain, hoci disponujú veľmi podobnými a často aj lepšími vlastnosťami. Najznámejšími kryptomenovými platformami, ktoré spadajú do tejto kategórie, sú napr. Maidsafe[13] či IOTA[14]. Ďalšou takou

[12] Viac informácií na: https://ipfs.io/

[13] Viac informácií na: https://maidsafe.net/

[14] Viac informácií na: https://www.iota.org/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

platformou, ktorá sa často označuje za blockchain, aj keď technologicky implementuje rozdielnu dátovú štruktúru, je napr. platforma Corda[15], ktorá sa často využíva v korporátnom prostredí. Práve pre tieto technické detaily sa často používa pojem DLT (Distributed Ledger Technology) namiesto blockchainu, pretože zahŕňa v sebe viacero podobných technológií.

Analýza sa skladá z desiatich kapitol a začína úvodom a manažérskym zhrnutím. Tretia kapitola sa venuje základným princípom, na ktorých kryptomeny a ďalšie kryptotechnológie fungujú a štvrtá kapitola analyzuje technologickú a filozofickú zmenu paradigmy, ktorú prinášajú. Piata a šiesta kapitola sa venuje potenciálnemu využitiu kryptosystémov, partikulárne kryptomenám a technológii blockchain v súkromnom a verejnom sektore. Siedma kapitola sa zaoberá presahom kryptotechnológií do šedej ekonomiky, analyzuje možnosti budúceho vývoja. Ôsma kapitola sumarizuje projekty využívajúce kryptotechnológie ktoré už existujú alebo sú v štádiu plánovania. Analýza končí zhrnutím a Bibliografiou.

[15] Viac informácií na: https://www.r3.com/platform/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

1. MANAŽÉRSKE ZHRNUTIE

Kryptosystémy, či už kryptomeny alebo Blockchain technológie, predstavujú spolu s ďalšími nastupujúcimi exponenciálnymi technológiami obrovské výzvy nielen pri implementácii v jednotlivých odvetviach v rámci verejného či privátneho sektora, ale aj pre spoločnosť ako takú. Cieľom tejto analýzy je popísať kľúčové princípy krypto-technológií, súčasný stav odvetvia, ako aj pokúsiť sa predpovedať potenciálny ďalší vývoj a dopad týchto technológií na ekonomicke procesy v rámci verejného a privátneho sektora ako aj šedej ekonomiky. Témy analyzované v tejto štúdii sú usporiadané v nasledujúcej štruktúre:

- V kapitole 3 je hlavný dôraz kladený na vysvetlenie základných technologických konceptov a prvkov aplikovaných pri krypto-technológiách, ktoré sú nevyhnutné pre správne pochopenie fungovania týchto sytémov, ako napríklad asymetrická kryptografia, hašová funkcia, časové pečiatky a podobne. Ďalej nasleduje analýza a popis fungovania Bitcoinu z hľadiska samotného protokolu, ako aj druhej najväčšej blockchainovej siete Ethereum. Vysvetlený je hlavný prínos blockchainu ako technológie, transparentnosť a nemeniteľnosť dát, ako aj rozdiely medzi privátnými a verejnými blockchainami. V závere analyzujeme alternatívne dátové štruktúry či konsenzuálne mechanizmy implementované v blockchainoch, ako aj súčasný stav vývoja nových technologických vrstiev na Bitcoine a Ethereu.

- Kapitola 4 sa venuje zmene paradigmy súvisiacej s príchodom krypto-technológií, kryptomien a blockchainu, z technologického ako aj filozofického pohľadu. Táto kapitola analyzuje historické korene týchto technológií ako aj filozofické podhubie, v rámci ktorých sa vyvíjali. V tejto kapitole sa zaoberáme vznikom a implementáciou asymetrickej kryptografie naprieč širokou verejnosťou, prvými digitálnymi menami a prechodcami súčasných kryptomien, ako aj aktivistickými hnutiami, ktoré boli

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

propagátormi týchto technológií od ich samotného vzniku. Dôraz je tiež kladený na paradigmatické zmeny spôsobené tokenizáciou aktív.

- V kapitole 5 analyzujeme potenciálne využitie týchto technológií v súkromnom sektore. Začiatok kapitoly sa sústreďuje na využitie kryptomien ako platobného nástroja a výhody s tým spojené. V kapitole ďalej predstavujeme aplikácie z novovznikajúceho odvetvia v rámci blockchainu – decentralizovaného finančného systému či množiny protokolov, ktoré budú tvoriť novú podobu decentralizovaného webu. Kapitola ďalej analyzuje využitie blockchainu na tokenizáciu aktív ako aj na sledovanie životného cyklu produktov v logistike a dodávateľských reťazcoch.

- Kapitola 6 analyzuje využitie blockchainu a krypto-technológií v rámci verejného sektora. Dôraz sa kladie na využitie transparentnosti blockchainu, zvýšenie efektivity procesov pri verejnom obstarávaní, platbách, verejných registroch, zdravotných záznamoch a podobne. Kapitola taktiež predstavuje nástroje a aplikácie, pomocou ktorých sa dá využiť blockchain na časové pečiatky. V tejto kapitole ďalej analyzujeme postoj kľúčových inštitúcií, ako vlády či centrálnej banky ku kryptomenám a blockchainu v rámci EÚ či OECD.

- Vplyvom týchto technológií na šedú ekonomiku sa venujeme v kapitole 7, v ktorej popisujeme vznik a históriu tzv. Darknetu ako aj nástrojov, ktoré jeho fungovanie umožňujú. Dôraz je kladený na analýzu jednotlivých protokolov anonymných kryptomien a trhovísk. Kapitola ďalej pojednáva o regulačnom prostredí vo vybraných krajinách ako Čína, Singapur, Švajčiarsko či Malta a končí analýzou právneho prostredia súvisiaceho s krypto-technológiami na Slovensku.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- Kapitola 8 analyzuje vybrané projekty privátneho a verejného sektora, ktoré implementujú blockchain či krypto-technológie v rôznych odvetviach. V kapitole pojednávame o finančných aplikáciach blockchainu v rámci paralelného decentralizovaného finančného systému. Dôraz je kladený na hĺbkovú anlýzu vybraných projektov v hernom priemysle, logistike či voľbách.

- Záver obsahuje vyhodnotenie našej analýzy ako aj súhrn predikcií súvisiacich s využitím krypto-technologií v budúcnosti.

Oblasť krypto-technológií je veľmi široká a okrem kryptomien a blockchainu môže potenciálne súvisieť s ktoroukoľvek technológiou, nakoľko kryptografické protokoly tvoria základné stavebné kamene nielen webových či komunikačných technológií, ale v princípe akýchkoľvek digitálnych aplikácií a procesov. Jedná sa o veľmi komplexnú tému, ktorá zasahuje do množstva odvetví, od matematickej analýzy a kryptografie cez webovú infraštruktúru, softvérove inžinierstvo či financie až po právo, ekonómiu a filozofiu. Kryptosystémy majú dnes vplyv takmer na všetky oblasti našej spoločnosti a tento vplyv, ako aj ich prepojenie s ďalšími spoločenskými či technologickými aspektami, sa bude v budúcnosti len zvyšovať. Z toho dôvodu sa dá na viacero aspektov, ktoré sú predmetom tejto analýzy, nazerať z rôznych uhlov. Len na Bitcoin samotný sa dá nahliadať napríklad ako na platobný systém, alternatívne peniaze, digitálnu komoditu, globálnu decentralizovanú databázu či podkladový komunikačný protokol pre internetovú infraštruktúru budúcnosti. Napriek tomu, že je náročné obsiahnuť komplexitu týchto technológií a predikovať všetky ich potenciálne dopady, dá sa pomerne s veľkou istotou predpokladať, že zasiahnu náš ekonomický a spoločenský systém výrazne vo viacerých smeroch.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2. POPIS A PRINCÍPY FUNGOVANIA KRYPTOTECHNOLÓGIÍ

V rámci tejto kapitoly popíšeme fundamentálne vlastnosti kryptomien, blockchainu ako aj kľúčových kryptografických prvkov, ktoré sa v nich najčastejšie používajú.

2.1. Kryptografia s verejným kľúčom

Kryptografia s verejným kľúčom je založená na asymetrickom šifrovaní, a teda používa dva kľúče - privátny a verejný. Verejný kľúč slúži na šifrovanie, a ako vyplýva z názvu, môže byť zdieľaný verejne, zatiaľ čo privátny kľúč slúži na dešifrovanie a nemal by byť zdieľaný so žiadnou treťou stranou okrem prijímateľa správy. Tento technologický princíp sa dnes už bežne využíva v množstve informačných systémov vo verejnom či privátnom sektore. Na Slovensku napríklad aj pri systéme Elektronickej identifikačnej karty (eID). Zatiaľ čo vo väčšine informačných systémov sa tento kľúčový pár používa v kombinácii s rôznymi ďalšími informáciami o užívateľoch, v prostredí kryptomien však verejný kľúč reprezentuje častokrát jedinú informáciu o identite strán, ktoré vykonávajú transakciu. Pri Bitcoine a iných kryptomenách sa tento princíp však nevyužíva na šifrovanie, ale na generovanie digitálnych podpisov a na vytvorenie párového kľúča, prostredníctvom ktorého sa determinuje adresa prijímateľa transakcie. Ide o verejný kľúč, ktorý je derivovaný z privátneho kľúča. Verejný kľúč teda slúži na prijímanie transakcie, a privátny kľúč slúži na autorizovanie odchádzajúcich transakcií prostredníctvom digitálneho podpisu. Tento podpis je možné kryptograficky overiť všetkým účastníkom siete, bez toho aby bolo nutné zverejniť aj privátny kľúč odosielateľa (Antonopoulos, 2017:56).

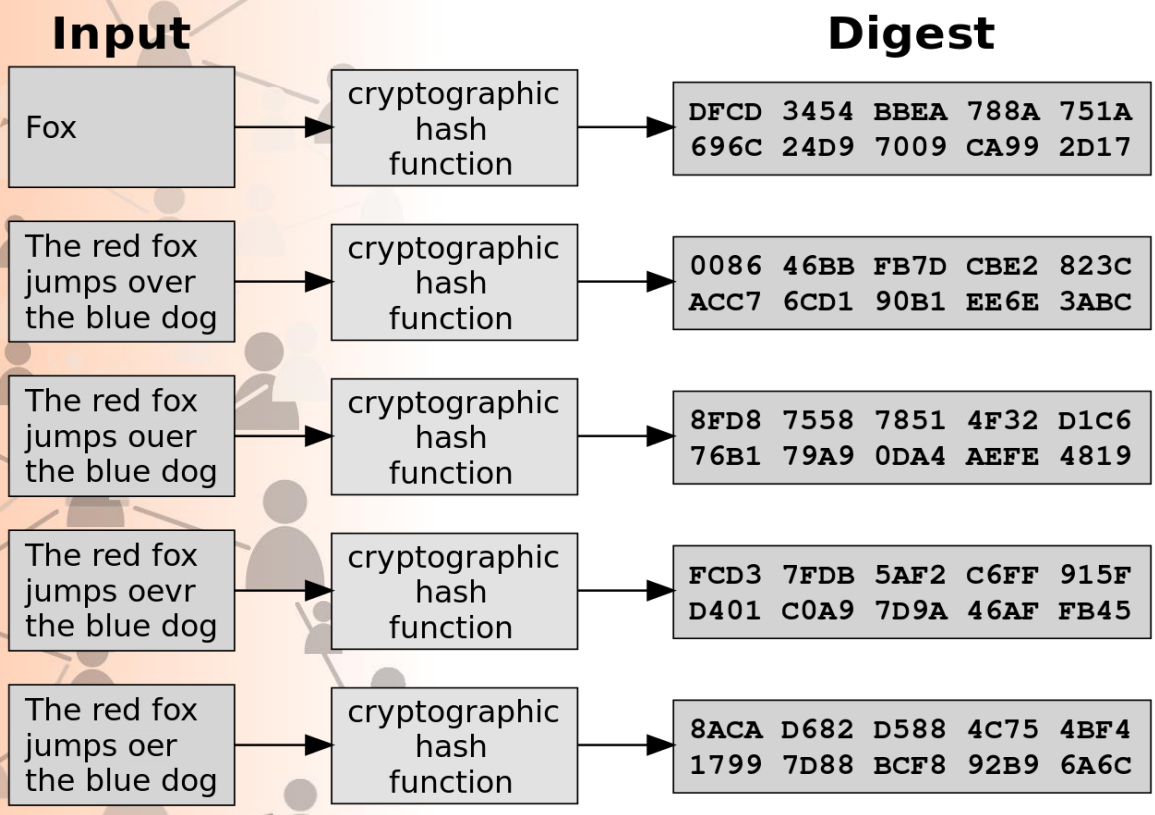
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2.1.1. Haš

Koncept hašovej funkcie je taktiež jedným zo základných technologických prvkov, ktoré sa využívajú nielen v kryptosystémoch, ale taktiež naprieč internetovou infraštruktúrou. Kľúčovou vlastnosťou hašových funkcií je, že mapujú vstupy arbitrárneho množstvo dát na výstupy s fixnou dĺžkou. Výstup takéhoto výpočtu je vždy unikátny. V teórii existuje šanca, že dva rôzne vstupy môžu vyprodukovať rovnaký výstup - hash, ale pravdepodobnosť takejto situácie je tak nízka, až je zanedbateľná. Hash sa dá teda svojou unikátnosťou analogicky prirovnať k digitálnemu odtlačku prstov dát. Ďalšou kľúčovou vlastnosťou hašových funkcií je, že sú tzv. jednosmernými funkciami, t. j. unikátny hash môže byť vygenerovaný z akýchkoľvek dát, zatiaľ čo vstupné dáta sa nedajú odvodiť od hašu.

Obrázok 1: Hašová funkcia



Zdroj: Wikipedia

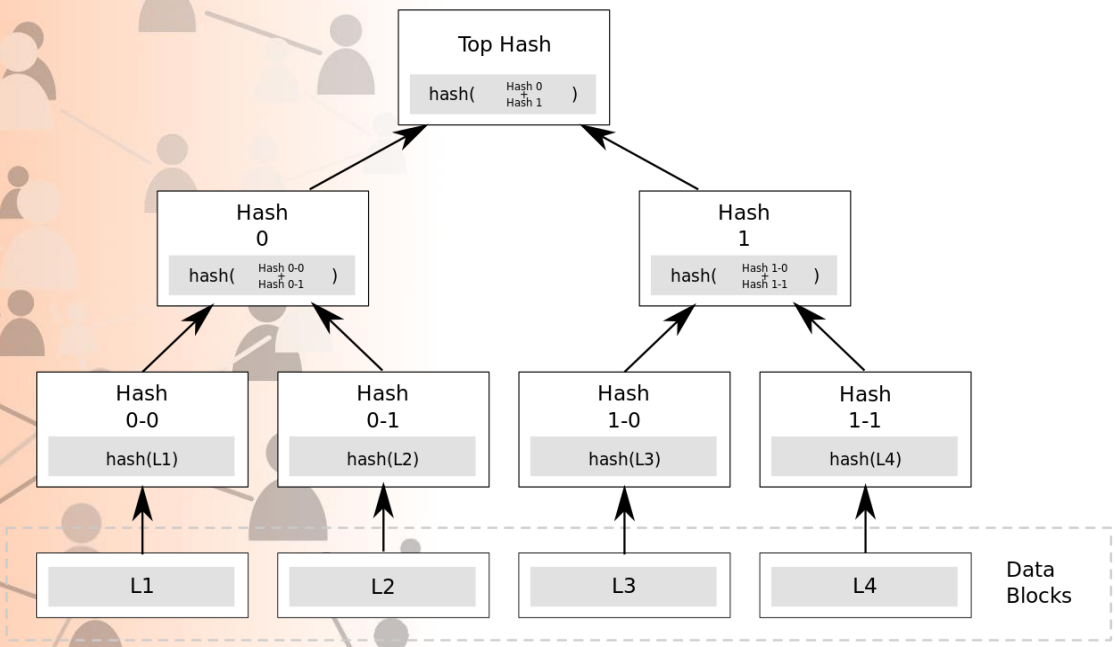
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2.1.2. Hašové stromy

Hašové stromy (z angl. Hash Trees alebo Merkle Trees) sú v kryptografii veľmi často používanou dátovou štruktúrou. Jedná sa o štruktúru pripomínajúcu svojou štruktúrou strom, ktorý má vo všetkých svojich "listoch" dáta a všetky jeho vrcholy obsahujú hodnotu odpovedajúcu výsledku kryptografickej hašovej funkcie. Na úplnom vrchole stromu je koreňový haš. Na rozdiel od podobných štruktúr, ako sú hašové reťazce alebo lineárne zoznamy hašov, hašový strom umožňuje efektívne a bezpečne overovať integritu veľkého množstva dát v logaritmickom čase vzhľadom na počet dátových uzlov. Okrem kryptomien ako Bitcoin a Ethereum sa využíva aj napríklad v populárnom verzovacom systéme Git či decentralizovanom dátovom úložisku IPFS.

Obrázok 2: Hašový strom



Zdroj: Wikipedia

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2.1.3. Timestamping (Časová pečiatka)

Časová pečiatka je taktiež technológia, ktorá sa bežne využíva v prostredí internetu na overenie časových údajov súvisiacich s vytvorením či modifikáciou digitálnych dokumentov. V rámci verejného sektora sa táto technológia používa napríklad v Obchodnom registri, na súdoch, či Ústrednom portáli verejnej správy. Typicky je časová pečiatka vyhotovená využitím dôveryhodného zdroja času sprostredkovaného dôveryhodnými autoritami a ich servermi časových pečiatok. Využitie technológie blockchainu umožňuje využívať časové pečiatky bez toho, aby bolo nevyhnutné dôverovať akejkoľvek centrálnej autorite. O tom, ako takýto proces funguje, píšeme neskôr v tejto kapitole.

2.1.4. Kryptografia na báze eliptických kriviek

Kryptografia na báze eliptických kriviek je typ asymetrickej kryptografie založenej na obtiažnej riešiteľnosti matematických problémov diskrétnych logaritmov. Eliptické krivky sa pri Bitcoine využívajú na generovanie verejných adries z privátneho kľúča. Tento proces je založený na tom, že pomocou eliptických kriviek je pomerne jednoduché násobiť čísla (vytvárať adresy), ale je extrémne náročné tieto čísla deliť a teda reverznúť tento proces. Bitcoin napríklad využíva Secp256k1[16], čo je konkrétny parameter eliptických kriviek implementovaných v kryptografickej schéme Bitcoinu, ktorý je definovaný aj v dokumente Standards for Efficient Cryptography (SEC)[17]. Tento konkrétny parameter nebol pred Bitcoinom takmer vôbec využívaný, ale v posledných rokoch sa stáva čím ďalej tým viac populárnejší vďaka niektorým jeho vlastnostiam, ktoré umožňujú pomerne efektívne výpočty.

[16] Viac informácií na: https://en.bitcoin.it/wiki/Secp256k1

[17] Viac informácií na: http://www.secg.org/sec2-v2.pdf

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2.1.5. Digitálne podpisy

Digitálne podpisy sa všeobecne využívajú na overenie integrity údajov. Zatiaľ čo sa často používa aj pojem "elektronický" podpis, tieto dva pojmy nie sú zameniteľné. Taktiež, definície týchto termínov sa líšia naprieč jurisdikciami. V prostredí štátnej správy či korporácií sa za elektronický podpis môže často považovať aj kliknutie na frázu "Súhlasím" v rôznych on-line procesoch. Pri krypto systémoch však digitálne podpisy striktne využívajú prvky kryptografických protokolov. Bitcoin napríklad využíva ECDSA (Elliptic Curve Cryptographic Digital Signature Algorithm), kryptografický algoritmus na vytváranie digitálnych podpisov, ktoré zaručujú, že Bitcoiny môžu byť utratené len právoplatným vlastníkom, ktorý disponuje korešpondujúcim privátnym kľúčom. Vo svojej podstate je v takomto prípade digitálny podpis len súbor dvoch čísel, ktoré slúžia ako matematický dôkaz toho, že sa uskutočnila podpisovacia operácia. Takýto podpis je vygenerovaný z hašu dokumentu, ktorý má byť podpísaný v kombinácii s privátnym kľúčom, ktorý ten dokument podpisuje. Následne matematické algoritmy dokážu pomocou verejného kľúča overiť, že podpis bol vygenerovaný takýmto spôsobom.

2.2. Fungovanie Bitcoinu

V tejto sekcii vysvetlíme základné princípy fungovania Bitcoinu a Etherea ako aj blockchainu ako technológie so zreteľom na jej rôzne implementácie. Pre účely tejto analýzy sa zameriame na tie procesy a aspekty Bitcoin blockchainu, ktoré sú relevantné aj pre iné aplikácie založené na blockchaine. Zameriame sa na vysvetlenie Bitcoinu, pretože je prvou kryptomenou a zároveň aj kryptomenou s najväčšou trhovou kapitalizáciou. Zároveň platí, že je to aj najrobustnejšia Peer-to-Peer (P2P) sieť na svete, fungujúca na blockchain technológii. Taktiež je to jediná aplikácia blockchainu, ktorá úspešne funguje už viac než desať rokov a dosiahla určitú úroveň maturity ako ekosystému, tak aj relevantnej dokumentácie. Pri väčšine

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

blockchainových sietí platí, že sú ešte v skorom štádiu a častokrát k nim neexistuje potrebné množstvo relevantnej dokumentácie, či ešte nefungujú v prevádzkovej fáze.

Bitcoin sa objavil ako koncept prvýkrát v roku 2008, keď ho človek alebo skupina ľudí pod pseudonymom Satoshi Nakamoto zverejnil v rámci kryptografického mailing zoznamu. Autor zverejnil tzv. White Paper, v ktorom opísal základné princípy fungovania Bitcoinu. Bitcoin ako koncept staval na jeho predchodcoch z deväťdesiatych rokov, ako napr. B-money, Hashcash, Bitgold či RPOW. Bitcoin bol prvá kryptomena, ktorej sa podarilo unikátnym spôsobom skombinovať niekoľko rokov staré koncepty a technológie ako Proof-of-Work či identitu založenú na kryptografii s verejným kľúčom. Bitcoin je teda prvá skutočne decentralizovaná Peer-to-Peer sieť s fungujúcou menou. Označenie P2P znamená, že všetky počítače či servery, ktoré participujú na sieti, sú si medzi sebou rovné, neexistuje tam žiadna hierarchia a ani servery s nadradenými právomocami, a teda absentuje tam akákoľvek centrálna autorita. Vďaka tomuto dizajnu sú P2P siete omnoho odolnejšie voči akýmkoľvek útokom zo strany kyber zločincov, hackerov, alebo štátov. V realite však existuje určitá hierarchia medzi jednotlivými uzlami v sieti, nakoľko typicky rozpoznávame tri základné kategórie Bitcoinových (softvérových) klientov - ťažiarov, plné uzly a „light“ klientov.

Ťažiari sú vitálnou súčasťou ekosystému keďže využívajú dedikovaný špeciálny hardvér, verifikujú transakcie a súperia medzi sebou o právo vytvárať nové Bitcoinové bloky. Typicky si taktiež uchovávajú celú kópiu blockchainu a teda celej transakčnej histórie. Sú to práve ťažiari, ktorí investujú značné množstvo prostriedkov do náročných matematických výpočtov a pália obrovské množstvo elektriny. Podľa Cambridge Bitcoin Electricity Consumption Index od University of Cambridge[18], Bitcoinová sieť v súčasnosti ročne spáli takmer 75 terawatt hodín.

[18] Viac informácií na: https://www.cbeci.org/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Okrem ťažiarov sa Bitcoinová sieť skladá aj z tzv. plných uzlov (z angl. full nodes). Tento typ klientov participuje na sieti tým, že overuje validitu transakcií a taktiež uchováva lokálne kópiu celého blockchainu, no nepodieľa sa na ťažbe Bitcoinov. Posledným a najrozšírenejším typom softvérových klientov, ktorý je v sieti prítomný, sú „light" klienti. Toto sú typicky mobilné peňaženky, ktoré nedržia lokálnu verziu blockchainu, neverifikujú transakcie, a ani sa nepodieľajú na ťažbe, len sa pripájajú k serverom, ktoré tieto činnosti vykonávajú. Historicky sa množstvo plných uzlov v Bitcoinovej sieti pohybuje na úrovni okolo 10 000 uzlov[19], aj keď aj toto číslo je diskutabilné, nakoľko je determinované metodológiou, ktorú daný zdroj používa. Väčšina zdrojov ráta len tie uzly v sieti, ktoré majú otvorené spojenia a ku ktorým sa dá pripojiť. Tento typ uzlov sa nazýva "počúvajúce" (z angl. listening nodes). Niektoré zdroje však uvádzajú, že Bitcoin má vo svojej sieti až 100 000 uzlov[20], ak berieme do úvahy aj tie, s ktorými sa nedá nadviazať spojenie, no participujú na sieti.

V rámci kryptografických techník je Bitcoin zložený hlavne z dvoch základných konceptov:

1. Kryptografická hashovacia funkcia, presnejšie SHA-256 a RIPEMD-160
2. Eliptické krivky (ECDSA - Elliptic Curve Digital Signature Algorithm) - presnejšie Secp256k1[21]

Sieť je v princípe založená na komunikácii skrz správy, ktoré obsahujú informácie spojené s transakciou. Presnejšie obsahujú napr. množstvo Bitcoinov, adresu prijímateľa, výšku poplatku, či dodatočné dáta. Identita prijímateľa a odosielateľa v rámci siete funguje

---

[19] Viac informácií na: https://coin.dance/nodes

[20] Viac informácií na: https://thenextweb.com/hardfork/2019/05/06/bitcoin-100000-nodes-vulnerable-cryptocurrency/

[21] Viac informácií na: https://en.bitcoin.it/wiki/Secp256k1

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

kompletne na báze páru verejného a súkromného kľúča a rovnako digitálneho podpisu. Súkromný kľúč, inak nazývaný aj privátny kľúč, je vytvorený pomocou náhodne vygenerovaného čísla. Toto číslo je typicky generované v rámci peňaženky užívateľa lokálne a takým spôsobom, aby prístup k tomu číslu nemala žiadna tretia strana, teda ani vývojári, či správca aplikačného softvéru, ktorý peňaženku generuje.

Privátny kľúč teda umožňuje prístup ku kryptomenám, ktoré sú v rámci blockchainu pripísané korešpondujúcemu verejnému kľúču. Používa sa na generovanie digitálneho podpisu, ktorý autorizuje transakciu. Verejný kľúč je následne generovaný z privátneho kľúča a má formu kombinácie alfanumerických znakov. Verejný kľúč funguje v princípe ako emailová adresa či číslo bankového účtu a môže byť zdieľaný s kýmkoľvek.

Princípy fungovania transakcií

Bitcoin je decentralizovaná otvorená P2P sieť, do ktorej sa môže zapojiť ktokoľvek. Používateľ sa môže pripojiť do siete nainštalovaním si peňaženky do počítača alebo mobilu. Pri softvérových peňaženkách pre počítače si môže užívateľ zvoliť možnosť stiahnuť si celú kópiu blockchainu lokálne, a teda mať okamžitý prístup k celej transakčnej histórii siete. Mobilné peňaženky takúto možnosť neponúkajú keďže veľkosť blockchainu (pri Bitcoine v súčasnosti cca. 280 GB) presahuje kapacitu väčšiny mobilných zariadení.

Spoločnou črtou takmer všetkých typov peňaženiek je, že pri prvom spustení vygenerujú užívateľovi kľúčové páry unikátneho privátneho kľúča a korešpondujúcich verejných kľúčov. Tento privátny kľúč je ľahko zálohovateľný ako tzv. seed vo forme niekoľkých (typicky 12 alebo 24) anglických slov. Z privátneho kľúča sa teda následne dá generovať deterministickým spôsobom neobmedzené množstvo verejných kľúčov. Verejný kľúč je kombinácia niekoľkých

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

alfanumerických znakov, pričom Bitcoin využíva kódovací systém Base58[22], aby boli vylúčené znaky, ktoré sa na seba môžu podobať, ako napr. I a l či 0 a O. Verejný kľúč sa generuje pomocou jednosmernej hashovacej funkcie zo súkromného kľúča. Dôležité je poznamenať, že z verejného kľúča sa spätne nedá dopočítať súkromný kľúč.

V jednoduchosti, bitcoinová transakcia komunikuje všetkým uzlom v sieti, že vlastník určitého množstva Bitcoinov presúva vlastníctvo týchto bitocinov na iného užívateľa resp. jeho verejnú adresu. Kľúčovým konceptom pri Bitcoinových transakciách je UTXO (Unspent Transaction Output). Ako názov napovedá, jedná sa o výstup transakcie, ktorý prijímateľ transakcie obdrží a je teda autorizovaný predchádzajúcim vlastníkom utratiť ho v budúcnosti. UTXO je kvantifikované hodnotou Bitcoinovej transakcie. Takýto transfer sa zapíše do blockchainu, jeho kópiu uschovávajú desiatky tisícok uzlov v sieti. Ak teda užívateľ „A“ pošle do siete transakciu, v ktorej chce poslať 3 Bitcoiny užívateľovi „B“, všetky uzly v sieti samostatne verifikujú takúto transakciu a overujú, či užívateľ „A“ v transakcii uviedol adresu, ktorá disponuje daným množstvom UTXO (t. j. Bitcoinov), v jednoduchosti, či užívateľ má na účte aspoň toľko peňazí, koľko sa snaží poslať. Uzle v sieti zároveň verifikujú digitálny podpis transakcie a teda, či adresa uvedená v transakcii skutočne patrí užívateľovi „A“.

V prípade, že používateľ odosiela Bitcoiny, tak transakcia prebieha niekoľkými krokmi:

- Odosielateľ vytvorí transakciu, obsahujúcu UTXO a adresu (haš verejného kľúča) prijímateľa.
- Na transakčné dáta aplikuje hašovaciu funkciu SHA256 a následne RIPEMD160, čoho výstupom je haš transakcia.
- Haš podpíše svojim súkromným kľúčom.

[22] Viac informácií na: https://en.bitcoin.it/wiki/Base58Check_encoding

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- Odošle podpísanú transakciu do siete.

Verifikáciu transakcie vykonáva každý uzol v sieti:

- Verifikuje podpis odosielateľa a použije jeho verejný kľúč na dešifrovanie, pričom mu ostane odtlačok.
- Zoberie dáta a použije rovnaký postup ako odosielateľ. To znamená, že použije hašovaciu funkciu SHA256, pričom mu vznikne odtlačok/podpis týchto dát.
- V poslednom kroku porovná ním hašované dáta a dáta, ktoré sú hašované a odoslané odosielateľom.
- V prípade, že sa tieto odtlačky zhodujú, znamená to, že nikto nezmenil pôvodné dáta (v ktorých sú zapísané základné údaje transakcie), a to čo tvrdí odosielateľ je pravda.

Synchronizácia siete prebieha nasledovne:

1. Každý uzol „počúva", posúva ďalej a ukladá si transakcie zo siete, z ktorých počíta haš.
2. Pri každom bloku sieť náhodne vyberie uzol, ktorý získa právo vyťažiť blok.
3. Uzol je vybraný na základe princípu PoW, t. j. dôkaze o práci. Ten uzol, ktorý ako prvý vypočíta haš s potrebnými parametrami, získava právo vyťažiť blok.
4. Ostatné uzly v sieti akceptujú blok, len ak spĺňa určité podmienky súvisiace s validitou transakcií a podpismi.
5. Akceptáciu bloku vyjadria zahrnutím jeho hašu do vstupných dát, z ktorých počítajú ďalší haš.

Synchronizácia siete pomocou Proof-of-Work

Jeden z hlavných technologických prínosov Bitcoinu spočíva v spôsobe koordinácie uzlov v decentralizovanej P2P sieti. Problémom decentralizovaných systémov je, že na to, aby boli funkčné, je potrebné dosiahnuť stav, kedy sú schopné prenášať informácie aj v situácii kedy

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

časť siete je pod útokom resp. nie je funkčná. Tento problém pri decentralizovaných sieťach existuje už desaťročia a hovorí sa mu aj problém Byzantských generálov. Prvýkrát bol popísaný v roku 1982 Marshallom Peasom, Robertom Shostakom a Leslie Lamportom[23]. Problém sa zjednodušene ilustruje na armáde, ktorá sa snaží dobyť mesto. Mesto je obkľúčené niekoľkými divíziami, pričom každá z nich má svojho veliteľa. Velitelia komunikujú spolu prostredníctvom poslov, ktorí im odovzdávajú správy, kedy sa začne spoločný útok na mesto. Na úspešné dobytie mesta je potrebné, aby sa všetci generáli skoordinovali a zaútočili v rovnaký čas. Ak sa tak nestane, ich útok zlyhá a budú porazení. Zlyhanie koordinácie divízií v takomto prípade môže byť spôsobené zlyhaním (alebo klamaním) jedného či viacerých poslov, alebo jedného či viacerých generálov.

Preto generáli musia mať nejaký spôsob, vďaka ktorému dosiahnu konsenzus o čase útoku, a ktorý zaručí, že:

1. Lojálni generáli, ktorí budú dôverovať algoritmu, sa zhodnú na určitom pláne, pričom nebudú brať ohľad na zradcov.
2. Malé množstvo zradcov nemôže spôsobiť to, že lojálni generáli budú súhlasiť s ich plánom.

Tento problém vyriešili práve prostredníctvom aplikácie Proof-of-Work algoritmu ako nástroja na dosiahnutie konsenzu v distribuovanej sieti. Akákoľvek transakcia v Bitcoin sieti je potvrdzovaná všetkými tzv. uzlami (z angl. nodes) v sieti paralelne. Tieto uzle si navzájom šíria medzi sebou informácie o každej transakcii. Zároveň si každý (plný) uzol uschováva lokálne celú transakčnú históriu. Počet aj poradie transakcií, o ktorých jednotlivé uzly vedia, sa však môže líšiť. Práve na synchronizáciu všetkých uzlov v sieti, a teda nadobudnutie

[23] Viac informácií na: https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

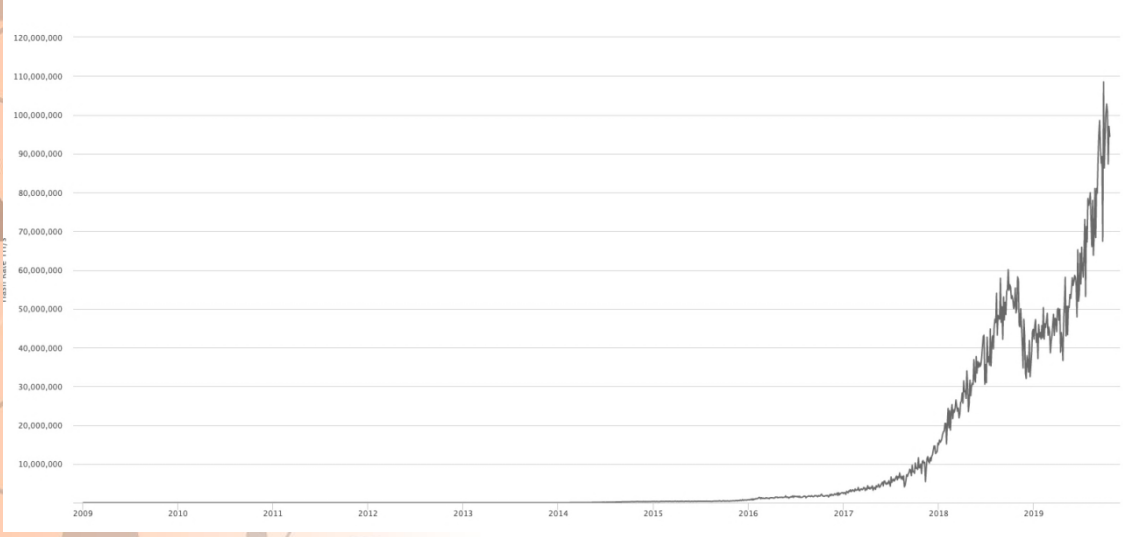
distribuovaného konsenzu, sa v Bitcoine využíva PoW, pretože na základe tohto princípu sieť vždy vyberie jeden uzol, ktorého blok s transakciami preberú všetky ďalšie uzly v sieti. Tento uzol teda získa právo určiť, ktoré transakcie sa uložia do daného bloku. Pri každom bloku sieť vyberie ten uzol, ktorý ako prvý vypočíta haš s predefinovanými parametrami, a teda poskytne sieti dôkaz o práci. Tento proces sa volá ťažba (z angl. mining). Je dôležité dodať, že vzhľadom na otvorenosť Bitcoin siete je možné, aby si ktokoľvek stiahol Bitcoin Core klienta a participoval týmto spôsobom na sieti. Ťažiari týmto spôsobom verifikujú transakcie, ťažia nové Bitcoiny, a generujú nové bloky. Ťažba blokov je teda len iný názov pre počítanie matematických operácií, ktoré sú náročné na spotrebu elektrickej energie. Vykonávaním týchto operácií ťažiari zároveň zabezpečujú sieť voči útokom.

V období spustenia Bitcoinovej siete bolo možné ťažiť Bitcoiny na bežných počítačoch. V posledných rokoch však výpočtová sila siete a teda aj obtiažnosť ťažby narástli exponenciálnym spôsobom. Tento fakt je výsledkom toho, že ťažba Bitcoinu sa stala vysoko špecializovaným odvetvím. Ťažiari začali využívať špeciálne vyvinuté hardvérové zariadenia tzv. ASIC, ktoré sú optimalizované výhradne na ťažbu Bitcoinov. Algoritmus Bitcoinovej siete reaguje na nárast výpočtovej sily zvýšením obtiažnosti ťažby. Toto sa deje práve zmenou požadovaných parametrov hašu, ktorý ťažiari počítajú.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Obrázok 3: Nárast výpočtovej sily Bitcoinu (tzv. hashrate) za posledných 10 rokov



Zdroj: Blockchain.com

Zhrnutie ekonomických vlastnosti Bitcoinu:

- Fixné množstvo Bitcoinov, ktoré budú v obehu, presnejšie 21 miliónov. V súčasnosti je v obehu viac ako 18 miliónov Bitcoinov.
- Nové Bitcoiny sa emitujú do obehu pri vyťažení každého nového bloku, približne každých 10 minút.
- Množstvo nových Bitcoinov, ktoré sa dostanú do obehu ako odmena pre ťažiara po vyťažení bloku, je v súčasnosti 12,5 Bitcoinu.
- Táto odmena sa približne každé 4 roky (210 000 blokov) zmenší o polovicu.
- Najbližšie nastane delenie odmeny (tzv. halving) v máji 2020.
- Väčšina Bitcoinov bude vyťažená do roku 2030 pričom posledný Bitcoin bude vyťažený okolo roku 2130.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- Inflácia Bitcoinu v roku 2019 bola cca. 3,7 % a v nasledujúcich rokoch sa bude výrazne znižovať. V roku 2020 bude 1,8 %[24].
- Najmenšia jednotka je tzv. Satoshi, stomilióntina jedného Bitcoinu.

Zhrnutie technologických vlastností Bitcoin blockchainu:

- Doba vygenerovanie bloku a z toho vyplývajúca doba verifikácie transakcie je približne 10 minút.
- Denne sa tak vygeneruje približne 144 blokov.
- S narastajúcim výpočtovým výkonom siete sa automaticky upravuje aj obtiažnosť ťažby. Týmto je zabezpečené, že generovanie blokov vždy trvá približne 10 minút.
- Obtiažnosť siete sa upravuje približne každé dva týždne (2016 blokov).
- Bitcoinová sieť sa skladá z veľkého množstva uzlov v rozmedzí 10 000 - 100 000.
- Relatívne vysoká spotreba elektrickej energie pri Bitcoine ja zamýšľaná ako dizajnová vlastnosť systému, ktorá zabezpečuje nemeniteľnosť dát.
- Vysoká spotreba elektrickej energie nie je nevyhnutným predpokladom fungovania Bitcoinovej siete, pretože systém môže fungovať teoreticky aj na obyčajných osobných počítačoch pri zlomku súčasnej spotreby elektriny.
- Práve vysoká spotreba energie robí z Bitcoinu systém, ktorý poskytuje najväčšiu možnú garanciu nemeniteľnosti dát na svete.

[24] Viac informácií na: https://usethebitcoin.com/bitcoin-inflation-rate-will-drop-under-2-in-2020-why-does-this-matter/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- Je to tzv. open-source projekt, teda s otvoreným zdrojovým kódom, to znamená, že jeho zdrojový kód je voľne dostupný na internete.

2.3. Evolúcia Bitcoin protokolu

Bitcoin ako protokol sa významne vyvíja v čase. Množstvo vývojárov a energie, ktorú ľudia investujú do vývoja tohto protokolu, len podčiarkuje jeho globálny význam. Bitcoin sa dokonca v posledných rokoch stal štvrtým najvyvíjanejším protokolom na Githube. Vo vývojárskej aktivite ho predbehli len tri protokoly - Https, Wifi a Bluetooth. Tieto protokoly sú snáď najkľúčovejšími prvkami internetovej infraštruktúry. Fakt, že Bitcoin sa radí do skupiny týchto protokolov, implikuje dôležitosť a využitie tohto protokolu do budúcna. V rámci globálnej komunity vývojárov sa návrhy na modifikáciu zdrojového kódu Bitcoinu predkladajú vo forme BIP-ov (Bitcoin Improvement Proposal). Práve preto je veľmi dôležité uvedomiť si, že v budúcnosti sa technologické vlastnosti Bitcoinu môžu, a aj budú meniť. V nasledujúcej časti analyzujeme jednotlivé návrhy na zmenu protokolu, ktoré sú alebo budú integrované do Bitcoinu, a teda nejakým spôsobom budú mať implikácie na jeho využitie.

Podľa výskumu spoločnosti Bitmex[25], medzi najočakávanejšie modifikácie Bitcoin protokolu patria techniky ako Taproot, MAST (Merkelized Abstract Syntax Tree) či Schnorrove podpisy. Taproot je vylepšenie Bitcoin protokolu, ktoré bolo navrhnuté začiatkom roku 2018[26] jedným z Bitcoin Core vývojárov Gregorym Maxwellom. Pre vysvetlenie tohto konceptu je nutné chápať koncept skriptov v Bitcoine. Skript je pár riadkov kódu, ktorý je embednutý priamo do Bitcoinovej transakcie a ktorý definuje podmienky, za ktorých môže byť transakcia utratená.

[25] Viac informácií na: https://blog.bitmex.com/the-schnorr-signature-taproot-softfork-proposal/

[26] Viac informácií na: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

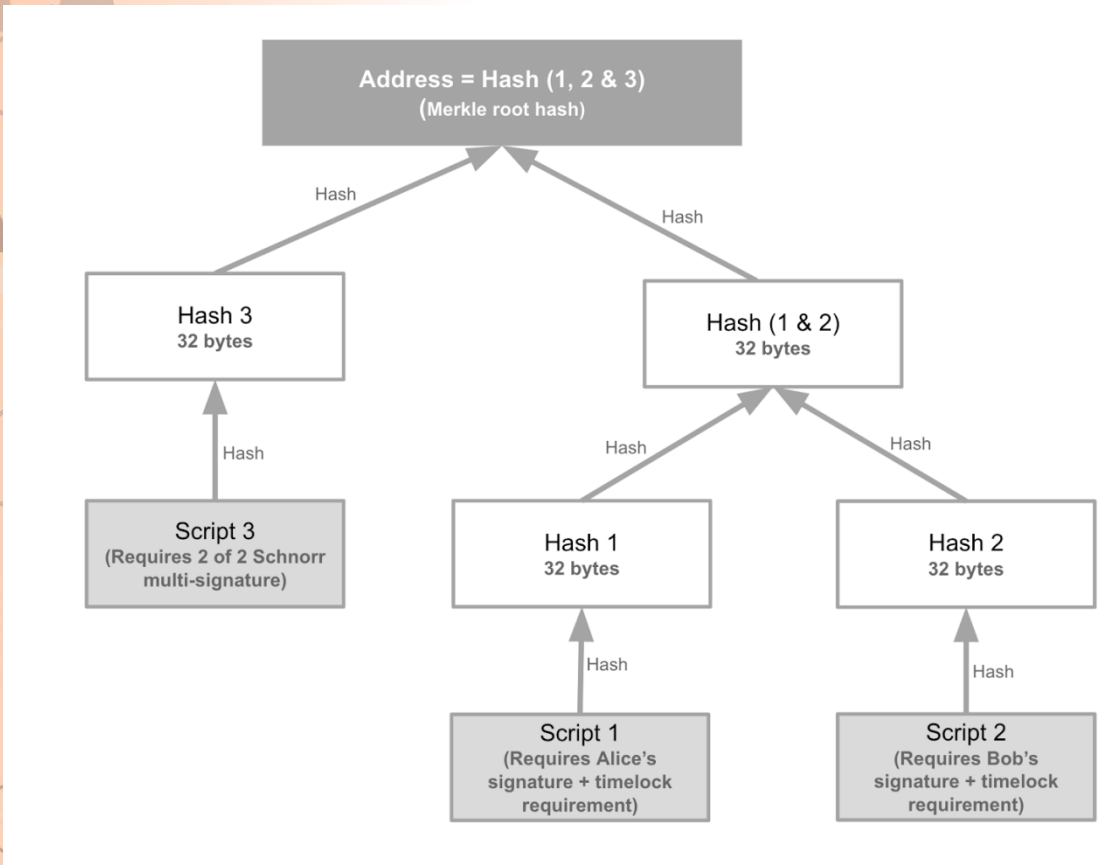
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tieto podmienky môžu zahŕňať napríklad počet potrebných podpisov (pri multi-sig transakciách) alebo špecifickú výšku bloku (pri časovaných transakciách), či iné. Jedna či viac takýchto podmienok môže byť vtesaná priamo do tela transakcie a tak vytvoriť pomerne komplexný smart kontrakt. Vďaka technikám ako P2SH (Pay to Script Hash) transakcie, obsahujúce takéto skripty, nemusia byť uložené na blockchain, pretože stačí ak na blockchain uložíme haš takéhoto skriptu. V momente, kedy bude takáto transakcia utratená právoplatným majiteľom mincí, sa však celý skript so všetkými podmienkami transakcie zverejní na blockchaine. Takýto proces je pomerne dátovo náročný a nechráni súkromie strán, ktoré sú zahrnuté v transakcii. Jedným z navrhnutých opatrení, ktoré rieši súkromie a efektívnosť týchto dát, je koncept nazvaný MAST. MAST využíva koncept hašových stromov, ktorý sme spomínali vyššie, aby vytvoril individuálny haš každej jednej transakčnej podmienky. Haše týchto podmienok potom tvoria hašový strom s jediným koreňovým hašom na vrchole stromu. Výsledkom takéhoto riešenia je, že na blockchain sa dostanú dáta len z tých transakčných podmienok, ktoré sa naplnili, ostatné ostávajú zahašované.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Obrázok 4: MAST



Zdroj: Bitmex Research

Ďalšou nevyhnutnou podmienkou pre implementáciu Taprootu sú Schnorrove podpisy, ktoré prinášajú benefity v oblasti dátovej optimalizácie transakcií. Je to primárne preto, že Schnorrove podpisy dovoľujú agregáciu viacerých podpisov do jedného, a teda výrazne šetria miesto na blockchaine. Pri komplexnejších multi-sig transakciách môže práve Taproot docieliť ďalšie zvýšenie efektivity a súkromia. Taproot teda za pomoci MAST a Schnorrových podpisov dovoľuje užívateľom modifikovať ich podpisy takým spôsobom, že komplexná multi-sig transakcia môže ostať skrytá a mať formu obyčajnej transakcie, bez toho aby bolo možné či nutné odhaliť existenciu komplexnej štruktúry využívajúcej MAST. Tieto inovatívne techniky predstavujú evolúciu nielen v Bitcoin protokole ale aj v kryptografii ako takej.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Sidechainy: Rsk a Liquid

RSK[27] je ďalší z projektov, ktorý rozširuje Bitcoin protokol o ďalšiu vrstvu, a to prostredníctvom tzv. Sidechainu čo je vlastne blockchain, ktorý tvorí akúsi nadstavbu k Bitcoinovému blockchainu. Bitcoin býva často kritizovaný za to, že nepodporuje tzv. smart kontrakty. Samotné definície smart kontraktov sa líšia, a ako sme poukázali v predchádzajúcej časti, Bitcoin podporuje určitý typ smart kontraktov. Pravdou však je, že platformy na smart kontrakty ako Ethereum, EOS, alebo TRON podporujú oveľa komplexnejšie smart kontrakty a decentralizované aplikácie v porovnaní s Bitcoinovými skriptami. RSK rieši túto limitáciu Bitcoinu tým, že buduje nad Bitcoinom sidechain, ktorý kopíruje virtuálnu mašinu Etherea, a teda podporuje komplexné smart kontrakty priamo nad Bitcoinom. V princípe je možné teda vziať akúkoľvek decentralizovanú aplikáciu z Ethereum siete a spustiť ju na Bitcoin protokole a mať Bitcoiny ako podkladové aktívum. To, že Bitcoiny môžu fungovať ako podkladové aktívum je dané tým, že RSK sidechain využíva obojsmerný peg mechanizmus, ktorý zabezpečuje, že natívna jednotka sidechainu – RBTC (Smart Bitcoin) – je krytá Bitcoinami. RSK navyše umožňuje vyššiu transakčnú priepustnosť, a to približne 400 transakcií za sekundu[28]. Liquid[29] je ďalší z projektov, ktorý stavia nad Bitcoinom sidechain, ktorý je primárne určený burzám či brokerom a finančným inštitúciám, ktoré plánujú byť aktívne v Bitcoin ekosystéme. Liquid podporuje instantné a privátne transakcie, ako aj vydávanie vlastných tokenizovaných aktív.

---

[27] Viac informácií na: https://www.rsk.co/

[28] Viac informácií na: https://developers.doc.rsk.co/docs/rsk-introduction

[29] Viac informácií na: https://blockstream.com/liquid/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2.4. Vznik a princípy fungovania Ethereum siete

Ethereum je druhá najväčšia blockchainová sieť na trhu podľa trhovej kapitalizácie a zároveň najpopulárnejšia platforma pre vývoj smart kontraktov a decentralizovaných aplikácií. Ethereum vzniklo v roku 2014 ako reakcia na obmedzenú funkcionalitu Bitcoinového programovacieho jazyka Script[30], ako aj rastúceho dopytu po využití smart kontraktov na blockchaine. Zakladateľom Etherea bol Vitalik Buterin, ktorý projekt po prvý krát oznámil ako koncept v roku 2013. Sieť ako taká bola spustená v lete roku 2015. Buterin pôvodne pracoval na projekte Counterparty[31], ktorý sa snažil o rozšírenie funkcionality samotného Bitcoinu. Buterinova predstava však bola o dosť radikálnejšia v porovnaní s vývojármi Counterparty protokolu. Začal preto pracovať na koncepte nového blockchainu s novým programovacím jazykom, ktorý by umožňoval spustenie v princípe akéhokoľvek softvéru, a teda aj smart kontraktov a decentralizovaných aplikácií. Ethereum vyzbieralo finančné prostriedky na vývoj prostredníctvom ICO (Initial Coin Offering) v roku 2014, kedy sa im podarilo vyzbierať viac než 16 miliónov dolárov predajom internej jednotky siete s názvom „Ether“. Ether, podobne ako Bitcoin, má čisto digitálnu formu a môže byť posielaný v rámci celého sveta. Na rozdiel od Bitcoinu, ktorý bol zamýšľaný ako alternatívne platidlo či peniaze, Ethereum ako sieť je zamýšľaná a dizajnovaná ako globálny počítač, ktorý je prístupný komukoľvek na svete, pretože ktokoľvek môže doňho nahrať program a interagovať so sieťou. Na vykonanie transakcie, teda zapísanie dát do globálnej databázy Etherea, je nevyhnutné zaplatiť transakčný poplatok práve vo forme Etheru. Ether teda slúži ako platidlo za využívanie tohto globálneho počítača a aj ako palivo pre decentralizované aplikácie. Decentralizované aplikácie sú v princípe akékoľvek aplikácie, ktoré sú spustené na decentralizovanej sieti ako Etheruem,

[30] Viac informácií na: https://learnmeabitcoin.com/guide/script

[31] Viac informácií na: https://counterparty.io/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

či siete podobného druhu ako napr. Dfinity[32], EOS[33], NEM[34]a podobne. Napriek tomu platí, že Ether sa dá rovnako použiť ako platidlo či uchovávateľ hodnoty.

Ethereum má zároveň najväčšiu a najaktívnejšiu komunitu zo všetkých blockchainových projektov. Podobne ako pri Bitcoine či iných decentralizovaných sieťach, ani za Ethereom nie je žiadna centrálna autorita, spoločnosť, či firma, ktorá by mala moc nad sieťou. Akýsi dohľad nad vývojom protokolu vykonáva Ethereum Foundation, v ktorej sa neformálne združuje väčšina vývojárov, či už Etherea samotného, alebo pridružených aplikácií a protokolov. Z technologického hľadiska sa Ethereum skladá z nasledujúcich komponentov[35]:

Účty – podobne ako pri Bitcoine, globálne databáza Etherea sa skladá z obrovského množstva objektov, to jest účtov, ktoré medzi sebou interagujú. Každý účet má priradenú adresu o veľkosti 20 bytov. Každý jeden účet v sieti má teda unikátny 160 bitový identifikátor. V rámci Etherea existujú dva typy účtov. Prvým typom sú externe vlastnené účty (z angl. Externally Owned Accounts alebo aj EOA), ktoré sú typicky ovládané užívateľmi siete pomocou privátneho kľúča. Tieto účty nemajú priradený žiadny kód.

Druhým typom účtov sú kontraktové účty, ktoré sú kontrolované kódom kontraktu a teda majú asociovaný kód. Hlavným rozdielom medzi týmito dvoma typmi účtov je, že externe vlastnené, alebo užívateľské účty, môžu posielať správy iným užívateľským či kontraktovým účtom vytvorením a podpísaním transakcie, zatiaľ čo kontraktové účty nemôžu samy od seba inicializovať transakcie. Pri typickej transakcii medzi dvoma užívateľskými účtami sa jedná

---

[32]Viac informácií na: https://dfinity.org/

[33]Viac informácií na: https://eos.io/

[34]Viac informácií na: https://nem.io/

[35]Viac informácií na: https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

o presun nejakej hodnoty, transakcia z užívateľského účtu na kontraktový účet aktivuje kód, ktorý je s daným účtom asociovaný. Takýto kód následne vykoná inštrukcie, ktoré sú v ňom obsiahnuté, ako napr. zápis do internej databázy, razenie nových digitálnych mincí či vykonanie určitých kalkulácií. Kontraktové účty môžu vykonať transakcie len v reakcii na podnety (transakcie), ktoré dostanú či už od užívateľského účtu alebo od iného kontraktového účtu.

Stav účtu – Ethereum na rozdiel od Bitcoinu nepoužíva transakčný model založený na transakčných outputoch (UTXO), ale zachytáva stavy účtov. Stav siete sa rovnako mení na základe transakcií. Takýto stav je zachytený pomocou štyroch komponentov:

- *Nonce* – Ak sa jedná o užívateľský účet, tak toto číslo reprezentuje množstvo transakcií vykonaných daným účtom, pri kontraktových účtoch toho číslo zachytáva počet vytvorených kontraktov daným účtom.
- *Bilancia* – Množstvo etherov, ktoré sú na danom účte.
- *Koreňový haš (StorageRoot)* – Koreňový haš hašového stromu, ktorý vyjadruje haše dát v úložisku prislúchajúce danému účtu.
- *Haš kódu (codeHash)* – haš kódu prislúchajúcemu danému účtu (pri kontraktových účtoch)

Schopnosť Etherea zachytiť informácie a dáta súvisiace s rôznymi účtami vo forme dátových štruktúr ako hašové stromy (z angl. Merkle Trees) je kľúčová hlavne pre tzv. Light peňaženky, ktoré neuchovávajú celú transakčnú históriu siete, ale len hlavičky jednotlivých blokov. Naopak, plné uzly rovnako ako pri Bitcoine uchovávajú celý blockchain lokálne. Aplikovaná dátová štruktúra umožňuje komukoľvek jednoducho overiť integritu dát či transakcií v blokoch.

Gas a transakčné poplatky – Jedným z kľúčových aspektov Etherea sú podobne ako pri Bitcoine transakčné poplatky, ktoré však v tomto prípade fungujú trochu inak. Akékoľvek vykonanie

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

operácie na Ethereum blockchaine je podmienené zaplatením patričného poplatku. Transakčné poplatky na Ethereum sieti sú denominované ako tzv. „gas“. Gas je teda jednotka používaná na meranie transakčných poplatkov, prislúchajúcich operáciám a výpočtom v rámci Etheruem siete. Podobne ako pri Bitcoine, kedy užívateľ v transakčnom poplatku určí koľko je ochotný zaplatiť za danú transakciu, pri transakciách v Ethereum sieti musí užívateľ v rámci nastaviteľných transakčných parametrov určiť tzv. „Gas price“, teda maximálnu cenu, ktorú je ochotný zaplatiť za danú transakciu. Táto cena je meraná v jednotke „gwei“. Jeden gwei sa rovná hodnote jednej miliardy „Wei“. Wei je najmenšia nominálna jednotka v Ethereum sieti, pričom platí, že jeden ether má 10^{18} jednotiek Wei. V prípade, že odosielateľ transakcie nemá dostatok etheru na účte a pošle transakciu, táto transakcia zlyhá. Záznam o zlyhaní transakcii sa však zapíše, a keďže tento zápis sám o sebe vyžaduje výpočtovú kapacitu siete, transakčný poplatok s tým súvisiaci nebude odosielateľovi vrátený. Aj pri Ethereu platí, že čím väčší maximálny poplatok odosielateľ zvolí, tým vyššia šanca, že ťažiari zaradia transakciu do svojich blokov, a teda že bude transakcia rýchlejšie potvrdená. Rovnako platí, že akákoľvek transakcia, resp. výpočet nutný na vykonanie inštrukcií v kóde, je vykonaný na každom jednom uzle v sieti. Avšak, výkon výpočtov a operácií v rámci siete sú pomerne drahé, a preto je vhodné do smart kontraktov dávať pomerne jednoduché inštrukcie, ktoré nie sú náročné na výpočtovú kapacitu. Ako uvádzame vyššie, transakcie ako také sú zodpovedné za zmenu stavu siete.

Bloky – Z povahy blockchainu, aj pri Ethereum sieti sú transakcie ukladané do blokov. Tieto bloky sú taktiež matematicky prepojené pomocou hašov. Jednou z kľúčových častí blokov sú ich hlavičky, ktoré obsahujú najdôležitejšie informácie zahrnuté v bloku. Medzi tieto informácie patria napríklad dáta ako stav obtiažnosti siete, haš predchádzajúceho bloku, poradové číslo bloku, časovú pečiatku, či haš transakcií zahrnutých v danom bloku.

Transakcie – Vo svojej podstate je transakcia kryptograficky podpísaná inštrukcia vygenerovaná užívateľským účtom a odoslaná do siete. Ako spomíname vyššie, kontrakty môžu medzi sebou navzájom taktiež komunikovať. Môžu tak robiť prostredníctvom dvoch

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

základných typov transakcií – správ a interných transakcií. Ak jeden kontraktový účet pošle internú transakciu inému kontraktovému účtu, spustí sa tak vykonanie inštrukcií, ktoré má prijímajúci kontrakt obsiahnuté vo svojom kóde. Transakcie musia spĺňať určité parametre dané protokolom na to, aby boli považované za platné. Musia mať správny formát[36].

Ťažba – Podobne ako pri Bitcoine, aj pri Ethereu, jediný spôsob pre ťažiarov, ako môžu nájsť a vygenerovať blok, je vykonať milióny matematických operácií, až kým nenájdu správny haš. Taktiež, rovnako platí, že očakávaný čas nájdenia správneho hašu je úmerný výške obtiažnosti siete. Aj keď Ethereum má na rozdiel od Bitcoinu tento limit nastavený výrazne nižšie a to na približne 14 sekúnd (pri Bitcoine to je 10 minút).

2.5. Blockchain a nemeniteľnosť dát

Existuje niekoľko rôznych definícii blockchainu. Aj na základe predchádzajúcich častí tejto kapitoly však Blockchain môžeme najjednoduchšie definovať ako distribuovanú, transparentnú a nemennú účtovnú knihu. Distribuovaná ju voláme, pretože jej kópia je uložená na tisíckach serverov a počítačov, ktoré môžu byť rozmiestnené po celom svete. Do tejto účtovnej knihy sa zapisujú všetky transakcie, ktoré sa dejú v sieti. Technológia blockchain získala svoje meno hlavne kvôli spôsobu, akým sa ukladajú transakcie do blokov. Keďže sú tieto bloky matematicky prepojené, tvoria akúsi pomyselnú reťaz blokov. Matematická prepojenosť blokov prostredníctvom hašov má za následok aj jednu z najkľúčovejších vlastností blockchainu – a to nemeniteľnosť dát. To znamená, že raz keď sa zapíšu akékoľvek dáta do blockchainu, je takmer nemožné ich spätne meniť. To je spôsobené práve tým. že dáta

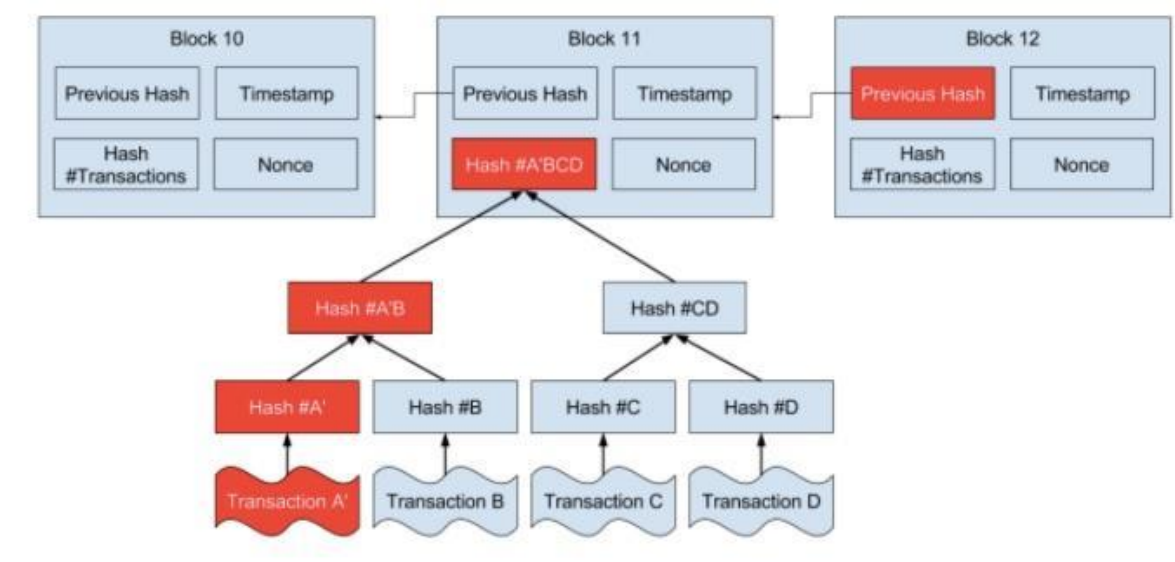
[36] Ethereum využíva formát „RLP“ (Recursive Length Prefix).

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

v blokoch sú hašované, a teda akákoľvek zmena vstupných dát pozmení aj korešpondujúci haš, to následne zmení ďalšie haše v rámci štruktúry hašových stromov, vrátane koreňového hašu, až po haš samotného bloku. Takáto zmena by automaticky ovplyvnila haše všetkých nasledovných blokov, keďže každý blok v rámci blockchainu obsahuje haš predchádzajúceho bloku, a to má za následok akúkoľvek manipuláciu s dátami ľahko detekovateľnú.

Obrázok 5: Spôsob detekovania manipulácie s dátami

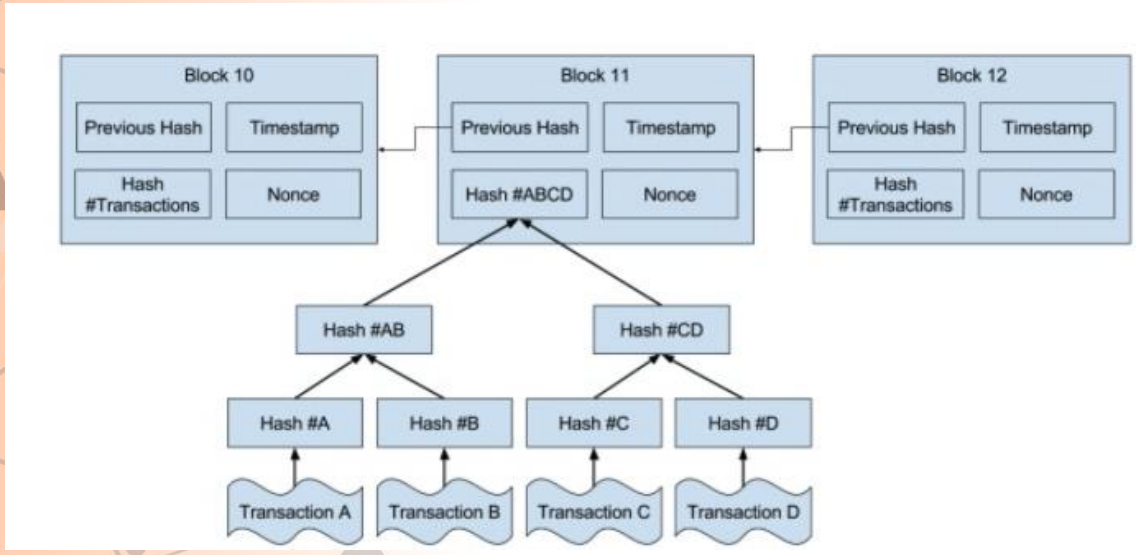


Zdroj: Linux Foundation

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Obrázok 6: Dátová štruktúra použitá v blockchaine



Zdroj: Linux Foundation

Avšak, je dôležité dodať, že nemeniteľnosť blockchainu je skôr relatívna ako absolútna. Napriek tomu, že je pomerne nepraktické pre potenciálneho útočníka napadnúť blockchainovú sieť a zmeniť v nej dáta, je to teoreticky možné. Taktiež v histórii existuje niekoľko príkladov, ktoré demonštrovali relatívnosť nemeniteľnosti dát v blockchaine. Snáď najznámejším takýmto príkladom bol 51 % útok na blockchainovú sieť Ethereum Classic začiatkom januára 2019[37]. Útočníkovi sa vtedy podarilo napadnúť sieť a spätne zvrátiť niekoľko transakcií, čo malo za následok škody vo výške približne jedného milióna dolárov. Nemeniteľnosť dát v blockchaine do veľkej miery súvisí s veľkosťou siete, ako aj s konsenzuálnym algoritmom, ktorý je v danej sieti implementovaný. Napriek tomu, že Proof-of-Stake algoritmy sa stávajú čím ďalej tým populárnejšie a sú často implementované do blockchainových sietí, ich bezpečnostné garancie sa vo všeobecnosti považujú za nižšie

[37] Viac informácií na:.https://bravenewcoin.com/insights/etc-51-attack-what-happened-and-how-it-was-stopped

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

v porovnaní s Proof-of-Work algoritmami, ktoré sú však kritizované za vysokú spotrebu elektrickej energie. Relatívne vysoká spotreba elektrickej energie je však práve to, čo do veľkej miery garantuje nemeniteľnosť dát v (Bitcoin) blockchaine. Je to dané tým, že pri takomto type zabezpečenia siete je skrátka akýkoľvek pokus o spätnú zmenu dát extrémne drahý, pretože to zahŕňa obrovské množstvo matematických výpočtov, ktoré spotrebujú veľké množstvo energie. Pri Proof-of-Stake algoritmoch však existuje možnosť generovať bloky bez toho aby bolo treba počítať náročné výpočty, a to môže mať za následok to, že validátor blokov môže teoreticky vytvárať dve rôzne verzie transakčnej histórie (blockchainu), a pokúsiť sa o prepísanie dát z minulosti.

V konečnom dôsledku môžeme povedať, že bezpečnosť dát v blockchaine je priamo úmerná výške nákladov, ktoré sú spojené s 51 % útokom[38]. Čím vyššie sú náklady na takýto útok, tým menšia je pravdepodobnosť takého útoku, a teda tým vyššie bezpečnostné garancie blockchain poskytuje. Ako uvádzame v tabuľke nižšie, náklady na 51 % útok sa diametrálne líšia naprieč rôznymi kryptomenami. Zároveň je nutné dodať, že tieto čísla sú len orientačné, a do celkovej evaluácie siete a jej rezistencie voči 51 % útoku vstupujú aj ďalšie faktory. Jedným z takých faktorov sú už spomínané konsenzuálne algoritmy. Niektoré siete nezabezpečujú dáta len prostredníctvom PoW algoritmu, ale kombinujú ho s PoS či iným algoritmom. Takýmto prípadom je napríklad aj kryptomena Dash, v ktorej sieti sú bloky generované nielen ťažiarmi, ale aj vrstvou tzv. Master uzlov (z angl. masternodes) nad nimi, ktoré využívajú PoS. To má za následok, že na to, aby potenciálny útočník vykonal 51 % útok, musel by disponovať nielen značnou výpočtovou kapacitou, ale aj značným množstvom Dash mincí. Ak sa jedná o externého útočníka, ktorý žiadne také mince nemá, nákup by sa mu pravdepodobne mohol

[38]Viac informácií na: https://www.exaking.com/51

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

značne predražiť. Vzhľadom na veľmi volatilnú cenu, ako aj obchodované objemy kryptomien na svetových burzách, je ťažké vypočítať finálne náklady spojené s takýmto útokom.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tabuľka 1: Porovnanie nákladov na 51 % útok naprieč kryptomenami

Kryptomena	PoW Algoritmus	Výpočtová kapacita siete (hashrate)	Náklady na 51 % útok na 1 hodinu	Dostupnosť cez Cloudovú ťažbu
Bitcoin	SHA-256	32,8 PH/s	$553 982	2%
Ethereum	Ethash	213 TH/s	$360 114	3%
Bitcoin Cash	SHA-256	4,268 PH/s	$72 093	12%
Litecoin	Scrypt	313 TH/s	$64 954	6%
Monero	CryptoNightV7	402 MH/s	$21,151	13%
Dash	X11	2 PH/s	$15 439	27%
Ethereum Classic	Ethash	6TH/s	$10,643	89%

Zdroj: Exaking.com

Ďalším významným faktorom pri zabezpečení blockchain sietí, ktoré využívajú PoW algoritmus, je dostupnosť hardvéru na ťažbu. Niektoré kryptomeny, ako Bitcoin či Dash, sa v praxi ťažia výlučne špecializovaným hardvérom, tzv. ASIC-om. Keďže je na trhu len niekoľko málo výrobcov takého hardvéru, a je to historicky nedostatkový tovar, je pomerne náročné získať veľké množstvo ASIC-ov. Väčšia časť kryptomien sa však ťaží prostredníctvom výkonných grafických kariet (z angl. GPU - Graphic Processing Unit). Na trhu grafických kariet je relatívne väčšia konkurencia výrobcov, no aj to nemusí stačiť na pokrytie potrieb a dopytu

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

trhu, ako to bolo napríklad aj počas roku 2017, kedy kryptomeny všeobecne nabrali na popularite. Efektívnosť ťažby danej kryptomeny grafickými kartami sa ďalej líši v závislosti od konkrétnej hašovej funkcie, ktorá je v danom algoritme použitá. Tieto, ako aj ďalšie faktory majú teda v konečnom dôsledku vplyv na náklady súvisiace s napadnutím danej blockchainovej siete.

2.6. Verejný vs. súkromný blockchain

Blockchain sa ďalej najčastejšie delí na verejný a súkromný (alebo privátny). Verejné blockchainy sa typicky využívajú práve pri kryptomenách a ich najvýraznejšou charakteristickou črtou je, že participácia na ich sieti je otvorená komukoľvek, kto má záujem. Ktokoľvek môže vytvárať či validovať bloky, a teda aj dáta v nich, ak si stiahne patričný softvér. Taktiež, ak je blockchain verejný, a teda ktokoľvek si môže stiahnuť celú transakčnú históriu do vlastného počítača, je väčšia šanca, že sieť bude čo najviac decentralizovaná.

Privátne blockchainy sa väčšinou používajú v korporátnom prostredí, kedy právo participovať na sieti je dané len serverom jednej či viacerých korporácií. Tým pádom je uzlov v sieti výrazne menej ako pri verejných blockchainoch, a každý uzol v sieti vie identitu všetkých ostatných uzlov. Toto má za následok, že privátne blockchainy sú mnohonásobne rýchlejšie v procesovaní transakcií v porovnaní s verejným blockchainom. Je to však za cenu väčšej centralizácie.

Napriek tomu, že dáta vo verejných blockchainoch sú prístupné komukoľvek, nemusí to nevyhnutne znamenať, že sa nedajú šifrovať a teda uchovávať informácie súvisiace s obchodnými tajomstvami a podobne. Najmä v posledných pár rokoch sa veľká časť teoretického výskumu ale aj praktického vývoja sústreďuje na implementáciu tzv. zero-

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

knowledge protocols (ZKP), teda protokolov s nulovými rozšírením informácií. Inštancia ZKP je implementovaná v súčasnosti napríklad v kryptomene Zcash[39].

Verejné blockchainy sa označujú aj ako „permissionless blockchain platforms," čo znamená, „platformy bez povolenia." To znamená, že ktokoľvek do nich má prístup, môže participovať na sieti napríklad formou validácie transakcií, a nepotrebuje na to súhlas tretej strany. Napriek tomu, aj keď blockchainy kryptomien ako Bitcoin, Ethereum alebo Litecoin sú verejné, je možné na nich postaviť riešenia, ktoré budú mať vlastnosti ako súkromné blockchainy. Rovnako, nakoľko sa jedná o otvorený zdrojový kód, ktokoľvek ho môže použiť a spustiť si vlastnú sieť, ktorá bude technologicky identická danému protokolu, ale bude sa skladať z iných uzlov, a teda mať aj kompletne inú transakčnú históriu. Toto je špecifické najmä pre blockchain Etherea.

Blockchain Etherea, Litecoinu alebo Bitcoinu je verejný z dôvodu, aby mohla byť zachovaná anonymita a súkromie pre používateľov siete. Tu treba upozorniť, že blockchain spomínaných kryptomien je pseudo-anonymný. S tým súvisí jeho otvorenosť, aby každý mohol transparentne do neho nazerať, avšak nikto nevidí reálne identity za jednotlivými adresami. Naopak, pri privátnych blockchainoch je to opačne, keďže cieľom je mať kontrolu nad sieťou, ako aj nad identitou užívateľov a zároveň si vyberať komu bude umožnené posielať transakcie, či nazerať do histórie transakcií. Medzi projekty privátnych blockchainov patrí napr. Hyperledger, Hashgraph, Corda.

[39] Viac informácií na: https://z.cash/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tabuľka 2: Porovnanie privátneho a verejného blockchainu

Verejný blockchain	Privátny blockchain
- ktokoľvek môže participovať - relatívne pomalšie - viac uzlov v sieti - vyššia miera decentralizácie - vyššia miera anonymity - typický pri kryptomenách	- participujú len vybrané uzly jednej či viacerých organizácií - relatívne rýchlejšie - menej uzlov v sieti - menej decentralizované - absencia anonymity - typicky využitie v korporátnom prostredí

Zdroj: Štúdia možností a potenciálu technológie „blockchain“ pri zlepšovaní eGovernment riešení, E&Y

Z vyššie uvedeného vyplýva aj nastavenie motivácií v systéme. Pri verejných blockchainoch sa často pracuje s rôznymi modelmi založenými na teórii hier. Cieľom týchto modelov je nasimulovať motivácie participantov v sieti takým spôsobom, aby bolo v ich záujme správať sa podľa pravidiel protokolu, a naopak penalizovať ich za správanie, ktoré je v rozpore s protokolom. To znamená, že poctiví používatelia, ktorí sa správajú podľa pravidiel, sú v sieti odmeňovaní, zatiaľ čo nepoctiví odmeňovaní nie sú.

Naopak v rámci privátnych blockchainov rozhoduje o potrestaní za správanie mimo pravidiel organizácia, alebo konzorcium organizácií, ktoré je zodpovedné za jeho správu. Napriek tomu oba typy blockchainov majú svoje výhody, ale aj nevýhody.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2.7. Konsenzuálne algoritmy

Jedným z najväčších technologických prínosov Bitcoinu bolo práve využitie princípu PoW ako nástroja na dosiahnutie konsenzu medzi tisíckami anonymných serverov, ktoré sa neustále pripájajú či odpájajú zo siete. Konsenzuálne algoritmy sa dovtedy skúmali v rôznych oboroch v rámci informačných technológií ako problémy súvisiace s replikáciou stavu počítačových mašín. Zatiaľ čo konsenzuálne algoritmy, ktoré umožnili replikovať ten istý stav naprieč viacerými počítačmi, existovali od osemdesiatych rokov, ich fungovanie do veľkej miery záviselo na viacerých faktoroch, ako napríklad známa identita počítačov. Tieto algoritmy fungovali teda len v prostredí, v ktorom bolo vopred definované kvórum počítačov, ktoré mali medzi sebou komunikovať. Zároveň platilo, že každý počítač poznal identitu všetkých počítačov v sieti. Takéto nastavenie funguje dobre pri uzavretej skupine organizácií či skupín v rámci jednej organizácie. Avšak, nefunguje pre skutočne decentralizovanú sieť, kde neexistuje centrálny koordinátor, a kde sa každú chvíľu mení počet, lokalita a identita počítačov v sieti. V takomto prostredí je navyše prítomná pomerne vysoká latencia t. j. oneskorenie súvisiace s prenosom informácií, a komunikácia medzi tisíckami počítačov je veľmi problematická. PoW sa ukázal byť skvelým riešením tohto problému. Naviazal vygenerovanie každého jedného bloku na vyriešenie matematickej úlohy, ku ktorej neexistujú skratky, a dá sa získať len pomerne náročnými výpočtami, ktoré pália elektrinu. Postupom času ako Bitcoinová sieť začala rásť, rástol aj počet ťažiarov a tým aj náročnosť ťažby. Napriek tomu, že je to práve množstvo spotrebovanej elektrickej energie čo garantuje nezmeniteľnosť dát v blockchaine, býva Bitcoin často kritizovaný za neudržateľnosť a problematickosť hlavne v súvislosti so životným prostredím. Z toho dôvodu sa po popularizácii Bitcoinu začali v rámci výskumu hľadať alternatívne konsenzuálne mechanizmy, ktoré by mohli plnohodnotne nahradiť PoW.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Proof-of-Work (PoW)

Proof-of-Work sa ako koncept objavil už v deväťdesiatych rokoch. Adam Back ho už v spomínanej práci nazvanej Hascash[40] navrhol ako mechanizmus proti spamu v emailovej komunikácii. Logika systému spočívala v tom, že užívateľ musel pred poslaním emailu vypočítať kryptografický hash, ktorý reprezentoval token, ktorý bol následne zasadený do hlavičky emailu a prijímaciemu serveru signalizoval validitu. Bežného užívateľa by množstvo takýchto výpočtov nezaťažilo, no užívateľovi, ktorý by chcel poslať desiatky tisíc správ ako spam by to zvýšilo náklady na elektrinu. Hoci prvé koncepty digitálnych peňazí ako B-money či Bitgold tiež pracovali s konceptom PoW, Satoshi Nakamoto bol prvý kto použil PoW ako nástroj na dosiahnutie konsenzu ohľadom stavu transakcií v rámci P2P siete. Ako sme spomínali na začiatku tejto kapitoly, hašový algoritmus premení akékoľvek množstvo vstupných dát na výstup nemennej veľkosti (napr. 256 bitov), čo predstavuje digitálny odtlačok dát. Kľúčovou vlastnosťou hašových algoritmov je, že je v realite takmer nemožné nájsť dva rozdielne dátové vstupy, ktoré by vyprodukovali rovnaký výstup. V prípade, že by sa tak stalo, vravíme o kolízii. Taktiež platí, že je nemožné dopredu vedieť aký výstup bude vypočítaný z daného vstupu. Preto, ak chceme výstup, ktorý spĺňa určité nami dané charakteristiky, neostáva nám nič iné len vypočítať rad za radom haš z náhodných vstupov. Toto je presne princíp na ktorom funguje ťažba Bitcoinov. Algoritmus siete predeterminuje aké kritéria by mal haš spĺňať, a ťažiari počítajú haš z kombinácie transakčných dát v rámci blokov a náhodne zvolených dát (tzv. nonce).

Hoci bol teda Proof-of-Work vynájdený už v 90. rokoch, spôsob akým bol aplikovaný v Bitcoine, vyriešil problém koordinácie uzlov v distribuovanej sieti. Napriek tomu, že sa tento problém

---

[40] Viac informácií na: http://www.hashcash.org/papers/hashcash.pdf

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

skúmal už desiatky rokov, po objavení Bitcoinu sa tempo výskumu v tejto oblasti rapídne zvýšilo a začali sa skúmať alternatívne konsenzuálne algoritmy a mechanizmy, ktoré by boli šetrnejšie k životnému prostrediu a ich bezpečnostné garancie by neboli postavené na energeticky náročných výpočtoch. V posledných rokoch sa najpopulárnejšou alternatívou k PoW stáva Proof-of-Stake (PoS) algoritmus, ktorý je používaný naprieč širokým spektrom kryptomenových projektov. V nasledujúcej časti analyzujeme nielen PoS ale aj alternatívne systémy zabezpečenia blockchain sietí.

Proof-of-Stake (PoS)

PoS systém je založený na podobných princípoch ako PoW, a teda je taktiež zraniteľný voči 51 % útoku. Veľkým rozdielom ale je, že váha jednotlivých uzlov v rámci siete nie je meraná proporčne k ich výpočtovej sile, ale k množstvu mincí, ktoré majú. Takže ak má daný uzol 10 % všetkých mincí v obehu z danej kryptomeny, je to ekvivalentné tomu, ako keby mal 10 % z celkovej výpočtovej kapacity kryptomeny založenej na PoW systéme, a teda daný uzol „vyťaží" približne každý desiaty blok. Trend popularizácie PoS je zrejmý a demonštruje ho napríklad aj Ethereum ako druhá najväčšia kryptomenová sieť. Ethereum od svojho spustenia fungovalo na PoW systéme podobnému Bitcoinu. No v posledných rokoch sa developeri a výskumníci v rámci Ethereum komunite venujú práve prechodu z PoW na PoS mechanizmus. Samotná transformácia by sa mala odohrať v priebehu roka 2020[41]. V rámci PoS systémov existuje veľké množstvo modifikácií a nastavení, ktoré môžu mať obrovský vplyv na zabezpečenie siete. Jednou z častých kritík PoS systémov je, že poskytujú menšie bezpečnostné garancie vzhľadom na to, že vytvorenie blokov nič nestojí a teda validátor blokov môže teoreticky budovať viacej verzií blockchainu (a teda viacej verzií transakčnej histórie), čo predstavuje potenciálny vektor útoku. Existuje niekoľko možných riešení ako je možné mitigovať takéto riziko. Jedno z

[41]Viac informácií na: https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/proof-of-stake/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

najpopulárnejších je penalizácia validátorov, ktorí nepostupujú v súlade s protokolom[42]. Toto opatrenie je implementované do nadchádzajúceho protokolu Etherea, ako aj iných sietí, ako napr. Cosmos[43].

Delegated Proof-of-Stake (DPoS)

Delegated Proof-of-Stake vznikol ako modifikácia PoS systémov a bol prvý krát implementovaný v rámci Bitshares[44] siete. Jedná sa o systém, v ktorom participanti siete delegujú svoje rozhodovacie právo na užšie kvórum uzlov (typicky niekoľko desiatok), ktoré má následne na starosti validáciu blokov. Výhodou tohto systému je, že pre nižší počet uzlov umožňuje vyššiu priepustnosť transakcií. Nevýhodou je zas vyššia miera centralizácie. V rámci DPoS systémov existuje taktiež viacero možných modifikácií, ktoré majú implikácie na fungovanie a vlastnosti systému. V súčasnosti sa tento mechanizmus využíva vo viacerých sieťach, ako napr. Neo[45] či Decent[46].

Proof-of-Importance (PoI)

Proof-of-Importance bol implementovaný prvý krát v roku 2015 v rámci NEM[47] blockchainu. V princípe sa jednalo o vylepšenie PoS a to takým spôsobom, že sa pri výpočte váhy jednotlivých uzlov v sieti berú do úvahy aj ďalšie faktory okrem množstva mincí, ktoré uzol vlastní. Takými faktormi môže byť napríklad množstvo prichádzajúcich či odchádzajúcich transakcií, ako aj „dôležitosť" uzlov, s ktorými daný uzol vykonáva transakcie. Ako sme spomínali vyššie, v rámci

[42] Viac informácií na: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#can-multi-currency-proof-of-stake-work

[43] Viac informácií na: https://cosmos.network/

[44] Viac informácií na: https://bitshares.org/

[45] Viac informácií na: https://neo.org/

[46] Viac informácií na: https://decent.ch/

[47] Viac informácií na: https://nem.io/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

konsenzuálnych mechanizmov existuje široká škála riešení, ktoré sa líšia v rôznych implementačných detailoch, ktoré však nie sú významné pre účely tejto analýzy. Pre úplnosť je však na mieste spomenúť ďalšie významné protokoly, ktoré sú momentálne v štádiu výskumu a pracuje sa na ich implementácii do blockchainových sietí. Väčšinou sa jedná o modifikácie PoS algoritmov a medzi najvýznamnejšie patrí Ourobros v rámci Cardano siete[48], či Avalanche v rámci AVA siete[49].

Alternatívne dátové štruktúry

V rámci blockchain ekosystému nájdeme okrem širokej škály konsenzuálnych algoritmov taktiež aj technológie rôznych dátových štruktúr, ktoré sa využívajú v rámci distribuovaných P2P sietí, a ktoré sa dajú z určitého uhla pokladať za alternatívy k blockchainu. Keďže neexistuje striktná definícia blockchainu, tak sa tieto technológie často považujú za blockchain tiež, napriek tomu, že ich dátová štruktúra nepripomína reťaz blokov. Aj pre tieto menšie technické nuancie sa často používa termín DLT (z angl. Distributed LEdger Technology), pod ktorý sa môžu tieto technológie zahrnúť. Najčastejšou alternatívou pri dátových štruktúrach je orientovaný acyklický graf (z angl. Directed Acyclic Graph - DAG). Implementácie acyklických grafov sa taktiež môžu navzájom výrazne líšiť. Najznámejšími kryptomenovými systémami, ktoré využívajú takúto dátovú štruktúru sú Maidsafe[50], IOTA[51] či Hashgraph[52]. Okrem

[48] Viac informácií na: https://cardanodocs.com/cardano/proof-of-stake/

[49] Viac informácií na: https://hackernoon.com/avalanche-ava-blockchain-3-0-a-novel-metastable-consensus-protocol-28cdc4ee8984

[50] Viac informácií na: https://maidsafe.net/

[51] Viac informácií na: https://www.iota.org

[52] Viac informácií na: https://www.hedera.com/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

acyklického grafu sa v poslednej dobe začali objavovať aj nové typy databáz využívajúce aj novú dátovú architektúru ako napríklad Radix[53] alebo Holochain.

2.8. Technologické riešenia na vyšších vrstvách

Blockchain ako technológia priniesla so sebou doteraz nevídané garancie týkajúce sa nemeniteľnosti dát, avšak za cenu toho, že takých dát nemôže byť veľa. Kapacita blokov takmer v každej významnejšej blockchain sieti je pomerne striktne obmedzená a to robí blockchain nevhodným nástrojom na uchovávanie väčšieho množstvá dát. Tento fakt má obrovský vplyv na škálovateľnosť blockchainu a priepustnosť pri množstve transakcií za sekundu. Z toho dôvodu sa v posledných rokoch venuje veľká pozornosť budovaniu rozširujúcich vrstiev nad hlavným blockchainom, či už ide o Bitcoin alebo Ethereum. V prípade Bitcoinu sa najznámejšia inštancia 2. vrstvy volá Lightning Network. V prípade Etherea existuje podobných riešení viacero napr. Raiden[54], Plasma[55] alebo stavové kanály (z angl. State Channels).

Lightning Network

Bitcoin má robustnú sieť skladajúcu sa z niekoľko desiatok tisíc serverov. Dizajn siete bol navrhnutý tak, aby sieť dosiahla čo najväčšiu možnú decentralizáciu a aby bolo relatívne nenáročné pre kohokoľvek sa pripojiť do siete a rozbehnúť si vlastný uzol v sieti. Toto rozhodnutie však prinieslo určité obmedzenia týkajúce sa výkonnosti a kapacity protokolu. Z tohto dôvodu sa nedajú všetky modifikácie a vylepšenia protokolu implementovať v rámci prvej vrstvy protokolu a je nevyhnutné vytvárať nové vrstvy nad samotným blockchainom. V súčasnosti pracuje niekoľko tímov na rôznych riešeniach predstavujúcich druhú či dokonca

[53] Viac informácií na: https://docs.radixdlt.com/kb/learn/platform

[54] Viac informácií na: https://raiden.network/

[55] Viac informácií na: https://plasma.io/plasma-contracts.html

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

tretiu vrstvu nad Bitcoin protokolom. Najznámejším takým riešením je Lightning Network, ktoré bolo prvý krát navrhnuté v roku 2016[56].

Lightning Network umožňuje vytvárať off-chain platobné kanály, v rámci ktorých je možné posielať tisícky transakcií za sekundu a teda výrazne zvýšiť transakčnú kapacitu siete. Tieto transakcie však nie sú priamo zapisované do blockchainu, a teda poskytujú relatívne nižšie bezpečnostné garancie. Namiesto toho, po vytvorení kanálu užívatelia vykonávajú transakcie medzi sebou, a finálny zostatok účtov je zapísaný do blockchainu v momente, keď sa rozhodnú kanál zatvoriť. Pri vytvorení platobného kanála užívateľ zároveň nabije kanál určitým množstvom Bitcoinov, ktoré sú uzamknuté v multi-sig transakcii, a ktoré predstavujú kapacitu kanála. Hodnota transakcií v rámci kanálov nemôže prekročiť túto kapacitu. Vytvorenie, ako aj zatvorenie platobného kanála vyžaduje vykonanie on-chain transakcie. Transakcie vykonané v rámci off-chain kanálov majú omnoho nižšie poplatky v porovnaní s on-chain transakciami. Zaujímavou vlastnosťou Lightning siete je to, že transakcie nemusia byť vykonané len v rámci jedného kanála, ale v rámci celej siete kanálov. Napriek tomu, že je Lightning Network považovaná stále za experiment, má sieť v súčasnosti (október 2019) viac než 10 000 uzlov, viac než 35 000 platobných kanálov, ktoré majú v sebe uzamknutých viac ako 800 Bitcoinov[57] (cca 7 miliónov USD). Na rozdiel od prvej vrstvy, v ktorej transakčné poplatky získavajú ťažiari, v rámci Lightning siete idú transakčné poplatky vlastníkom uzlov, cez ktoré sa prenášajú transakcie, a ktorí poskytujú likviditu sieti. Architektúra a fungovanie Lightning siete má teda obrovské implikácie na praktické vlastnosti Bitcoinu, nakoľko výrazne zvyšuje nielen transakčnú kapacitu siete, ale aj anonymitu transakcií.

---

[56]Viac informácií na: https://lightning.network/lightning-network-paper.pdf

[57]Viac informácií na: https://1ml.com/statistics

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tabuľka 3: Porovnanie vlastností prvej a druhej vrstvy Bitcoin protokolu

Bitcoin blockchain (1. vrstva)	Lightning Network (2. vrstva)
vyššie transakčné poplatky	nižšie transakčné poplatky
transakcie vyššej hodnoty	mikro transakcie
vyššia bezpečnosť	nižšia bezpečnosť
transparentný záznam o transakciách	privátne transakcie
nízka priepustnosť transakcií	vysoká priepustnosť transakcií
pomalé transakcie	instantné transakcie

V súčasnosti existuje sedem rôznych implementácií Lightning siete, ktoré sú vyvíjané rôznymi skupinami vývojárov v rôznych programovacích jazykoch[58]. Väčšina z týchto implementácií sú však navzájom kompatibilné, takže z pohľadu užívateľa nezáleží na tom, ktorú z nich použije. Väčšina z nich však vyžaduje, aby užívateľ mal vlastný uzol v rámci Lightning siete. Prerekvizitou k tomu je taktiež vlastný uzol v rámci Bitcoin siete. Toto samozrejme nie je praktické pre väčšinu užívateľov, a dá sa očakávať, že v blízkej budúcnosti bude čím ďalej tým viac Lightning aplikácií a peňaženiek, ktoré umožnia užívateľom vykonávať transakcie aj bez

[58] Viac informácií na: https://github.com/bcongdon/awesome-lightning-network

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

toho, aby museli mať vlastný uzol. Ako bolo spomenuté, sieť je stále v experimentálnej fáze a jej funkcionalita sa bude pravdepodobne výrazne meniť a vyvíjať v budúcnosti.

Druhá vrstva Ethereum siete

Podobne ako pri Bitcoine, škálovanie je pomerne veľkým problémom pri väčšine blockchainových sietí. Zatiaľ čo Ethereum vývojári sa snažia implementovať škálovacie techniky aj priamo v hlavnom blockchaine Etherea, paralelne sa pracuje aj na druhej vrstve Ethereum siete, ktorá by umožňovala sprocesovať tisícky transakcií za sekundu. V súčasnosti je hlavný blockchain Etherea schopný spracovať niekoľko desiatok transakcií za sekundu. Berúc do úvahy cieľ Etherea stať sa globálnym počítačom pre decentralizované aplikácie, toto číslo je príliš malé. V rámci druhej vrstvy Etherea sa v súčasnosti paralelne pracuje na niekoľkých technologických riešeniach. Stavové kanály (z angl. State Channels) sa svojím dizajnom podobajú na platobné kanály v Lightning sieti pri Bitcoine, ale na rozdiel od nich nie sú obmedzené len na prenos hodnoty, ale aj stavu programu. Prvou a snáď najznámejšou implementáciou stavových kanálov na Ethereu bol projekt s názvom Raiden Network[59]. Raiden, podobne ako Lightning, umožňuje vytvárať stavové kanály mimo hlavného blockchainu. Na rozdiel od Lightningu, pri kanáloch v Raidenie sa zatiaľ dajú transakcie posielať len jedným smerom, hoci toto obmedzenie by sa malo v budúcnosti zrušiť. Ďalším príkladom implementácie stavových kanálov je napríklad projekt Connext[60]. Hlavným rozdielom týchto dvoch implementácií je, že Raiden Network má svoj vlastný token, zatiaľ čo Connect funguje bez tokenu.

[59] Viac informácií na: https://raiden.network/

[60] Viac informácií na: https://connext.network/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Ethereum blockchain dovoľuje podobne ako pri Bitcoine vytváranie vedľajších blockchainov, tzv. sidechainy, ktoré sú napojené na hlavný blockchain. Tie fungujú na podobných princípoch ako v Bitcoine už spomínaný Liquid projekt, a preto ich nebudeme hlbšie analyzovať. Avšak, ďalšou dôležitou škálovacou technológiou v rámci Ethereum ekosystému je Plasma[61]. V porovnaní so sidechainom či stavovými kanálmi sa jedná o novšiu technológiu, ktorá sa delí na tri ďalšie podmnožiny – Plasma MVP, Plasma Cash a Plasma Debit. Plasma MVP využíva podobne ako Bitcoin UTXO model a spolieha sa na pomerne centralizovanú architektúru. Plasma Cash využíva model, v ktorom každý depozit do siete je reprezentovaný vo forme unikátnych NFT (z angl. Non-Fungible Tokens) tokenov. Plasma Debit je podobná Plasme MVP avšak vytvára pre každý token separátny platobný kanál. Všetky vyššie uvedené koncepty Plasmy sú pomerne nové a málo preskúmané technológie, ktoré sa začnú viac využívať pravdepodobne až v budúcnosti. Každé z riešení ma vlastné výhody a nevýhody. Pri stavových kanáloch je napríklad zatiaľ nutné, aby každý užívateľ bol online aby si mohol viesť záznamy o stave kanálov lokálne. Táto nevýhoda je eliminovaná pri sidechainoch, no je pravdepodobné, že tomu v budúcnosti tak bude aj pri stavových kanáloch.

[61] Viac informácií na: https://www.learnplasma.org/en/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

3. KRYPTOSYSTÉMY: TECHNOLOGICKÁ A FILOZOFICKÁ ZMENA PARADIGMY

Kryptosystémy, kryptomeny či iné šifrovacie systémy so sebou priniesli aj výraznú paradigmatickú zmenu, ktorá sa neskôr prejavila aj v dizajnových aspektoch týchto technológií. Počiatok tejto novej filozofickej paradigmy spájame s publikáciou s názvom „New Directions in Cryptogprahy“[62] od významných matematikov a vedcov Whitfielda Diffieho a Martina Hellmana z roku 1976. Do tohto dátumu bola kryptografia prevažne doménou štátnych či armádnych organizácií, v ktorých sa koncentrovala výrazná väčšina výskumníkov, vedcov a inžinierov zaoberajúcich sa kryptografiou. Vyššie spomínaná publikácia znamenala obrovský míľnik nielen preto, že sa považuje za objavenie asymetrickej kryptografie, ale hlavne preto, že to bol moment, kedy verejnosť mala po prvý krát v histórii prístup k skutočne silnému šifrovaniu, ktoré nevedeli prelomiť ani bezpečnostné zložky. Diffie a Hellman chceli touto publikáciou aktívne podporiť rozvoj, výskum a šírenie kryptografie naprieč širokou verejnosťou, na čo odkazujú aj v závere svojej práce:

„Zručnosť v produkcii kryptoanalýzy bola vždy doménou profesionálov, ale inovácie v oblasti dizajnu nových kryptografických systémov často pochádzajú od amatérov. Thomas Jefferson, amatérsky nadšenec kryptografie, vynašiel systém, ktorý sa stále používal počas druhej svetovej vojny, a snáď najvýznamnejší kryptografický systém dvadsiateho storočia, rotorový stroj, bol vynájdený simultánne a separátne štyrmi rôznymi ľuďmi, ktorí bolí všetci amatéri. Dúfame, že táto práca inšpiruje ostatných k práci v tomto fascinujúcom odbore, v ktorom participácia bola odradzovaná takmer úplným monopolom vlády.“

[62] Viac informácií na: https://ee.stanford.edu/~hellman/publications/24.pdf

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Trvalo niekoľko rokov, kým idea asymetrickej kryptografie dostala formu konkrétnych aplikovaných technológií. Osemdesiate roky boli v znamení rozvoja týchto myšlienok, no väčšina z nich stále na papieri. David Chaum, ideový otec digitálnych peňazí, vyprodukoval v tomto období obrovské množstvo vedeckých štúdií v oblasti kryptografie, ktoré neskôr inšpirovali celé hnutie digitálneho aktivizmu bojujúceho za slobodu a anonymitu v digitálnom prostredí. Jeho snáď najvýznamnejšími prácami z tohto obdobia sú „Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms“[63], či „Blind Signatures for Untraceable Payments“[64]. Sám David Chaum aplikoval tieto teoretické koncepty po prvý krát v praxi až začiatkom deväťdesiatych rokov, keď založil firmu DigiCash. V tomto období sa rozmach šifrovacích technológií výrazne zrýchlil a jedným z dôležitých míľnikov tejto doby bolo zverejnenie šifrovacieho softvéru PGP[65] v roku 1991. Práve zverejnenie PGP odštartovalo v USA mohutnú spoločenskú diskusiu, a neskôr aj sériu súdnych sporov, ktoré sa týkali práve šírenia kryptografických nástrojov. Kryptografia a šifrovanie boli v tej dobe klasifikované ako armádne zbrane a teda podliehali reštrikciám, týkajúcim sa šírenia či exportu do zahraničia. V dobe, kedy sa internet dostával do povedomia širokých más, bolo takmer nemožné uplatniť takéto reštrikcie v prípade softvéru, akým bol aj PGP. Snahy americkej vlády o kontrolu šírenia týchto informácií a uplatnenie reštrikcií na šifrovacie softvéry či algoritmy vošli do dejín pod označením „Crypto Wars“[66]. Rast internetu, ako aj e-commerce odvetvia však časom ukázal, že v takejto situácii nebolo možné reálne vymôcť tieto zákony. Aplikovanie šifrovacích algoritmov bolo čím ďalej rozšírenejšie a prinášalo benefity a zvýšenie bezpečnosti a ochrany súkromia naprieč odvetviami. Snáď najvýznamnejšou manifestáciou tohto trendu bolo

---

[63] Viac informácií na: https://nakamotoinstitute.org/static/docs/untraceable-electronic-mail.pdf

[64] Viac informácií na: https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF

[65] Viac informácií na: https://www.openpgp.org/

[66] Viac informácií na: https://en.wikipedia.org/wiki/Crypto_Wars

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

prevzatie kryptografie s verejným kľúčom v prostredí internetových prehliadačov, konkrétne v prehliadači Netscape, ktorý začal používať technológiu SSL ako metódu ochrany proti podvodom s kreditnými kartami. Rovnako sa v tomto období začali objavovať viac či menej formálne skupiny aktivistov za súkromie a slobodu v digitálnom priestore, ako napr. Electronic Frontier Foundation (EFF)[67] či Cypherpunks[68]. Vyvrcholením Crypto Wars bolo oznámenie Clintonovej administratívy o plánoch implementovať tzv. Clipper čip do mobilných zariadení či počítačov. Čip bol vyvinutý a propagovaný NSA, a jeho hlavnou vlastnosťou bolo, že každý čip bol unikátny a obsahoval v sebe špeciálny kľúč, ktorý bol nasadený priamo do čipu a umožňoval americkej vláde resp. jej tajným zložkám získať prístup ku komunikácii z akéhokoľvek zariadenia, ktoré takýto čip obsahovalo. Americká vláda oznámila tento plán v roku 1993 s tvrdením, že je to nevyhnutný krok pre zabezpečenie národnej bezpečnosti. Tento návrh okamžite spôsobil vlnu nevôle zo strany aktivistov a organizácií ako EFF či Electronic Privacy Information Center, ktoré začali burcovať spoločnosť. Verejnosť kritizovala čip aj kvôli tomu, že bol klasifikovaný za tajný a teda neprešiel auditom odbornej verejnosti a teda bol považovaný potenciálne za napadnuteľný. Ďalším argumentom bol fakt, že americká vláda mohla vymáhať implementáciu tohto čipu len pri amerických spoločnostiach, ktoré by tak mohli do budúcnosti stratiť konkurenčnú výhodu oproti zahraničným firmám, ktoré by čip nemuseli implementovať. Šírenie mobilných zariadení od firiem, ktoré nepochádzajú z USA by rovnako malo za následok, že by americká vláda v konečnom dôsledku nedosiahla svoj deklarovaný cieľ. Na stranu aktivistov sa časom pridali aj niektoré korporácie či osobnosti verejného života, čo viedlo k tomu, že v roku 1996 americká vláda svoj plán stiahla. Debata sa oživila opäť potom, čo bývalý kontraktor americkej CIA Edward Snowden zverejnil niektoré špionážne praktiky amerických tajných služieb v roku 2013. Firmy Apple a Google následne na

[67]Viac informácií na: https://www.eff.org/

[68]Viac informácií na: https://en.wikipedia.org/wiki/Cypherpunk

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

to reagovali oznámením o implementovaní šifrovacích algoritmov do ich zariadení, ktoré by neumožnili sprístupniť informácie z ich zariadení ani na príkaz americkej vlády. Do určitej miery však táto téma ostáva otvorená vo viacerých krajinách, ktoré uvažujú o obmedzení používania šifrovacích nástrojov v širokej verejnosti.

Cypherpunks

Hnutie Cypherpunks bolo neformálne zoskupenie aktivistov, inžinierov, matematikov, a programátorov, ktoré vzniklo koncom roka 1992. Zakladajúcimi členmi hnutia boli John Gilmore, Timothy May a Eric Hughes, ktorí začali v tej dobe organizovať neformálne stretnutia pre nadšencov technológií na mesačnej báze v San Franciscu. Názov hnutia vznikol kombináciou anglického slova „cipher" a „cyberpunk"[69]. Väčšina diskusií v rámci hnutia prebiehala následne prostredníctvom emailového zoznamu, ktorého záznamy sú dostupné na serveri www.cryptoanarchy.wiki. Záznamy obsahujú celú komunikáciu za viac ako 10 rokov hnutia. Do diskusií sa zapojilo niekoľko známych osobností vrátane významného kryptografa Brucea Schneiera či zakladateľa WikiLeaks Juliana Assangea. Väčšina účastníkov diskusií sa identifikovala s ideologickými hnutiami libertarianizmu, krypto-anarchie či Rakúskej ekonomickej školy. Viacerí významní programátori či tvorcovia konceptov digitálnych peňazí ako Wei Dai, Nick Szabo alebo Hal Finney pravidelne participovali na diskusiách, a je pravdepodobné, že tak robil aj tvorca Bitcoinu Satoshi Nakamoto. Hlavne ciele a hodnoty hnutia boli predstavené v ikonickom dokumente „A Cypherpunk's Manifesto"[70], ktorého autorom bol zakladateľ hnutia Erich Hughes. Hughes v ňom opisuje nevyhnutnosť ochrany súkromia v otvorenej spoločnosti v nastávajúcej elektronickej dobe, ako aj dôležitosť

[69] „Cipher" znamená šifra, „cyberpunk" je žáner v science fiction literatúre

[70] Viac informácií na: https://www.activism.net/cypherpunk/manifesto.html

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

decentralizovanej architektúry systémov, ktoré sú imúnne voči štátnej cenzúre. Dôraz na decentralizáciu sa postupom času zvyšoval najmä potom, čo americká vláda sprísnila v roku 2006 regulácie firiem, ktoré poskytovali služby digitálnych mien, tak ako napríklad E-gold či Liberty Reserves. Viacerí predstavitelia týchto firiem boli trestne stíhaní a perzekuovaní. Vymáhanie prísnych regulácií pre finančné inštitúcie bolo pri týchto firmách pomerne jednoduché, nakoľko každá mala nejaký centrálny server, sídlo a vedenie či manažment. Prvé pokusy o decentralizované digitálne meny boli v podobe projektov ako B-money či Bitgold.

B-money a Bitgold

B-money[71] ako koncept bol pôvodne navrhnutý v roku 1998 vývojárom a kryptografom Weiom Daiom. Dai navrhol dva protokoly, ktoré fungovali kompletne na princípe distribuovanej P2P sieti, využívajúc identifikačný systém založený na asymetrickej kryptografii. B-money sa dá považovať za technologického predchodcu Bitcoinu pre viacero podobných čŕt, vrátane konceptu distribuovanej účtovnej knihy. Dai taktiež prišiel s nápadom zakotviť spotrebu elektrickej energie ako funkciu monetárnej zásoby digitálnej meny. V jeho koncepte však navrhol zachovať proporčnosť medzi mierou inflácie meny a nákladmi na elektrinu spotrebovanú na výpočty hašov. Toto bolo však problematické, pretože by to znamenalo že ťažiari musia súhlasiť s jednotnou cenou pri nákladoch na výpočty, čo je však v realite takmer nemožné, nakoľko náklady na elektrinu, a teda výpočty, sa líšia naprieč krajinami. Dai vo svojom návrhu konceptu neskrýval fascinovanosť konceptom krypto-anarchie od Timothy Maya. V hnutí Cypherpunks nebol jediný. Sympatie k tomuto konceptu neskrýval ani tvorca ďalšieho významného konceptu BitGold, Nick Szabo.

[71] Viac informácií na: https://nakamotoinstitute.org/b-money/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Bitgold[72] vznikol ako koncept takmer v rovnakom období ako B-money, avšak bol publikovaný až v roku 2005. Nick Szabo, podobne ako Wei Dai, bol viacerými členmi hnutia označovaný za Satoshiho Nakamota, no obaja to popreli. Tieto domnienky vznikli práve pre podobnosť oboch konceptov s Bitcoinom. BitGold taktiež fungoval ako digitálna mena na báze distribuovanej siete, bez akejkoľvek centrálnej autority. Szabo v názve projektu zachytil svoje sympatie k zlatu, ktoré nielen on ale aj viacerí prívrženci Cypherpunks či Rakúskej ekonomickej školy pokladali za kvalitatívne lepšiu formu peňazí v porovnaní s klasickými FIAT peniazmi, akými sú národné meny ako dolár či euro.

Ďalšou výraznou črtou a paradigmou vo väčšine kryptosystémov je ich otvorenosť a transparentnosť. Drvivá väčšina kryptomien či blockchainových projektov fungujú na báze open-source, teda ich zdrojový kód je prístupný verejnosti. Toto má niekoľko implikácií. V prvom rade to eliminuje nevyhnutnosť dôverovať autorom kódu, resp. aplikácie, nakoľko presné znenie a fungovanie kódu si môže overiť každý nezávisle. Druhou, nemenej dôležitou implikáciou je, že kód sprístupnený širokej či odbornej verejnosti ma väčšiu šancu byť bezpečný a neobsahovať chyby. Zdrojové kódy aplikácií častokrát prechádzajú bezpečnostnou previerkou zo strany nezávislého auditu, no ten nemusí stačiť. V samotnom zdrojovom kóde Bitcoinu sa našli chyby až po niekoľkých rokoch. Bitcoin je pritom svojím syntaxom, ako aj funkcionalitou programovacieho jazyka pomerne jednoduchší a menej komplexný než väčšina blockchainových sietí. Komplexita kódu je pri platformách na smart kontrakty neporovnateľne vyššia. V histórii Etherea sa udialo niekoľko incidentov, kedy chyba[73] v kóde spôsobila škody za niekoľko miliónov dolárov. Preto je nesmierne dôležité, aby bol kód prístupný verejnosti a teda auditovateľný čo najväčším počtom ľudí.

---

[72] Viac informácií na: https://nakamotoinstitute.org/bit-gold/

[73] Viac informácií na: https://hackernoon.com/how-the-170-million-ethereum-bug-could-have-been-prevented-819053c3b2cb

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tokenizácia

Jedným z dôvodov, prečo tak markantne vzrástol záujem o kryptosystémy či kryptomeny, bola najmä vlna ošiaľu spôsobená ICOs (z angl. Initial Coin Offerings) v roku 2017. Jedná sa o primárnu emisiu digitálnych tokenov, ktoré typicky využívajú infraštruktúru niektorej z blockchainových sietí, ako aj funkcionalitu smart kontraktov. Prvé ICO sa udialo v roku 2013 v rámci projektu Mastercoin[74]. Mastercoin bol dizajnovaný ako vrstva nad Bitcoinom, ktorá poskytovala rozšírenú funkcionalitu v rámci Bitcoin protokolu. Tvorcovia projektu sa rozhodli tokenizovať tento protokol a ponúknuť komunite nadšencov možnosť finančne podporiť tento projekt výmenou za novovzniknuté tokeny Mastercoin protokolu. Časť tokenov bola rezervovaná pre vývojársky tím, aby bola zabezpečená ich motivácia podieľať sa dlhodobo na vývoji protokolu. Hlavnou ideou za týmto nastavením bola myšlienka, že ako sa bude postupne protokol vyvíjať a zvyšovať svoju funkcionalitu, bude sa zvyšovať záujem po protokole samotnom a teda aj po tokenoch, ktoré sú integrálnou súčasťou protokolu. Toto by sa malo odraziť na rastúcej cene tokenu, a slúžiť ako odmena a kompenzácia pre komunitu za dôveru v projekt v rannom období vývoja. Vývojári Mastercoin projektu boli takýmto spôsobom schopní vyzbierať prostriedky v hodnote viac než pol milióna dolárov. Celý obnos bol vyzbieraný v Bitcoinoch, a krátko na to, ako začala narastať cena Bitcoinov, táto suma sa viac než zdesaťnásobila. Tento fenomén začal priťahovať pozornosť viacerých projektov, ktoré vyvíjali aplikácie v blockchain odvetví. Ethereum v roku 2014 vyzbieralo takýmto spôsobom viac než 16 miliónov dolárov[75] a len potvrdilo vzrastajúci trend ICOs. ICOs sa stali revolučným fenoménom práve vďaka tomu, že umožnili startupom a začínajúcim projektom pomerne jednoducho vyzbierať finančné prostriedky bez toho aby museli predávať podiel v spoločnosti,

[74] Viac informácií na: https://newconomy.media/news/the-origin-story-of-the-initial-coin-offering-ico-token-sale-history

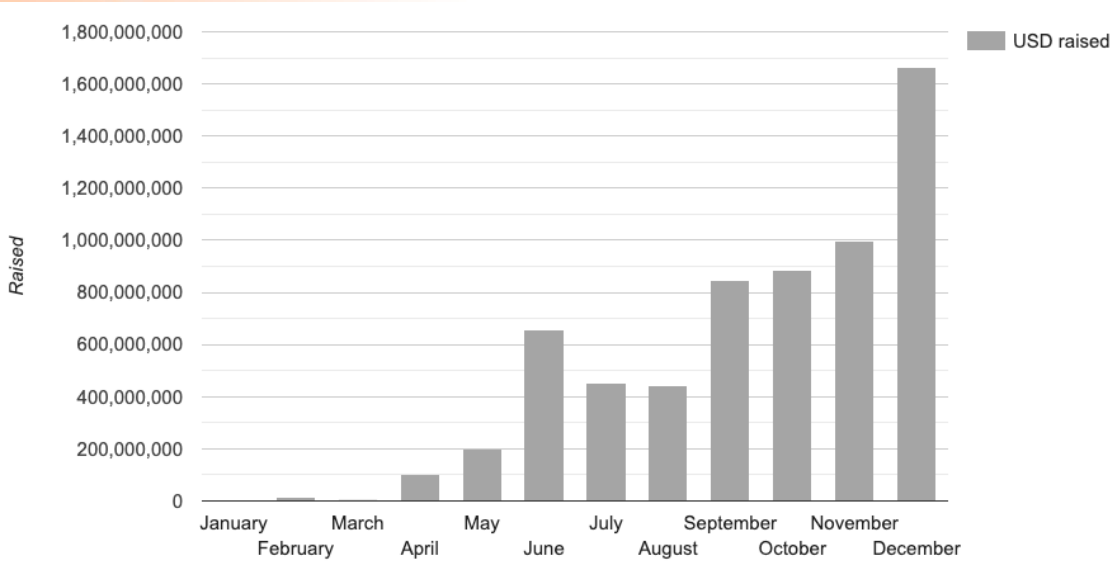
[75] Viac informácií na: https://icodrops.com/ethereum/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

či dokonca bez toho aby nejakú spoločnosť, resp. právnu entitu vôbec mali. Neprekvapivo, toto bola lákavá predstava pre mnoho startupov a ICO nabrali v roku 2017 extrémne na popularite, ako vidieť na grafe nižšie.

Obrázok 7: Množstvo vyzbieraných prostriedkov prostredníctvom ICO v roku 2017



Zdroj: www.icodata.io

ICO v roku 2017 začali výrazne konkurovať fondom rizikového kapitálu, špecializujúcim sa na investície do startupov v rannom štádiu. Jedným z dôvodov, prečo sa stali ICO tak populárne bol fakt, že na rozdiel od klasického regulovaného trhu s rizikovým kapitálom, ICO boli dostupné komukoľvek bez ohľadu na vek, status či krajinu. Ašpirujúci investor nemusel žiadnym spôsobom doložiť svoju identitu, či preukazovať dostatočnú solventnosť. Nakoľko transfer prostriedkov prebiehal v kryptomenách, identita investorov mohla byť utajená. ICO teda priniesli výraznú zmenu paradigmy, demokratizáciu trhu s rizikovým kapitálom tým, že zrovnoprávnili investorov všetkých kategórií, najmä tých retailových. Tento trend sa však neudržal príliš dlho, nakoľko objem vyzbieraných prostriedkov prostredníctvom ICO sa rádovo znižuje v čase. Zatiaľ čo v roku 2017 či 2018 to boli miliardy dolárov, v roku 2019 sú to už „len“

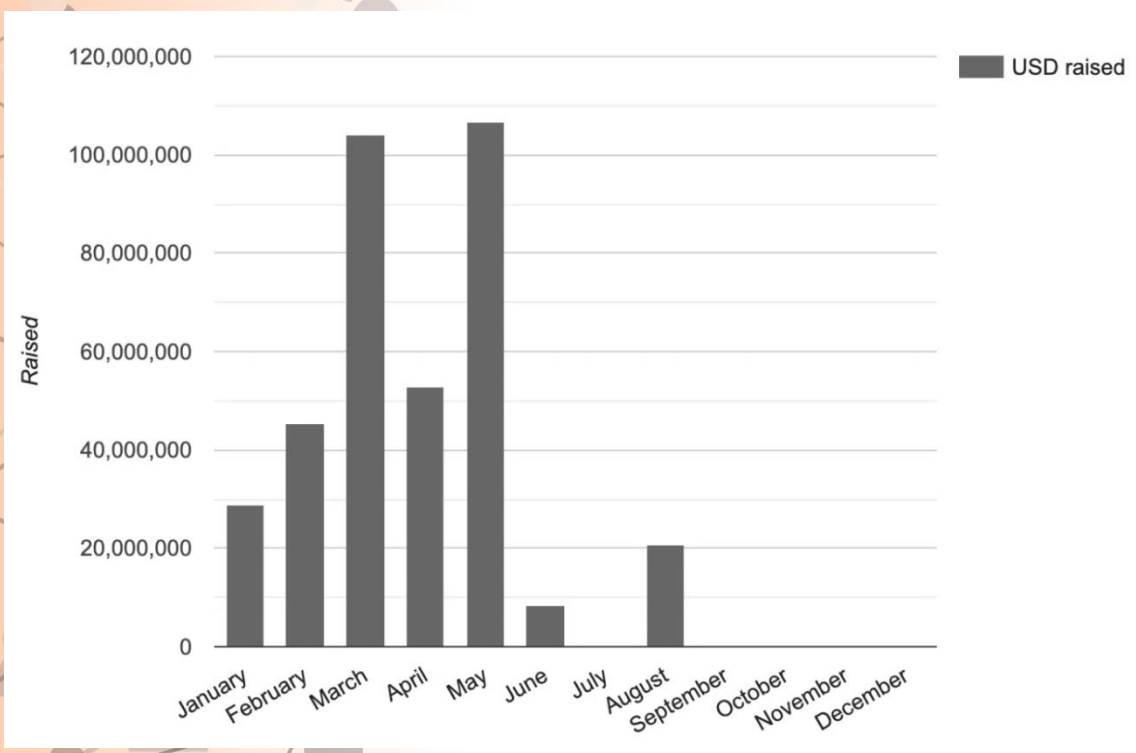
Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

stovky miliónov amerických dolárov. Jedným z faktorov, ktoré prispeli k tejto situácii, je rozmach podvodných ICO, ktoré využili anonymnú povahu týchto technológií na vlastné obohatenie. Viaceré zdroje uvádzajú, že hlavne v roku 2017 sa na vlne ICO zviezloiekoľko projektov, ktoré využili možnosť pomerne jednoduchého získania značných finančných prostriedkov na projekty, ktoré nikdy neboli spustené či zrealizované.

Jedným z dôvodov pre pokles objemu finančných tokov v rámci ICO je častokrát nešpecifikovaný právny status tokenov, ktoré sú predmetom investície, keďže mnohokrát nie je jasné či dané tokeny spadajú pod reguláciu cenných papierov. Tento problém je posilnený aj tým, že ICO fungujú ako globálny fenomén, a regulácie týkajúce sa cenných papierov sa líšia naprieč krajinami. Zatiaľ čo pri finančných tokoch v prostredí bankového sektoru sa dajú tieto roky pomerne jednoduchšie dohľadať a regulovať, pri kryptomenových aktívach to je o niečo ťažšie, miestami až nemožné. Táto situácia mala za následok však rozvoj nového fenoménu a tým sú STO (Security Token Offerings, voľne preložené ako ponuka tokenov reprezentujúcich cenné papiere). Tokenizácia akýchkoľvek aktív sa stala populárnym trendom hlavne pre výhody, ktoré by mala priniesť:

Obrázok 8: Množstvo vyzbieraných prostriedkov prostredníctvom ICO v roku 2019



Zdroj: www.icodata.io

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Nonstop obchodovateľné aktíva – Z povahy blockchain technológii ako distribuovanej účtovnej knihy, ktorá sa aktualizuje v reálnom čase naprieč viacerými servermi či lokáciami vyplýva, že redukuje čas na rekonciliáciu databáz jednotlivých entít a teda znižuje technické nároky na obchodovanie aktív bez časových obmedzení. Zatiaľ čo pri kryptomenách je takéto obchodovanie úplne bežné, pri cenných papieroch, komoditách či akciách tomu tak nie je. Aktíva na blockchaine by mali byť teda ľahšie obchodovateľné.

Frakčné vlastníctvo – Jednou z často proklamovaných výhod tokenizácie býva možnosť frakčného vlastníctve aktív. Tento trend sa v blockchaine javí byť na vzostupe hlavne na trhu s realitami[76] či umeleckými dielami[77]. Možnosť vlastniť len malú časť reálneho diela či budovy umožňuje, aby sa do investície zapojili aj investori, ktorí by nemali dostatočné množstvo prostriedkov na celú investíciu. To má za následok masívne zväčšenie množiny potenciálnych investorov, a teda v teórii aj zvýšenie likvidity tokenizovaných aktív.

Zvýšenie efektivity a transparentnosti obchodovania – Aj vzhľadom na vyššie uvedené dôvody je logické, že tokenizácia aktív zvyšuje efektivitu obchodovania a teda aj alokácie zdrojov. Najväčším prínosom z globálneho hľadiska je však zvýšenie transparentnosti pri obchodovaní. Vzhľadom na technologické vlastnosti (verejného) blockchainu, všetky transakcie sú viditeľné a verifikovateľné každým, čo výrazne znižuje pravdepodobnosť podvodov či nekalých aktivít.

Nižšie operatívne náklady – Jednou z obrovských výhod verejných blockchainov, teda mohutných autonómnych sietí, ktoré sú udržiavané tisíckami serverov po celom svete je, že ich môže ktokoľvek využívať bez toho, aby sa musel zaoberať udržiavaním siete či iným interným systémom. Aktíva tým pádom môžu byť obchodované prostredníctvom systému,

[76]Viac informácií na: https://thetokenist.io/assetblock-to-tokenize-60-million-worth-of-real-estate-on-algorand/

[77]Viac informácií na: https://www.blockchainappfactory.com/art-tokenization

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ktorý nemá žiadneho admina či správcu. Tento fakt značne znižuje náklady na údržbu IT systémov, nakoľko blockchainová sieť bude fungovať bez ohľadu na to, či sa dané aktíva na ňom budú obchodovať alebo nie.

Instantné prevody – Dizajnovou vlastnosťou väčšiny blockchianov je takmer okamžitá rekonciliácia a teda veľmi rýchle prevody aktív. Presný čas trvania prevodov, resp. ich sfinalizovania, sa líši v závislosti od daného blockchainu, v akomkoľvek prípade je proces niekoľko násobne kratší v porovnaní so súčasnými systémami.

Automatické vynucovanie pravidiel a regulácií – Väčšina blockchainov poskytuje funkcionalitu tzv. smart kontraktov. Smart kontrakt je v princípe softvér, ktorý automaticky vynucuje biznis podmienky a logiku, ktorá sa doňho naprogramuje. Táto definícia je veľmi podobná klasickým softvérom, no špecifikom smart kontraktov je, že tým, že fungujú na niektorej z blockchain sietí, sú spustené na tisíckach rôznych serverov zároveň. To má za následok, že je veľmi ťažké, či až nemožné zabrániť tomu, aby sa kód v nich vykonal. Zároveň platí, že sa do smart kontraktov dá naprogramovať biznis logika a reštrikcie súvisiace s identitou, solventnosťou či krajinou pôvodu investorov. Týmto spôsobom sa dajú výrazne znížiť náklady na vynucovanie regulácií a pravidiel vo finančnom sektore.

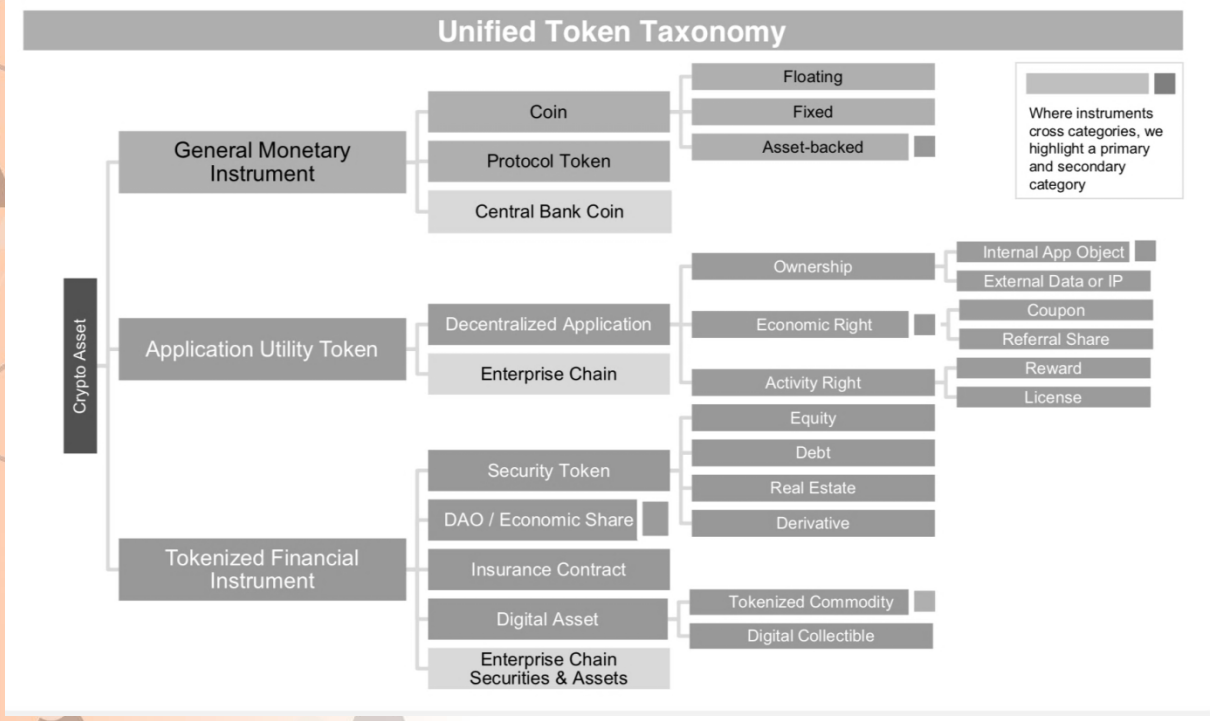
Vyššia likvidita – Všetky vyššie uvedené body môžu potenciálne výrazne zjednodušiť prístup investorov k aktívam a zároveň vytvoriť trh globálne obchodovateľných aktív. Je veľmi pravdepodobné, že toto by v konečnom dôsledku viedlo k zvýšeniu likvidity aktív, nakoľko by boli dostupnejšie pre investorov.

Okrem tokenizácie rôznych druhov aktív, ktoré náš právny poriadok pozná, je nutné dodať, že tokenizácia ako aj kryptomeny ako také so sebou priniesli nový druh hybridných aktív. Svojou povahou a funkcionalitou sa môžu zaradiť do viacerých kategórií zároveň. Regulátori na celom svete majú problém so správnou kategorizáciou týchto aktív a následným uplatnením patričných regulácií. Z tohto dôvodu vzniklo niekoľko pokusov o taxonomické delenie a popis týchto aktív v závislosti podľa ich funkcionality.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Obrázok 9: Kategórie tokenov
Zdroj: Autonomous NEXT



Zachytiť všetky technické detaily krypto aktív komplexne je pomerne náročné. Snáď najdôležitejším faktorom pri kategorizácií krypto aktív je to, či spadajú pod reguláciu cenných papierov. Ak áno, spadajú pod STO a musia spĺňať striktnejšie pravidlá ohľadom identifikácie investorov, ako aj pravidlá súvisiace s obchodovaním týchto aktív. Napriek upadajúcemu záujmu o ICO ako také, dá sa domnievať, že tento fenomén naďalej ostane ako relevantná alternatíva financovania malých a stredných podnikov aj do budúcna. Napriek tomu, že ICO zdieľajú určitú podobnosť s IPO, ako aj crowdfundingom, líšia sa v niekoľkých vlastnostiach, ktoré sú zhrnuté v tabuľke nižšie.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tabuľka 4: Porovnanie IPO vs. ICO

Aspekt	IPO	ICO
Typ financovania	- Rizikový kapitál - Po sérii D	- Rizikový kapitál - V rannom štádiu
Typ podniku	- Zabehnutý biznis-model - História a reputácia - Všetky odvetvia	- Ranné štádium - Bez histórie - Technologické firmy
Regulácie	- Jasne dané pravidlá	- Nejasná forma regulácie
Náklady	- 3-7 % z vyzbieranej sumy	- cca. 3 % zo sumy
Veľkosť vyzbieraných prostriedkov	- Väčšie sumy (v desiatkach miliónov)	- Menšie sumy (v miliónoch)
Rýchlosť uskutočnenia	- 0,5 – 1 rok príprav	- 2 - 6 mesiacov príprav
Investori	- Akreditovaní/inštitucionálni	- Bez obmedzení
Práva pre investorov	- Podiel vo firme - Dividendy - Hlasovacie práva	- Bez podielu - Možnosť hlasovania - Zvýhodnenie pri využívaní služby

Zdroj: icodata.io

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

4. POTENCIÁLNE VYUŽITIE KRYPTOSYSTÉMOV V SÚKROMNOM SEKTORE

Kryptosystémy, kryptomeny či blockchain ako technológia majú potenciálne široké využitie naprieč rôznymi sektormi a odvetviami. Blockchain sa dá z princípu považovať za typ distribuovanej databázy, a keďže všetky dnešné webové či mobilné technológie využívajú nejaký typ databázy, v teórii sa dá blockchain využiť skutočne pri mnohých aplikáciách. Avšak, napriek tomu sa určite na veľa aplikácií nehodí. Z povahy decentralizovanej infraštruktúry blockchainu má najväčší zmysel využiť ho pri aplikáciách, kedy je decentralizácia z nejakého dôvodu skutočne žiaduca. V tejto kapitole analyzujeme potenciálne využitia blockchainu naprieč rôznymi odvetviami.

4.1. Kryptomeny ako platobný nástroj

Kryptomeny už vo svojom názve zachytávajú snáď ich najzrejmejšie využitie, a to ako alternatívne peniaze, či platobné nástroje. Medzi samotnými vývojármi či prívržencami kryptomien panujú nezhody o tom čo vlastne kryptomeny sú a na čo je ich najlepšie použiť. Odpoveď na túto otázku má zásadný vplyv na smerovanie a vývoj jednotlivých kryptomien. Asi najlepším príkladom, kedy nezhoda okolo tejto otázky viedla v rámci Bitcoin komunity k pálčivej debate, bol tzv. „hardfork“ siete, ktorý sa stal 1. augusta 2017, a viedol efektívne k vytvoreniu novej kryptomeny – Bitcoin Cash[78]. Jadrom sporu bola práve otázka, ako by sa mal Bitcoin do budúcna používať a či by mal konkurovať výkonom siete napríklad firmám, ktoré vydávajú platobné karty, ako Visa či Mastercard. Zatiaľ čo Bitcoinová sieť je schopná vykonať približne 7 transakcií za sekundu, Visa či Mastercard dokážu spracovať niekoľko desiatok tisíc. Takýto výkon je však veľmi obtiažne dosiahnuť na decentralizovanej sieti, akou

[78] Viac informácií na: https://www.bitcoincash.org/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

je Bitcoin. Navýšenie nárokov (a teda aj nákladov) na hardvér, nevyhnutný na participáciu v Bitcoinovej sieti, by malo za následok, že by bolo menej uzlov v sieti a menej ľudí by validovalo transakcie v Bitcoin sieti, čím by sa zvýšila centralizácia siete a tým pádom znížila bezpečnosť. Z toho dôvodu sa väčšina vývojárov Bitcoinu zhodne na tom, že Bitcoin by sa nemal snažiť konkurovať klasickým platobným nástrojom vo výkone, minimálne priamo v blockchaine, nakoľko jeho silné stránky sú niekde inde. Je teda veľmi pravdepodobné, že Bitcoin ostane na svojej hlavnej vrstve pomalší v porovnaní s inými platobnými prostriedkami aj do budúcna. Avšak, je rovnako pravdepodobné, že im bude konkurovať na vrstvách, ktoré sú postavené nad hlavným protokolom ako Lightning Network či RSK, ktoré zvládnu kapacitne spracovať rádovo stovky násobne viac. Každopádne, aj napriek relatívne nízkej transakčnej kapacite siete Bitcoinu sa táto kryptomena často využíva na retailové platby. Medzi hlavné benefity využívania a prijímania kryptomien na platby za tovary a služby z pohľadu predajcov patria:

Bezpečnosť platieb: Platobné karty sa často stávajú predmetom hackerských útokov či podvodov. Z toho dôvodu sa niektorí predajcovia bránia prijímaniu platobných kariet pri niektorých platbách, hlavne pri vyšších objemoch, nakoľko je možné takéto platby zvrátiť. Pri platbe kryptomenami je takéto riziko výrazne nižšie. Taktiež, pri platbe online, sú kryptomeny omnoho bezpečnejšie, nakoľko užívateľ nemusí do (potenciálne hacknutého) webového prehliadača vpisovať žiadne údaje, čo je obrovskou výhodou.

Žiadny transakčný limit: Pri kryptomenách neexistujú žiadne limity súvisiace s veľkosťou transakcie. Z toho dôvodu sú vhodnejšie aj na mikro transakcie. Pri Bitcoine sú transakčné poplatky pomerne dosť dynamické a menia sa v čase, avšak Bitcoinová nadstavba Lightning Network bola vytvorená presne za účelom mikro platieb.

Nižšie konverzné poplatky: Konverzné poplatky súvisiace s výmenou kryptomien za eurá či doláre sú často nižšie, ako poplatky účtované kartovými spoločnosťami Visa či Mastercard. Navyše, transakčné poplatky súvisiace priamo s blockchainovou platbou platí odosielateľ, teda

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

v tomto prípade kupujúci. Predajcovia môžu vďaka tomu znížiť ceny tovarov a služieb o výšku procesných poplatkov pri kartových platbách.

Nezvratnosť transakcií: Blockchainové transakcie, ako aj akékoľvek iné dáta, sú prakticky nemeniteľné (hlavne pri Bitcoine), a teda eliminujú riziko tzv. „chargebackov" a zvrátenia platieb. Samozrejme, stále treba brať do úvahy, že blockchainové platby považujeme za nemeniteľné až po nejakej dobe resp. počte konfirmácií, nakoľko v prvých sekundách po transakcii existuje šanca, že platba bude zvrátená napr. pri tzv. útoku dvojitej útraty (z angl. double-spending attack).

Oslovenie nových potenciálnych zákazníkov: Začať prijímať kryptomeny je pomerne jednoduché pre ktoréhokoľvek obchodníka, a obchodníci tak často môžu osloviť nadšencov kryptomien ako potenciálne nových zákazníkov. Servery ako Coinmap.org[79] sa špecializujú výhradne na mapovanie predajných miest, ktoré akceptujú kryptomeny, a teda samotný akt akceptovania kryptomien má často pozitívny marketingový efekt pre obchodníka.

4.2. Decentralizovaný finančný systém

Kryptomeny ako také sú len prvým krokom k vybudovaniu paralelného decentralizovaného finančného systému. Bitcoin či mnohé ďalšie kryptomeny slúžia primárne ako platobný systém, no ten sám o sebe nestačí na plnohodnotné fungovanie nezávislého finančného systému. Ten sa začal formovať až s rozvojom smart kontraktových platforiem, hlavne v rámci infraštruktúry Ethereum siete. Približne od roku 2016 sa začal formovať samostatný ekosystém, ktorý dostal označenie DeFi (z angl. Decentralsied Finance), a ktorý sa skladá zo stoviek až tisícok rôznych decentralizovaných aplikácií, ktoré operujú ako algoritmy

[79] Viac informácií na: https://coinmap.org/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

s otvoreným kódom na decentralizovaných blockchainoch, a ktoré často krát imitujú funkcionalitu tradičných finančných inštitúcií. Z povahy infraštruktúry, na ktorej fungujú, sú na rozdiel od klasických finančných inštitúcií maximálne transparentné a automatizované. Algoritmy vo forme smart kontraktov môžu plniť funkcie decentralizovaných búrz, poskytovateľov likvidity či poistenia, digitálnych trhovísk, stabilných kryptomien, platforiem na mikropôžičky a mnoho ďalšieho.

Maker DAO[80] je jeden z najprominentnejších projektov v rámci DeFi ekosystému a jedna z prvých decentralizovaných autonómnych organizácií (z angl. DAO). Maker DAO sa skladá z niekoľkých smart kontraktov, ktoré manažujú systém pôžičiek v stabilnej kryptomene Dai[81], ktorá je naviazaná na hodnotu dolára kompletne iba prostredníctvom algoritmov a trhového mechanizmu. Maker DAO ako aj Dai analyzujeme do detailov neskôr v rámci kapitoly, ktorá sa venuje príkladom využitia blockchainu v rámci privátneho sektora. Ďalšie projekty, ktoré spadajú do tejto kategórie, analyzujeme hlbšie v iných kapitolách, v ktorých sú relevantné. Digitálne trhoviská, ako aj anonymné kryptomeny, analyzujeme napríklad v kapitole, ktorá sa venuje šedej ekonomike, nakoľko je to najviac relevantné práve v súvislosti s touto témou.

4.3. Decentralizovaný internet – Web 3.0

Blockchain, decentralizované aplikácie, smart kontrakty a tokenizácia protokolov mali za následok, že ľudia, firmy a vývojári začali dizajnovať mnoho aplikácií novým spôsobom, tak aby užívatelia týchto aplikácií boli čo najmenej závislí na tretích stranách. Súčasná infraštruktúra internetu má za následok vznik centralizovaných dátových síl vo forme korporácií ako Facebook, Cloudflare, Google a podobne. Tieto silá sa často stávajú terčom hackerov, ktorí sa

[80] Viac informácií na: https://makerdao.com/en/

[81] Viac informácií na: https://coinmarketcap.com/currencies/dai/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

vďaka centralizovanej infraštruktúre pomerne ľahšie dostanú k cenným dátam, ktoré často zahŕňajú citlivé informácie o užívateľoch týchto aplikácií. Ďalší, nemenej vážny problém je, že samotné korporácie sa často dopustia zneužitia informácií, ktoré im ich užívatelia zveria. Škandály ako Cambridge Analytica[82] sú len špičkou ľadovca v obrovskom mori káuz posledných rokov, ktoré poukazujú na nedokonalú štruktúru súčasného internetu. Mohutné blockchainové siete ako Bitcoin či Ethereum môžu však byť použité ako globálne zdieľané protokoly, ktoré budú slúžiť ako podklad pre komunikáciu medzi rôznymi komponentmi webovej infraštruktúry. Transformácia webu z centralizovanej infraštruktúry na decentralizovanú dostala pomenovanie Web 3.0[83]. Zatiaľ čo Web 1.0 ponúkal pomerne jednoduchý statický obsah, ktorý ktokoľvek mohol tvoriť a konzumovať, Web 2.0 priniesol viacej interakcie medzi jednotlivými komponentmi, ktoré umožnili užívateľom kolaborovať v reálnom čase. Web 3.0 priniesol možnosť programovať priamo do aplikácií tokeny, ktoré reprezentujú rôzne typy aktív a umožňujú okamžitý prenos hodnoty natívne v prostredí internetovej infraštruktúry. Jednou z najväčších proklamovaných výhod Webu 3.0 je, že užívatelia získajú kontrolu nad svojimi dátami. Za najvýznamnejšie projekty v rámci Web 3.0 sú považované okrem Etherea aj platformy ako Polkadot[84] či Blockstack[85]. Polkadot je protokol, ktorý sa zameriava primárne na umožnenie vzájomnej komunikácie medzi rôznymi blockchainami. Blockstack prináša riešenie pre univerzálnu digitálnu identitu. V súčasnosti sa buduje niekoľko na sebe závislých vrstiev v rámci infraštruktúry Webu 3.0, znázornených na tabuľke nižšie. V konečnom dôsledku by mali mať pre užívateľov niekoľko výrazných benefitov oproti súčasnému stavu. Samotný fakt, že užívatelia budú mať väčšiu moc nad svojimi dátami

[82]Viac informácií na: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[83]Viac informácií na: https://blockgeeks.com/guides/web-3-0/

[84] Viac informácií na: https://polkadot.network/

[85] Viac informácií na: https://blockstack.org/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

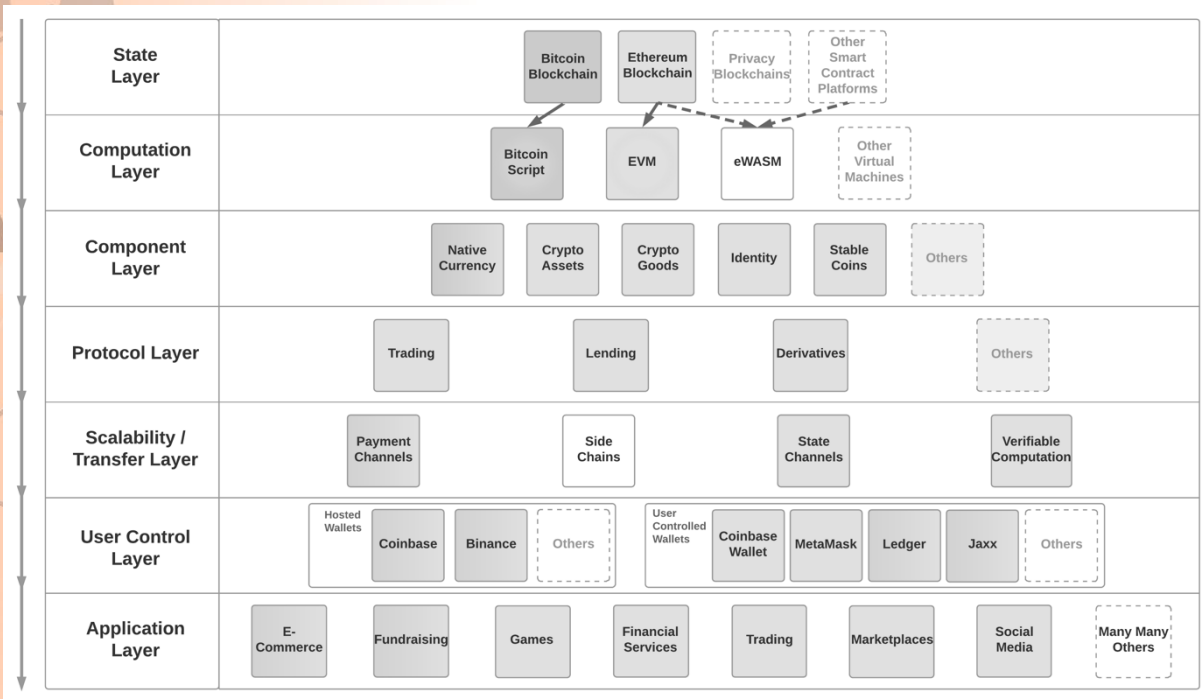
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

znamená podkopanie dominantného postavenia obrovských dátových síl v podobe korporácií, ktoré majú postavené svoj biznis model na monetizácii dát užívateľov. Ekonomická hodnota derivovaná z týchto dát by mala byť tak rovnomernejšie distribuovaná smerom k tým, ktorí ju reálne produkujú. Toto by malo mať za následok rovnako aj zvýšenie prenositeľnosti dát, ktoré sú v súčasnosti uzamknuté v rámci jednotlivých aplikácií. Separácia dát od jednotlivých aplikácií a teda dosahu tretích strán na ne má za následok zvýšenie rezistencie voči cenzúre. Táto vlastnosť má veľké implikácie hlavne v krajinách s autoritatívnymi režimami. Avšak, prínos decentralizovanej infraštruktúry je významný najmä v oblasti zvýšenia bezpečnosti dát, nakoľko bude pre hackerov omnoho ťažšie dostať sa k dátam, ktoré sú distribuované na tisíckach serverov. Je pravdepodobné, že v rámci tejto novej infraštruktúry vzniknú rôzne komplementárne aplikácie, ktoré budú schopné plnohodnotne poskytovať funkcionalitu webových aplikácií, na akú sme zvyknutí. Takéto aplikácie zahŕňajú platformy na komunikáciu, dátové úložiská, riešenia zabezpečujúce identitu užívateľov, orákulá, decentralizovaný DNS (z angl. Domain Name System) systém a podobne.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Obrázok 10: Web 3.0



Zdroj: Coinbase Blog

4.4. Tokenizácia aktív

Ako sme načrtli vo štvrtej kapitole, blockchain ako globálna distribuovaná účtovná kniha priniesol možnosť tokenizovať v princípe akékoľvek aktíva. V rámci privátneho sektora je teda možné očakávať, že sa v budúcnosti dočkáme tokenizácie cenných papierov, umenia, nehnuteľností, derivátov, akcií, komodít a podobne. Avšak, tokenizácia umožňuje podnikateľom a biznisom tokenizovať ich služby aj prostredníctvom tzv. utility tokenov, ktoré zvyčajne nespadajú pod reguláciu cenných papierov, nakoľko nereprezentujú podiely v spoločnosti, ani nárok na podiel na zisku či obratoch spoločnosti. Takéto tokeny sa dajú najľahšie prirovnať k digitálnym tokenom reprezentujúcim určitý typ kreditu v rámci nejakej aplikácie. Na rozdiel od súčasného stavu, kedy si každý poskytovateľ služby, resp. aplikácie vedie záznamy o stave kreditu každého užívateľa samostatne, tokenizácia takéhoto druhu

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

aktív prostredníctvom globálnej spoločnej databázy by výrazne zjednodušila život ako užívateľom, tak aj obchodníkom. Navyše, jedným z veľkých benefitov tokenizácie týchto aktív by bola vyššia likvidita, ktorá by umožnila vzájomný obchod a výmenu týchto kreditov vo forme tokenov, čoho výsledkom by bola aj vyššia efektivita alokácie zdrojov.

4.5. Logistika a dodávateľské reťazce

Jedným z najpopulárnejších využití blockchainu v súkromnom sektore, mimo kryptomien, je využitie v logistike. Zavedenie distribuovanej databázy naprieč dodávateľskými reťazcami bude mať veľký prínos v zvýšení transparentnosti a dohľadateľnosti pôvodu tovarov. Blockchain ukazuje svoje výhody hlavne v dohľadaní pôvodu produktov, v znížení bremena a obtiažnosti administratívnych náležitostí, ako aj v automatizácii procesov. Zapisovanie údajov súvisiacich s výrobou či spracovaním produktov do distribuovanej databázy, ktorá sa v reálnom čase aktualizuje, má potenciál výrazne zrýchliť viaceré byrokratické procesy súvisiace s dokumentáciou týchto procesov. Takýto spôsob zapisovania údajov môže výrazne zjednodušiť možnosť dohľadania pôvodu tovarov nielen pre koncových zákazníkov, ale aj pre štátne autority. Snáď najväčšia potreba aplikácie takejto technológie je vnímaná v potravinárskom sektore, v ktorom je problém dvojitej kvality potravín v rôznych krajinách Európy vážnym problémom. Blockchain sa však môže implementovať naprieč dodávateľskými reťazcami v rôznych odvetviach, ktoré trpia podobnými problémami.

Problémy odvetvia, riešenie a výhody

Dodávateľské reťazce v rámci medzinárodného obchodu bojujú s podobnými problémami, dobrým príkladom je napríklad medzinárodná lodná doprava kde sú prítomne tri hlavné problémy:

- *Regulačné bludisko* - veľká rozmanitosť importného-exportného práva, colnej správy, procesov a regulácií v tranzitných i destinačných krajinách.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- *Nedostatok transparentnosti* – záznamy sú kompletné len pred ďalšou zastávkou karga a v prípade dodatočných otázok a problémov nastávajú prieťahy, ktoré výrazne zvyšujú dodacie lehoty.
- *Manuálny, neefektívny proces* – vypĺňanie papierových tlačív je zdĺhavé a náchylné na chyby, ktoré potom odďaľujú spracovanie dodávok a predlžujú celý proces. Importéri, exportéri, logistické a distribučné firmy, prevádzkovatelia cestnej prepravy a prístavov, prípadných veľkoskladov, ich banky a aj colné a iné štátne úrady sa teda stretávajú s následkami toho, že si vedú rozličné a separátne záznamy.

Implementácia blockchainu ako jediného zdroja „pravdy“, do ktorého majú prístup všetky časti v rámci celého reťazca, môže výrazne prispieť k zvýšeniu efektivity mnohých procesov, ktoré sú nevyhnutné na správne fungovanie reťazcov. Pri správnej implementácii blockchainu môžu mať všetky zúčastnené strany prístup v reálnom čase k všetkým relevantným údajom, súvisiacim so spracovaním či transportom výrobkov. Navyše v momente, keď sú tieto údaje aktualizované jednou zo zúčastnených strán, táto zmena sa okamžite upraví v záznamoch všetkých strán. Ak každá zo strán prevádzkuje vlastný uzol v rámci siete, tak má tieto dáta u seba a znižuje sa tak nevyhnutnosť dôverovať tretej strane, ktorá spravuje server s týmito dátami.

Blockchain tak môže poskytnúť vždy aktuálny a kompletný digitálny obraz pravdy a stimulovať prostredie k harmonizácií procesov. Docieľuje to základnými vlastnosťami distribuovaného systému v spojení s potrebami, ktoré plynú zo spomínaných troch kľúčových problémov:

Nemennosť záznamov – eliminácia zmien či spätného mazania alebo upravovania záznamov o produkcii, spracovaní alebo preprave výrobkov zaisťuje kompletnú históriu všetkých úkonov a udalostí spojených so životným cyklom produktov.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Jediný zdroj pravdy – jediná a vždy aktuálna verzia histórie udržiavaná celou sieťou eliminuje nevyhnutnosť konsolidácie záznamov jednotlivých účastníkov procesov a zároveň poskytuje možnosť auditu v reálnom čase a nie až *ex post* ako obvykle.

Kryptografické šifrovanie – rôzne implementácie blockchainových sietí poskytujú viacero kryptografických techník na dosiahnutie uchovania tajnosti informácií, ktoré sú predmetom napríklad obchodného tajomstva, aj v prostredí kompletne transparentnej zdieľanej databázy.

Smart kontrakty – blockchain platformy, ktoré podporujú smart kontrakty, umožňujú automatizáciu mnohých procesov a biznis operácií a zároveň dovoľujú automatické vymáhanie rôznych pravidiel, regulácií a zákonov pomocou softvérových nástrojov. Tieto vopred preddefinované algoritmy dokážu vypĺňať tlačivá autonómne a umožňujú tak výrazne znížiť náklady na administratívne úkony, keďže dokážu automatizovať narábanie s dátami pre kontinuálne spĺňanie požiadaviek štátnych, colných či iných autorít.

Implementácia blockchainu teda môže priniesť viacero výhod a benefitov, ktoré do veľkej miery súvisia s celkovou digitalizáciou procesov a eliminácie manuálneho vypĺňania nevyhnutných papierov a záznamov. Automatizácia procesov a garancia integrity dát sú však do veľkej miery závislé na eliminácii ľudského faktora z týchto procesov. Nevyhnutným predpokladom je napríklad využitie rôznych druhov čipov, ktoré komunikujú s blockchainom, či klasickou databázou. Zapisujú do nich dáta bez toho, aby tieto dáta mohli byť ovplyvnené ľudským faktorom. Zapisovanie dátových vstupov pomocou čipov však taktiež nemusí garantovať presnosť informácií, nakoľko aj tieto čipy sa dajú v rôznych podmienkach manipulovať. Napriek tomu, že Blockchain dokáže výrazne pomôcť pri eliminácii spätného upravovanie dát, nerieši žiadnym spôsobom presnosť vstupných dát. Maximálne využitie všetkých benefitov blockchainu súvisí teda do veľkej miery s rozvojom digitalizácie ako takej, automatizácie procesov a rozvojom IoT ako odvetvia.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

5. POTENCIÁLNE VYUŽITIE KRYPTOSYSTÉMOV VO VEREJNOM SEKTORE

Dnes sa čím ďalej tým viac kladie dôraz na presadzovanie informačných technológií vo verejnom sektore. Technológia blockchain sa aj preto často skloňuje v súvislosti s kryptomenami. Cieľom využitia informačných technológií vo verejnom sektore je znižovanie nákladov a zefektívňovanie komunikácie. To znamená napríklad zjednodušovanie komunikácie s podnikateľmi či občanmi, zjednodušovanie administrácie rôznych podkladov, či zvyšovanie transparentnosti verejného sektora. Potenciálne využitie blockchainu sa nachádza vo viacerých oblastiach, ktoré analyzujeme nižšie.

5.1. Transparentná platba daní a rôznych poplatkov

Tým, že blockchain presne zaznamenáva transakcie platieb a obsahuje ich celú históriu, tak sa prakticky hodí na každú oblasť, kde sa posielajú platby a je potrebné zachovať transparentnosť platieb. A to preto, že najmä vo verejnom sektore, či už na úrovni štátneho rozpočtu, alebo krajov, miest a obcí, sa evidujú rôzne poplatky a dane od fyzických a právnických osôb. Pomocou blockchainu by mohli byť platby vykonávané instantne a automatizovane. Zároveň by sa zachovala transparentnosť a prehľadnosť histórie platieb a presne by sa vedelo, ktorá fyzická či právnická osoba uhradila ten-ktorý poplatok alebo daň. Na strane druhej túto oblasť riešia aj klasické databázy, avšak neposkytujú až takú vysokú mieru dôveryhodnosti. Príkladom je mesto Rotterdam v Holandsku, kde turistické dane sú vyberané prostredníctvom inteligentných zmlúv. Zamestnancom mesta tým odpadajú niektoré povinnosti či činnosti spojené s turistickou daňou[86].

[86] ERNST & YOUNG. Štúdia možností a potenciálu technológie „blockchain“ pri zlepšovaní eGovernment riešení. Str. 57 [online]. Dostupné na internete: < https://www.vicepremier.gov.sk/wp-

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Vo Švajčiarsku v municipalite Chiasso v kantóne Ticino môžu obyvatelia platiť od roku 2018 dane a poplatky v Bitcoinoch. Najviac môžu naraz zaplatiť 250 švajčiarskych frankov, čo je približne 230 eur[87].

5.2. Verejné obstarávanie

Verejné obstarávanie je tiež jednou z oblastí, kde môžu mať kryptotechnológie, a teda aj blockchain, využitie. Verejné obstarávanie obsahuje rôzne práce, služby či tovary, ktoré sa majú dodať. Oblasť verejného obstarávania je často kritizovaná práve kvôli možnej korupcii a nedostatočnej transparentnosti. Použitím inteligentných zmlúv môžu byť verejné obstarávania transparentnejšie, zautomatizované a rovnako samo-vynútiteľné. Prostredníctvom blockchainu by mohol mať každý občan v krajine prístup k údajom, teda kto vyhral tender, či splnil jeho podmienky, prípadne aká bola jeho ponuka. Zároveň môže ostať identita zatajená a pomocou šifrovania a krypto technológii môžu jednotlivé strany vo verejnom obstarávaní identitu potvrdiť, teda potvrdiť prepojenie medzi identitou virtuálnou a reálnou.

Pomocou inteligentných zmlúv by sa pri verejnom obstarávaní mohli selektovať ponuky na základe zadaných vstupov. To znamená podmienok, ktoré by mala ponuka spĺňať. Napríklad nákladovosť, počet potrebných ľudí, strojov a podobne. Záleží na obstarávanom predmete. Zároveň môže byť neskôr použitá iná inteligentná zmluva, ktorá by uvoľnila prostriedky len na základe zrealizovania určitej fázy zákazky. Napríklad pri diaľniciach postavenie mosta, či

---

content/uploads/2019/06/UPPVII-blockchain-studia-v2_3-20190318.pdf?fbclid=IwAR27kbeDLast6ljL6Sm9NI44BjF1duSKYf5U2OcYyoqxkPozizrJTP0CrA4 >

[87]SWISS INFO: Chiasso accepts tax payments in bitcoin [online]. Dostupné na internete: < https://www.swissinfo.ch/eng/business/swiss-fintech_chiasso-accepts-tax-payments-in-bitcoin/43503464 >

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

asfaltovanie cesty. V prípade, že by práca nebola odvedená, tak ako boli určené podmienky v inteligentnej zmluve, tak by sa prostriedky neuvoľnili.

V tejto oblasti napríklad pracuje Kanadská vláda, ktorá začala skúšobný proces v rámci využívania technológie blockchain na účely zvýšenia transparentnosti grantov v oblasti výskumu. „Národná rada pre výskum (NRC) využíva Catena Blockchain Suite, kanadský produkt postavený na blockchaine kryptomeny Ethereum na publikovanie informácií o Programe pomoci pre priemyselný výskum (NRC IRAP) a jeho financovaní v reálnom čase.“[88] V prípade, že NRC vytvorí alebo zmení grant, všetko sa odzrkadlí v blockchaine kryptomeny Ethereum. Zároveň sa zmeny prejavia aj v online databázach, ktoré sú prístupné verejnosti. Informácie je možné filtrovať podľa peňažnej hodnoty, dátumu, prijímateľa či regiónu. Systém by mal zvýšiť transparentnosť poskytovaných grantov a obyvatelia tak môžu sledovať kam smerujú dotácie[89].

5.3. Rôzne typy potvrdení

Ďalšou z oblastí, kde je možné využiť kryptotechnológie, je evidovanie rôznych potvrdení. Potom by nebolo potrebné napríklad opakovane chodiť fyzicky na úrady alebo aj iné inštitúcie súkromného sektora s dokladmi a potvrdeniami.

Koncom roka 2017 sa podobná iniciatíva spustila v rámci projektu DigitalCity Wien. Podľa štúdie Ernst & Young: „Projekt umožňuje obyvateľom overovať dátum a pravosť dokumentov,

---

[88] ERNST & YOUNG. Štúdia možností a potenciálu technológie „blockchain“ pri zlepšovaní eGovernment riešení. Str. 59 [online]. Dostupné na internete: < https://www.vicepremier.gov.sk/wp-content/uploads/2019/06/UPPVII-blockchain-studia-v2_3-20190318.pdf?fbclid=IwAR27kbeDLast6ljL6Sm9NI44BjF1duSKYf5U2OcYyoqxkPozizrJTP0CrA4strana 59

[89] Viac informácií na: https://globalnews.ca/news/3977745/ethereum-blockchain-canada-nrc/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ako sú dopravné trasy, vlakové poriadky a výsledky hlasovania. Cieľom projektu je zjednodušiť a automatizovať administratívne procesy (podávanie správ v oblasti energetiky a schvaľovanie a overovanie registrácie podnikov, ktoré je potrebné často aktualizovať).“[90] Od spustenia v roku 2017 do marca 2019 bolo do verejného blockchainu pridaných približne 400 dokumentov. Obyvatelia, zamestnanci mesta a vývojári môžu tak sledovať prípadné zmeny v údajoch. Zároveň umožňuje implementovaná technológia vydávanie notársky overených dokumentov mesta.

Na Malte uzavrelo Ministerstvo školstva a zamestnanosti dohodu s blockchainovou firmou Learning Machine Technologies. Cieľom je vytvoriť platformu na zdieľanie dokladov o akademickom vzdelaní. Celý systém je postavený na štandarde/platforme Blockerts, ktorá bola vyvinutá ešte v roku 2016 a slúži na vytváranie aplikácií, ktoré vydávajú a verifikujú oficiálne záznamy na blockchaine. Okrem akademického vzdelania sa môžu na platforme prijímať a ukladať certifikáty, a potvrdzovať rôzne odborné licencie.

V prípade rodných listov pracuje na blockchainovom riešení iniciatíva Illinois v Spojených štátoch amerických. Spoločne s firmou Evernym pracujú na riešení, kedy by vládne inštitúcie, teda matriky, vedeli overiť rodný list a kryptograficky zapísať atribúty totožnosti. Presnejšie meno a priezvisko, pohlavie a dátum narodenia. „Poverenia na prezeranie a zdieľanie týchto údajov sú ukladané prostredníctvom jednoznačného identifikátora, každý údaj je kryptograficky zabezpečený a prístupný iba s výslovným súhlasom držiteľa totožnosti, resp. v prípade novorodenca jeho zákonného zástupcu. Verejné inštitúcie, ako aj subjekty súkromného sektora, budú môcť overiť údaje o občanovi tým, že požiadajú o šifrovaný prístup

[90] ERNST & YOUNG. Štúdia možností a potenciálu technológie „blockchain“ pri zlepšovaní eGovernment riešení. Str. 59 [online]. Dostupné na internete: < https://www.vicepremier.gov.sk/wp-content/uploads/2019/06/UPPVII-blockchain-studia-v2_3-20190318.pdf?fbclid=IwAR27kbeDLast6ljL6Sm9NI44BjF1duSKYf5U2OcYyoqxkPozizrJTP0CrA4

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

k týmto údajom. To minimalizuje potrebu, aby subjekty vytvárali, prevádzkovali a spoliehali sa na svoje vlastné databázy údajov o totožnosti občanov“.[91]

Fínsko reagovalo na problém identity utečencov v Európe riešením, ktoré zaznamenáva údaje o utečencoch na blockchain. V rámci podpory žiadateľov o azyl poskytuje Fínsko predplatenú debetnú kartu namiesto hotovosti. Totožnosť držiteľov kariet ukladá na blockchain. Štát dokáže adresnejšie poskytovať pomoc a zároveň kontrolovať výdavky utečencov**.**

5.4. Notárske zápisy

Notára určuje štát, ktorý vykonáva určenú činnosť. Pre realizáciu napríklad prevodu majetku, vlastníctva, potvrdení, dohôd či závetov môžu byť použité kryptotechnológie. Výsledkom je záznam bez možnosti zmeny, ktorý je transparentný a v určitej miere každému dostupný. Následne na to môže byť naviazaná automatizácia, či už v prevode majetku, platieb či napĺňanie sankcií v prípade problémov.

5.5. Registre (registrácia áut, občanov, právnických osôb, živnostníkov)

Kryptotechnológie vďaka transparentnosti a nemennej histórii zápisov na blockchaine môžu nájsť uplatnenie aj v oblasti rôznych registrov, ktoré v rámci verejnej správy fungujú centralizovane.

---

[91] ERNST & YOUNG. Štúdia možností a potenciálu technológie „blockchain“ prizlepšovaní eGovernment riešení. Str. 60 [online]. Dostupné na internete: < https://www.vicepremier.gov.sk/wp-content/uploads/2019/06/UPPVII-blockchain-studia-v2_3-20190318.pdf?fbclid=IwAR27kbeDLast6ljL6Sm9NI44BjF1duSKYf5U2OcYyoqxkPozizrJTP0CrA4 >

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Takýto register by mohol by zavedený napríklad v oblasti predaja jazdených áut. V tejto oblasti sú hlavným problémom stočené kilometre, kedy predajca upravuje záznam o najazdených kilometroch vo vozidle. Podľa odhadov EÚ je dopad v krajinách EÚ na úrovni 5,6 až 9,6 miliardy eur ročne[92]. Do blockchainu by sa mohol zapisovať stav kilometrov popri iných úkonoch, ako napríklad pravidelná kontrola v servise, či pri technickej a emisnej kontrole. Stav kilometrov by bol priradený na konkrétne identifikačné číslo vozidla, tzv. VIN číslo. Aplikácia, ktorá by umožňovala sledovať stav vozidiel, by bola jednoducho prístupná.

Podobne by sa mohli evidovať na blockchaine rôzne registre, ktoré majú v správe rôzne úrady. Problémom týchto registrov je, že niektoré z nich nie sú prepojené a tak predstavujú administratívnu záťaž pre bežných ľudí, aj úradníkov. Napríklad v prípade, keď je potrebné niečo potvrdzovať, ako napríklad bezúhonnosť z registra trestov. Na blockchaine by mohol fungovať napríklad register trestov, živnostenský register, obchodný register, register partnerov verejného sektora či kataster nehnuteľností.

5.6. Služby poskytujúce časové pečiatky

Jednou z možností použitia blockchainu je digitálne značkovanie alebo označovanie údajov. V princípe ide o digitálnu notársku službu, ale na rozdiel od tradičnej notárskej služby nie je potrebná dôveryhodná tretia strana. Keďže blockchain poskytuje všetky charakteristiky dôveryhodnej tretej strany, uľahčuje zabezpečené online transakcie, je to decentralizovaná a

[92] Viac informácií na: http://www.europarl.europa.eu/news/en/headlines/society/20180525STO04312/fighting-mileage-fraud-on-used-cars

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

distribuovaná sieť a zapísané transakcie nie je možné spätne meniť. To umožňuje účastníkom lacnejšie overovať a auditovať transakcie.

Označenie súboru na blockchaine preukáže, že dokument existoval v danom okamihu. Ak užívateľ podpísal dokument pred označkovaním/opečiatkovaním, tak môže tvrdiť, že dokument bol v čase označenia v jeho držbe. Ďalšou výhodou je, že užívateľ môže dokázať pôvod, dátum, autentickosť a integritu súborov bez toho, aby zdieľal ich obsah.

Napríklad hudobník A môže vytvoriť novú skladbu a uložiť ju do počítača. Po uložení skladby aplikácia automaticky vytvorí digitálne podpísané časové označenie na Bitcoinovom blockchaine. Jeho známy, hudobník B, ho neskôr navštívi a po vypočutí jeho skladby sa ju rozhodne ukradnúť. O pár dní neskôr vydá tú istú pieseň, len pod iným názvom.

V prípade, že hudobník A správne podpísal a označil skladbu, tak vlastní silný argument voči hudobníkovi B, a teda, že mu ukradol jeho autorské dielo.

Časovú pečiatku v Blockchaine je možné použiť na akýkoľvek súbor, a to napr. holý text TXT, PDF, Microsoft Word (DOC, DOCX), obrázky (TIFF, JPEG atď.), tabuľky (XLS, XLSX), kresby (CAD) s akýmkoľvek obsahom.

Pečiatkovanie je úplne decentralizované, avšak nemusí byť (ako samotný blockchain), preto nie je potrebná tretia strana ani centralizovaná internetová služba, aby užívateľ mohol v budúcnosti dokázať autenticitu dokumentu. Užívateľ bude môcť preukázať pečiatku dokumentu odkazom na odtlačok dokumentu (hash) na verejne dostupnom blockchaine.

Dnes existuje na trhu už niekoľko projektov, platforiem a nástrojov, ktoré umožňujú využitie blockchainových technológií na služby časových pečiatok. V nasledujúcej časti analyzujeme hlbšie tie najvýznamnejšie z nich.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Originstamp

Origin Stamp[93] je webová služba, slúžiaca na timestamping, ktorá využíva blockchain na ukladanie anonymných časových pečiatok, chránených pred neoprávneným zásahom do obsahu. OriginStamp umožňuje používateľom hašovať súbory, e-maily alebo obyčajný text a následne ukladať vytvorené haše do blockchainu, ako aj overovať časové pečiatky, ktoré už sú v blockchaine. OriginStamp je zadarmo. Umožňuje komukoľvek, a to od študentov až po vedcov, dokazovať pravosť nejakej myšlienky či dokumentu.

Služba najprv hašuje daný súbor SHA-256. Následne raz denne algoritmus agreguje haše a posiela ich v transakcii do blockchainu. Používa pri tom kódovanie Base 58 a následne sa použije novo vytvorená Bitcoinová adresa, na ktorú sa pošle výsledný hash, ktorý má agregované všetky haše, s najnižšou hodnotou, teda 0,000055 Bitcoinu. Takto sa haše zapíšu do blockchainu. Následne po potvrdení transakcie sú jednotlivé haše dostupné každému, čo znamená, že každý môže overiť ich pravosť.

Za službou stojí Bela Gipp, ktorý mal prototyp timestampingu vytvorený už v roku 2011. Samotná služba a web fungujú od roku 2014.

Open Time Stamps

Open Time Stamps[94] je projekt, ktorý funguje na podobnom princípe ako predchádzajúce a hlási sa k nemu vývojár Peter Todd. Projekt vznikol v roku 2016 a jeho výhodami sú:

[93] Viac informácií na: https://originstamp.org/home

[94] Viac informácií na: https://opentimestamps.org/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- **Dôvera** - OpenTimestamps používa decentralizovaný, verejne kontrolovateľný Bitcoinový blockchain, čím odstraňuje potrebu dôveryhodných strán. Architektúra OpenTimestamps je navrhnutá tak, aby v budúcnosti podporovala rôzne kontrolovateľné notárske metódy.
- **Cena** - OpenTimestamps sa škáluje neurčito, čo umožňuje bezplatné vytváranie časových pečiatok kombináciou neobmedzeného počtu časových pečiatok do jednej Bitcoinovej transakcie.
- **Pohodlie** - OpenTimestamps môžu vytvoriť časovú pečiatku overiteľnú treťou stranou za pár sekúnd. Nie je potrebné čakať na potvrdenie, ako pri Bitcoinovej transakcii.

Digital Proof

Digital Proof[95] je produkt od slovenskej firmy Decent. Platforma prenáša právne dokumenty z analógovej podoby na digitálnu podobu – a zároveň zapisuje, kedy a kde bol dokument podpísaný. Systém pomáha chrániť podnikateľov, odstrániť právne rozdiely a vytvoriť ochranu na globálnej úrovni.

V súdnych sporoch sú potom k dispozícii digitálne dôkazy, ktoré dokazujú vytvorenie dokumentu – čo využívajú niektoré jurisdikcie na preukázanie vlastníctva. Napríklad najvyšší súd Číny minulý rok rozhodol, že dôkazy overené technológiou blockchain sú v právnych prípadoch záväzné. Okrem nej aj v Taliansku sú už právne uznateľné tzv. time-stamped súbory.

Cieľom platformy je nahradiť tradičného notára službou, ktorá je lacnejšia a bezpečnejšia. Platforma, ktorej ochrana duševného vlastníctva trvá iba niekoľko minút, by mohla sporom ušetriť desiatky hodín a financií.

[95] Viac informácií na: https://decent.ch/press-release/protect-what-is-yours-decents-digital-proof-securely-logs-ideas-patents-documents-and-more/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Digital proof funguje podobne ako ostatné spomínané služby. Na web sa nahrá súbor, ktorý sa digitálne podpíše a dostane časovú pečiatku. Následne sa môže tento súbor stiahnuť a ďalej používať. Služba zároveň ponúka možnosť overenia už podpísaných súborov, či niekomu nepatria.

Factom

Factom je v rámci kryptomien jedným z projektov, ktorý sa venuje registrom. Projekt existuje od roku 2015 a jeho účelom je tvorba a správa databáz alebo registrov.[96] Projekt na ukladanie dát využíva blockchain Bitcoinu. Zápis môže realizovať súkromná alebo verejná inštitúcia, pričom tieto dáta nemôžu byť ohrozené treťou stranou a zároveň sú v systéme nemenné. To znamená, že keď sú raz do systému zapísané, tak nie je možné ich zmeniť.

Napriek tomu, že Factom využíva blockchain Bitcoinu, tak sa ako kryptomena odlišuje. „V prípade kryptosystému Factom musí verejná inštitúcia pri tvorbe databázy postupovať nasledovne. Po prvé, musí nakúpiť menu Factomu – tzv. factoidy. Factoid môžeme prirovnať k Bitcoinu, čiže ho môžeme chápať ako finančnú jednotku – token systému. Nakúpené factoidy drží v zabezpečenej elektronickej peňaženke. Následne za factoidy nakupuje práva na ukladanie dát do systému. Týmito právami sú tzv. entry kredity.“[97]

V súčasnosti je Factom stále drahším riešením, než bežné cloudové služby, avšak to sa môže v budúcnosti zmeniť. Na strane druhej by mal byť bezpečnejším, nakoľko zabezpečuje nemeniteľnosť dát pomocou Bitcoin blockchainu. Projekt je stále vo vývoji. Niektoré jeho prvky už boli spustené. Na webe majú spomenuté riešenia v rámci autentifikácie dokumentov

---

[96] Factom pochádza zo slova Factum, čo znamená: „Čo je uvedené, to je skutočné“

[97] POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. Kryptosytémy a potenciál ich využitia v súkromnom a verejnom sektore. NADÁCIA F.A. HAYEKA 2016. s.8.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

alebo produktov, rovnako riešenie pre banky a hypotekárny biznis alebo pre autentifikáciu zariadení v rámci internetu vecí. Na prevádzku a vývoj využíva príspevky od investorov, napríklad aj z Bill & Melinda Gates Foundation[98].

Úplne najmenšou jednotkou je tzv. entry súbor (v nami popisovanom prípade konkrétne údaje o obyvateľovi), ktorý užívateľ (štát) vloží do vytváranej predmetnej databázy (tzv. chainu).

Predmetné databázy (chainy), si môžeme predstaviť ako zložky s dátami, pričom každá zložka je určená pre iné dáta. Jedna zložka bude obsahovať len dáta o obyvateľoch a druhá len lekárske záznamy. Nikdy sa nemôže stať, že dáta s lekárskymi záznamami sa dostanú do zložiek s údajmi o obyvateľoch. Na jednej strane by sa to nedostalo cez pravidlá, ktoré si každý užívateľ môže na začiatku v databáze definovať. Na strane druhej každý vkladaný entry súbor má svoju tzv. chain ID. To je identifikačné číslo vkladaného údaju, na základe ktorého sa ukladajú dáta do jednotlivých predmetných databáz (chainov).

Štát môže navyše definovať napr. databázu, ktorá bude brať do úvahy aj konkrétnu legislatívu alebo iné pravidlá a kritériá. Samozrejme v prípade zmeny legislatívy alebo pravidiel je možné ich primerane meniť v samotnej databáze, čo znamená, že pravidlá sa dajú priebežne aktualizovať. Využitie predmetných databáz je teda veľmi široké a záleží len od používateľa, povahy samotných dát a ich vzájomnej kombinovateľnosti.

Systém je zabezpečený vysokou mierou kryptografie. Každú minútu sa chainy (databázy) zaradia do vyššej vrstvy, ktorou je blok chainov, obsahujúci niekoľko chainov. Tie sa následne uložia do najvyššej vrstvy - tzv. directory bloku. Na konci každej minúty sa vytvorí jeden directory blok, kde sú uložené bloky chainov. Tento proces sa zopakuje 10-krát, pričom po zostavení 10-teho directory bloku, teda na konci 10 minúty, sa vytvorí celkový hash týchto

[98] Viac informácií na: https://coinsutra.com/factom-cryptocurrency-fct

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

blokov, ktorým sa 10 directory blokov na konci 10 minúty uloží do blockchainu. Všetky uložené dáta a rovnako aj jednotlivé úrovne dát sú tak zabezpečené kryptograficky.[99]

Hlavné výhody tohto systému sú:

- **Bezpečnosť -** nikto iný okrem samotného tvorcu chainu (našej databázy) nemá možnosť do neho zasahovať.
- **Flexibilita** - je zabezpečená tzv. prvým vstupom entry. To je aplikácia, ktorá sa dá flexibilne meniť vzhľadom na štruktúru dát a ich funkcionalitu.
- **Systém** - môže ušetriť náklady, či už sú to náklady na udržiavanie rôznych databázových systémov, alebo náklady spojené s bezpečnosťou.

Poslednou výhodou je možnosť previazania jednotlivých databáz. To znamená, že napríklad pri vybavovaní úveru bude vedieť banka stiahnuť potrebné údaje z rôznych druhov databáz. Napríklad identitu, bydlisko, súpis majetku.

5.7. Postoj kľúčových inštitúcií ku kryptomenám či blockchainu

Kryptomeny boli od vzniku Bitcoinu skôr len záležitosťou pár tisíc nadšencov, ktorí o ňom hovorili, prípadne sa podieľali na vývoji alebo ním platili či obchodovali. Postupne sa Bitcoin, ale aj ostatné kryptomeny dostali aj do povedomia širšej verejnosti, ako aj súkromného sektora, kde sa začalo diskutovať, ale aj vyvíjať množstvo potenciálnych riešení, ktorých

[99] POŠVANC, M. - CABAJ, A. – HAVRAN, T. – LINDÁK, M. – STANCEL, D. – THURZO, A. Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore. NADÁCIA F.A. HAYEKA 2016. s.9.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

súčasťou sú kryptomeny. Postupne sa začal dostávať aj do povedomia štátov a rôznych zoskupení či inštitúcií, ktoré na jednej strane musia reagovať a snažia sa vytvoriť právny rámec, ale na druhej strane sa pozerajú na kryptomeny a blockchain ako na prostriedok, ktorý môže zlepšiť ich fungovanie. V nasledujúcej kapitole si popíšeme postoje či aktivitu jednotlivých inštitúcií v tejto oblasti.

Centrálne banky

Podľa dokumentu Global Blockchain Benchmarking Study[100] je možné používať blockchain aj v rámci činnosti centrálnych bánk. Celkovo sa robil prieskum v 57 centrálnych bankách a 31 krajinách, kde sa pozerali na využitie blockchainu vo verejnej správe. Presnejšie, 49 % respondentov bolo z Európy a 35 % pochádzalo zo Severnej Ameriky a Ázie. V nasledujúcej tabuľke uvádzame výsledky prieskumu, ktorý sa zameriaval na jednotlivé oblasti, kde centrálne banky skúmajú využitie blockchainu.

[100]Viac informácií na: https://www.ey.com/Publication/vwLUAssets/ey-global-blockchain-benchmarking-study-2017/$File/ey-global-blockchain-benchmarking-study-2017

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tabuľka 5: Oblasti výskumu pre aplikáciu Blockchainu centrálnymi bankami

Oblasť v ktorej vyvíjajú centrálne banky aktivitu	Podiel
Virtuálne meny emitované centrálnou bankou	82 %
Platby	55 %
Dodržiavanie predpisov (oblasť regulácie)	36 %
Správa údajov z oblasti vlastníctva	23 %
Manažment identity	18 %
Audit	18 %
Správa osobných údajov	14 %
Dane	5 %
Ostatné	41 %

Zdroj: Global Blockchain Benchmarking Study

Medzi ostatné oblasti (41 %) patrí transfer aktív, klíring cenných papierov, syndikované pôžičky, alebo všeobecne financie. V rámci verejnej správy uvádza štúdia rovnako prieskum, ktorý sa pozeral na záujem v jednotlivých krajinách a danej oblasti.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tabuľka 6: Oblasti v ktorých vyvíjajú inštitúcie verejnej správy aktivitu

Oblasť	Podiel
Manažment identity	50 %
Správa údajov z oblasti vlastníctva	50 %
Správa obchodných záznamov	31 %
Správa osobných údajov	31 %
Audit	28 %
Voľby	25 %
Dodržiavanie predpisov (oblasť regulácie)	25 %
Platby	13 %
Dane	6 %
Ostatné	63 %

Zdroj: Global Blockchain Benchmarking Study

Medzi ostatné oblasti patrí (63 %) 3D tlač, kolektívne investovanie (crowdfunding), manažment dokumentov, internet vecí, logistika, manažment zásob, ukladanie zdravotníckych záznamov. Stav sa už mohol mierne zmeniť, pretože štúdia je z roku 2017.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Európska únia

V apríli 2018 podpísalo 21 členských krajín Európskej únie a Nórsko zmluvu, ktorou vytvorili Európske partnerstvo pre blockchain (EU blockchain Partnership). Zároveň založením deklarovali spoluprácu pri zakladaní Európskej infraštruktúry blockchainových služieb (European Blockchain Services Infrastructure). V nej ide o poskytovanie cezhraničných digitálnych verejných služieb. Neskôr sa pridalo ďalších 5 členov.

Partnerstvo by malo zabezpečiť výmenu a komunikáciu informácií medzi členmi vo vývoji, implementácii a regulácii blockchainu a naviazaných služieb. Zároveň by sa mali členovia podieľať na príprave a spustení celoeurópskych blockchain aplikácií v rámci jednotného digitálneho trhu. Tiež by sa malo napomôcť rozvoju služieb a spoločností, ktoré pracujú v oblasti blockchainu.

Medzi členské krajiny patria Belgicko, Luxembursko, Bulharsko, Malta, Česká republika, Holandsko, Rakúsko, Nórsko, Estónsko, Poľsko, Fínsko, Portugalsko, Francúzsko, Slovensko, Nemecko, Slovinsko, Írsko, Španielsko, Litva, Švédsko, Lotyšsko, Veľká Británia, Cyprus, Taliansko, Rumunsko, Dánsko, Grécko. Medzi krajiny, ktoré sa nepridali, patria Maďarsko a Chorvátsko.

European Blockchain strategy (EBS)

Podľa brožúry European Blockchain Strategy sú blockchain a ostatné súvisiace technológie prierezovými technológiami, ktoré môžu posilniť postavenie občanov, verejných služieb či podnikov a to v zmysle bezpečného a transparentného prenosu a zdieľania dát. Blockchain a ostatné decentralizované technológie sú podľa EBS vhodným doplnkom pre decentralizované a viacúrovňové riadenie v rámci Európskej únie.

Podľa European Blockchain Observatory and Forum a prieskumu medzi 400 startupmi z apríla 2019 je použitie blockchainu v jednotlivých sektoroch nasledovné. Umiestnenie startupov a

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

jednotlivých iniciatív sleduje EU Blockchain and observatory forum na mape. Podľa prieskumu je 32 % všetkých startupov umiestnených v Európe, 41 % v Severnej Amerike a 22 % v Ázii. Zvyšok je v Afrike, Južnej Amerike a v Oceánii.

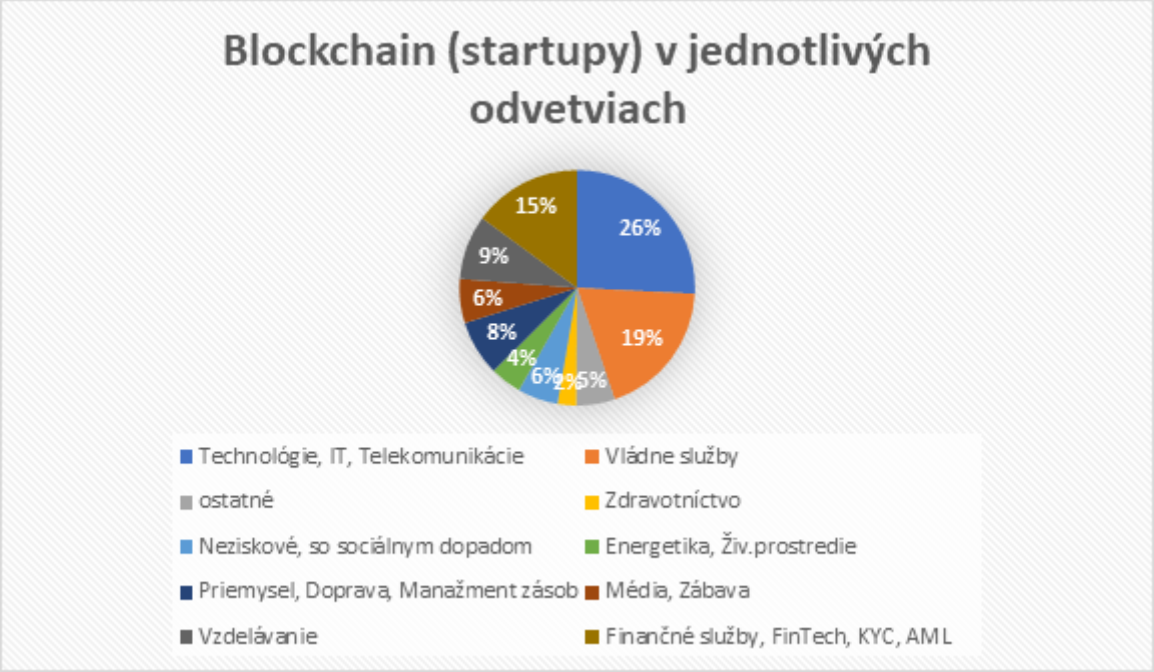
V rámci stratégie by chcela Európska únia:

- Viac prepájať štáty. To znamená, aby vo vyššej miere spolupracovali navzájom v oblasti blockchainu a decentralizovaných technológií.
- Verejno-súkromné partnerstvá – podpora vytvorenia The International Association of Trusted Blockchain Applications (INATBA).
- Podpora EU Blockchain Observatory and Forum, ktorá spája expertov z rôznych oblastí v rámci blockchainu.
- Investovanie do nových spoločností a startupov.
- V rámci programu Horizon 2020 investovala od roku 2015 celkovo 185 miliónov eur do oblastí ako kyberbezpečnosť, digitálna identita, internet vecí, E-health alebo energetika. Ďalších 60 miliónov by malo byť dostupných v roku 2020. Ďalšie prostriedky budú vyčlenené v rámci nového rozpočtu EÚ v roku 2021 - 2027 prostredníctvom Horizon Europe a v rámci Digital Europe Programme.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Obrázok 11: Blockchain startupy podľa odvetví



Zdroj: European Blockchain Observatory and Forum

International Association for Trusted Blockchain Applications (INATBA)

Ponúka vývojárom a používateľom decentralizovaných technológií globálne fórum, v ktorom môžu diskutovať s tvorcami politík a regulátormi. Cieľmi asociácie sú:

- Konštruktívny dialóg - Udržiavať trvalý a konštruktívny dialóg s orgánmi verejnej moci a regulačnými orgánmi, ktorý prispeje ku konvergencii regulačných prístupov k blockchainu a s ním spojenými technológiami.
- Model riadenia - Podporovať otvorený, transparentný a inkluzívny globálny model riadenia pre blockchain, ktorý odráža spoločné záujmy strán z priemyslu, začínajúcich podnikov a MSP, vlád a medzinárodných organizácií.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- Podpora vývoja - Podporovať rozvoj a prijímanie usmernení o interoperabilite, globálnych normách s cieľom posilniť dôveryhodné digitálne služby zamerané na užívateľa.
- Aplikácia decentralizovaných technológií - Vypracovať sektorovo špecifické usmernenia a špecifikácie pre vývoj a urýchlenie sektorových blockchainov a decentralizovaných technológií v konkrétnych sektoroch.

Celkovo má INATBA trinásť pracovných skupín, a to: vzdelávanie, spravovanie (z angl. governance), mobilita, nehnuteľnosti, energetika, zdravotníctvo, súkromie (z angl. privacy), sociálny dopad, financie, identita, verejný sektor, manažment zásob, a vzájomná kompatibilita (z angl. interoperability).

5.8. Podporené projekty na úrovni EÚ

Európska únia v rámci výskumu finančne podporila už viaceré projekty[101] z oblasti blockchainu. V rámci kapitoly opíšeme jedny z prvých podporených, a to jeden je z oblasti zdravotníctva a druhý z oblasti správy dát.

My Health My Data

Medicínske dáta sú často ukladané separátne a nie sú prístupné pacientom alebo vedcom. Zároveň sú náchylné na ukradnutie identity, či napadnutie úložísk, kde sa dáta nachádzajú. Cieľom projektu My Health My Data (MHMD) je používať blockchain na to, aby boli dáta uložené bezpečne a mohli sa jednoducho prenášať. Zároveň by sa mali projektom prepojiť

[101] Viac informácií na: https://ec.europa.eu/digital-single-market/en/news/eu-funded-projects-blockchain-technology

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

nemocnice a ostatné organizácie, narábajúce s dátami, a presvedčiť ich, aby dáta poskytovali anonymne vedcom, ktorí ich používajú vo výskume. Neskôr by mala vzniknú nad dátami analytika, ktorá by dokázala spracovávať dáta a využívať ich.

Celkovo má na účel My Health My Data Európska únia vyčlenených 3 455 190 eur z programu Horizon 2020. Krajiny, ktorý sa to týka: Taliansko (koordinátor), Rakúsko, Francúzsko, Nemecko, Grécko, Rumunsko, Švajčiarsko a Spojené kráľovstvo (nemocnice, univerzity a súkromné spoločnosti).[102]

Decode

Je projektom, ktorý pracuje na výskume v oblastí technológií, ktoré by bežným ľuďom priniesli viac kontroly nad citlivými osobnými dátami. A to najmä v oblasti internetu.

Užívatelia by mali mať v konečnom dôsledku svoje dáta plne pod kontrolou a bezpečne uložené. Výsledkom projektu by mala byť možnosť pre bežných ľudí zdieľať dáta s inovátormi, mimovládnymi organizáciami a rôznymi komunitami, ktoré môžu nad dátami vytvárať aplikácie a služby, ktoré uľahčia narábanie s dátami.

V roku 2018 boli spustené štyri pilotné projekty. Dva z toho v Amsterdame a dva v Barcelone. Projekty v Amsterdame sa sústredia na vývoj registra, ktorý by zaznamenával krátkodobé prenájmy a dokázal by používateľom poskytovať lepší prehľad. V Barcelone sa projekty zameriavajú na vývoj jednotného dátového cloudu, kde by boli všetky zozbierané dáta z rôznych zdrojov. Celkovo má na účel DECODE Európska únia vyčlenených 5 miliónov eur

[102]Viac informácií na: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership >

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

z programu Horizon 2020. Krajiny, ktorý sa to týka: Španielsko (koordinátor), Francúzsko, Taliansko, Holandsko, Švédsko a Spojené kráľovstvo.

5.9. OECD

Tak ako aj Európska únia, aj OECD sa už venovala blockchainu a jeho využitiu. A to v dokumente Blockchain Unchained: Blockchain Technology and its Use in the Public Sector z prvej polovice roku 2018**.** Cieľom dokumentu je informovať zamestnancov verejnej správy a odborníkov na blockchain či vedúcich predstaviteľov o možnostiach a dopade technológie blockchain. Zároveň však informuje o oblastiach, kde nie je vhodné blockchain použiť. Dokument rieši aj prípadové štúdie. Okrem tradičnej oblasti uplatnenia vo finančných transakciách, vidí OECD potenciál aj v oblasti digitálnej identifikácie, voľbách, či katastri. V dokumente sa poukazuje na to, že blockchain má potenciál zlepšiť efektívnosť, transparentnosť, znížiť byrokratické bariéry a podporiť zdieľanie a automatizáciu vďaka inteligentným zmluvám.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tabuľka 7: Rozšírenie blockchain projektov a ich využitie v odvetviach

1.	Stratégia/výskum (42)	Vládne služby (173)
2.	Identita (poverenia / licencie / osvedčenia) (25)	Finančné služby (73)
3.	Osobné záznamy (zdravotné, finančné, atď.) (25)	Technológia a IoT (26)
4.	Hospodársky rozvoj (24)	Zdravotníctvo (23)
5.	Finančné služby / Trhová infraštruktúra (20)	Nehnuteľnosti (22)
6.	Katastre nehnuteľností (19)	Dodávateľský reťazec (19)
7.	Digitálna mena (vydaná centrálnou bankou) (18)	Energetika (13)
8.	Výhody / Požiadavky (13)	Doprava (13)
9.	Súlad / Podávanie správ (12)	Vzdelávanie (8)
10.	Výskum / Štandardy (12)	Telekomunikácie (4)

Zdroj: OECD

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

6. ŠEDÁ EKONOMIKA A REGULÁCIA KRYPTOMIEN

Kryptomeny sú decentralizované a transparentné. Okrem toho sú v určitej alebo plnej miere taktiež anonymné. To vytvára vhodné podhubie pre rast a rozvoj šedej sféry ekonomiky v tej ktorej krajine. V nasledujúcej kapitole zanalyzujeme, ako sa vyvíjali čierne trhy v súvislosti s kryptomenami a následne popíšeme stav regulácie kryptomien v Európskej únii či v Spojených štátoch amerických. Zároveň aj na Slovensku.

6.1. Darknet

Darknet, ktorý sa označuje aj darkweb alebo deepweb, je časť webu, ktorá nie je bežne prístupná cez obyčajne používané prehliadače. Najčastejšie sa na prehľadávanie darknetu používa prehliadač Tor, ktorý slúži len na prístup na stránky z darknetu. Vďaka nemu sa IP adresy používateľov premiešavajú tak, aby sa nedali vystopovať.

Darknet sa často používa na obchodovanie všetkého nelegálneho, ako napríklad pornografie, zbraní, drog, ale aj vrážd či DDOS útoky. Napriek tomu používajú darknet aj disidentské či spravodajské organizácie, bezpečnostné služby alebo novinári z neslobodných krajín. Napríklad aj samotné Wikileaks bolo na darknete.

Napriek tomu, že darknet je dostupný prostredníctvom prehliadača Tor, tak nie je možné vyhľadávať stránky, ako na google. Existuje množstvo stránok na ktoré musíte mať presnú adresu, ktorá je známa len zainteresovaným stranám.

S príchodom bitcoinu, ktorý zabezpečuje pseudo anonymitu, prišli aj trhy vybudované na darknete, a to s obchodovaním nelegálnych tovarov či služieb za bitcoiny. Jedným z prvých takýchto trhov bol Silk Road.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Silk Road

Trhovisko Silk Road vzniklo začiatkom roka 2011 a za krátky čas sa stalo jedným z najpopulárnejších. Neskôr v roku 2013 bolo uzatvorené po tom, ako v Spojených štátoch vypátrali jeho administrátora Rossa Ulbrichta, ktorý bol v roku 2015 odsúdený na doživotie.

Počas necelých troch rokov dosiahli tržby 9,5 milióna Bitcoinov a celková provízia Ulbrichta tvorila viac ako 600-tisíc Bitcoinov. Celkovo na ňom fungovalo 3877 obchodníkov, ktorí mali viac ako 146-tisíc zákazníkov, pričom prebehlo viac ako 1,2 milióna transakcií. Najviac sa na Silk Road obchodovalo s drogami a liekmi na predpis. Rovnako boli v ponuke aj nástroje na hacking, falošné dokumenty či knihy.

Úlohou Rossa Ulbrichta bolo administrovať portál a zároveň kontrolovať obchodníkov a ich referencie, aby tak zaistil ich dôveryhodnosť a rovnako dôveryhodnosť ich služieb či tovarov, ktoré predávajú.

Dôvodom, prečo odhalili Silk Road, ktorý mal existovať mimo dosahu bežného sveta, bola chyba Ulbrichta. On sám bol programátorským samoukom a Silk Road nedostatočne zabezpečil. Vyšetrovateľom sa v konečnom dôsledku podarilo dostať ku serveru na ktorom fungovalo trhovisko a cez server sa dostali k používateľovi menom „Dread Pirate Roberts“. Následne potom ku aktivite na programátorskom fóre a k jeho emailu. Po kratšej dobe sledovania bol Ross Ulbricht zatknutý a trhovisko Silk Road zatvorené.

Napriek tomu krátko potom vzniklo Silk Road 2.0 a niekoľko ďalších trhovísk, kde sa predávali nelegálne tovary a služby, napríklad Atlantis, Dark Market Reloaded a Sheep Marketplace. Niektoré z nich, ako napríklad Valhalla, existujú už dlhšie než Silk Road.

Niektoré z nich už nefungujú, napríklad prevádzkovatelia Silk Road 2.0 boli vypátraní a zatknutí, avšak Silk Road 3.0 vzniklo niekoľko minút potom. Dark Market Reloaded zatvorili

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

a administrátori Sheep Marketplace a Atlantis skončili tzv. exit scamom. To znamená, že administrátori ukradli peniaze používateľov a zrušili burzu.

História Sheep Marketplace je v tomto ohľade špecifická. Drogový trh bol v prevádzke približne pol roka v roku 2013, kedy prevádzkovateľ uzavrel burzu a utiekol s prostriedkami. Väčšina týchto trhovísk totiž funguje na princípe tzv. Escrow kontraktu, kam nakupujúci pri obchode pošle peniaze, ktoré sa uvoľnia predávajúcemu až v momente, keď nakupujúci potvrdí prijatie tovaru vo vopred dohodnutom množstve a kvalite. Slabý bod tohto systému je správca, ktorý je v pokušení vziať peniaze z escrow kontraktu a utiecť. Aj keď by správca nemal mať problém utiecť, tak prípad Sheep Marketplace dokázal, že to problém bol. Podvedení užívatelia využili transparentnosť Bitcoinového blockchainu, kde sú všetky adresy a transakcie navždy zapísané a je možné ich prehľadávať. Na verejne známu adresu správcu zaslali menšiu sumu a potom sledovali, kam spoločne s ostatnými Bitcoinami poputuje. Nakoniec užívatelia zistili, že za tým bol Tomáš Juříkovský z Moravy, ktorý si kúpil nový dom zaplatený Bitcoinami. V konečnom dôsledku správcom bol brnenský programátor, ktorý ukradol Bitcoiny v hodnote desiatok miliónov dolárov.

Neskôr v roku 2014 prebehla operácia Onymous počas ktorej FBI a Europol zatvorili 14 darknet trhovísk. Po tejto operácii nastúpila nová generácia trhovísk, ktoré dokázali limitovať toto riziko a zároveň aj riziko ukradnutia prostriedkov zo strany správcu. Zaviedli multisig transakcie, kde je potrebných viac podpisov a správca tak nemá celú moc nad prostriedkami používateľov. Zaviedol sa šifrovaný chat, dvojfaktorová autorizácia a využívanie alternatívnych, skôr anonymných kryptomien.

Podľa magazínu Economist sú na trhoviskách najpopulárnejšie drogy, lieky na predpis ako antidepresíva a lieky na úzkostné stavy. Najmenšie zastúpenie majú morálne najproblematickejšie veci, ako detská pornografia, kradnuté čísla platobných kariet, či

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

hackerské nástroje. S rozvojom takýchto trhovísk sa zvyšuje aj bezpečnosť pre obchodníkov a ich zákazníkov.

Bitcoin, ale aj iné kryptomeny sa používajú na väčšine týchto trhovísk, keďže umožňujú anonymne a rýchle presúvať hodnotu naprieč štátmi a sú lepšou alternatívou ako hotovosť. Napriek tomu len minimum Bitcoinových transakcií sa týka nelegálnej činnosti. Podľa Chainalysis[103], spoločnosti, ktorá okrem iného sleduje aj aktivitu na darknete, sa Bitcoin používa na nelegálne aktivity len v menej ako jednom percente transakcií. V roku 2012 to bolo približne sedem percent z celkových transakcií.

6.2. Anonymné kryptomeny

Anonymné kryptomeny sa začali objavovať na trhu pár rokov potom, ako vznikol Bitcoin. Nakoľko sa Blockchain charakterizuje úplnou transparentnosťou všetkých transakcií, ktoré sa doňho zapíšu, je pomerne jednoduché dohľadať všetky relevantné meta dáta súvisiace s transakciami, ako kto, kedy, komu a koľko poslal peňazí. Viaceré kryptomenové projekty sa práve túto vlastnosť blockchainu snažia upraviť pomocou rôznych kryptografických techník, ktoré zakrývajú odosielateľa transakcie a v niektorých prípadoch dokonca aj príjemcu či sumu. V nasledujúcej časti analyzujeme tie najvýznamnejšie z nich.

Monero

Podobne ako Bitcoin vznikla aj kryptomena Monero[104]. Vznikla bez vedúceho predstaviteľa, bez zakladajúcej spoločnosti, či inej formálnej organizácie. Na rozdiel od Bitcoinu je Monero

[103] Viac informácií na: https://www.chainalysis.com/

[104] Viac informácií na: https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

úplne anonymné. Bitcoin je pseudo-anonymný, čo znamená, že všetky transakcie a adresy sú online viditeľné. V prípade, že sa podarí priradiť ku adresám identitu, tak od tej doby už nie je vlastník anonymný a je možné v súvislosti s jeho adresou všetko dohľadať. Zároveň je výhodou to, že pri Monere sa nedá určiť, či minca bola použitá nelegálne alebo nie. V prípade Bitcoinu to možné je a následne aj keď je minca v legálnych rukách, tak sa môže stať, že niektoré podniky alebo verejný sektor ju považujú za nelegálnu a tak ju neprijme. Dokonca môžu zmraziť účet.

Naopak Monero je pomerne vysoko anonymnou kryptomenou a len vlastník adresy vidí stav a históriu svojho účtu. Súkromie je zabezpečené pomocou týchto kryptografických technológií:[105]

- Dual-key stealth adresy: skrývajú príjemcu transakcie.
- Ring signatures: skrývajú odosielateľa transakcie.
- RingCT: skrývajú hodnotu transakcie.
- i2P Kovri: skrýva IP adresu používateľov (v súčasnosti sa implementuje).

Monero je takmer úplne anonymnou kryptomenou a nie je možné sa dopátrať ani k štatistikám, kde sú zobrazené najbohatšie účty držiace Monero. V prípade ostatných kryptomien ako Pivx alebo ZenCash či Zcoin to možné je. Zároveň pri spomínaných kryptomenách je posielanie anonymne len alternatívou a väčšina transakcií je neanonymných. Tým pádom je tu vyššie nebezpečenstvo odhalenia identity anonymných adries či transakcií.

Monero naviac okrem verejného a súkromného kľúča, ktoré používa aj Bitcoin, používa aj ďalšie dva. A to verejnú a súkromnú časť, tzv. view key, ktorý môže poskytnúť tretej strane na prezeranie stavu účtu. Tretia strana nemôže iniciovať žiadne pohyby na účte.

[105] Viac informácií na: https://www.alza.sk/monero

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Na rozdiel on Bitcoinu, Monero nemá nemennú monetárnu zásobu. Jeho emitovanie sa v čase znižuje až na nemennú konštantu, a teda bude mať konštantnú inflačnú monetárnu politiku. Zároveň má Monero dynamickú veľkosť bloku. A väčšinou so zväčšujúcim sa množstvom transakcií sa zväčšuje aj maximálna dátová veľkosť blokov.

Zároveň sa algoritmus upravuje tak, aby sa nemohla centralizovať ťažba pomocou tzv. zariadení ASIC, ktoré sú pri ťažbe efektívnejšie. Vývojári k tomu pristúpili po tom, čo začala náročnosť ťažby Monera rýchlo narastať. To spôsobuje, že GPU ťažiari sú v nevýhode a môže sa zvyšovať centralizácia ťažby v prospech vlastníkov ASIC. Vývojári sa dohodli, že ťažobný algoritmus kryptomeny zmenia. Monero tým zabezpečuje čo najväčšiu možnú decentralizáciu a bezpečnosť siete. Vývojári sa zaviazali k zmene algoritmu kvôli bezpečnosti v polročných periódach.

Dash

Kryptomena[106] vznikla v januári v roku 2014 pod názvom XCoin. Ešte v tom mesiaci sa premenovala na Darkcoin a v marci 2015 na Dash. Kryptomena od začiatku mala byť alternatívou Bitcoinu a vynikať v rámci rýchlosti transakcií. Kým v Bitcoine sa blok generuje každých približne 10 minút, tak v Dashi sa generuje každé 2,5 minúty.

Zároveň sa Dash zaraďuje medzi anonymné kryptomeny, pretože ponúka možnosť Private Send, čo znamená, že môžete spraviť transakciu pri odosielaní anonymnou, avšak potrebujú mať zriadenú tzv. Masternode. Pri nej musí užívateľ držať 1000 mincí Dash na osobitnej peňaženke, ktorá musí byť online a objem mincí nesmie podliezť hranicu 1000.

[106] Viac informácií na: https://docs.dash.org/en/stable/introduction/about.html

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

„Masternode jednoducho funguje tak, že mixuje odosielané jednotky so zapnutou funkciou Private Send s tými, ktoré sú v peňaženke prevádzkovateľa masternode. Odosielané jednotky sa namiešajú s jednotkami s celkom inou transakčnou históriou, a tým dôjde k zachovaniu anonymity odosielateľa. Prevádzkovatelia týchto masternodov za odmenu získavajú 45 % z poplatkov za vyťažený blok.“[107]

Nevýhodou kryptomeny Dash je, že jej vedenie nie je decentralizované. Vývoj Dashu riadi a koordinuje Evan Duffield, ktorý je jeden z hlavných vývojárov. Odhaduje sa, že okolo 40 % v súčasnosti emitovaných dashov (približne 9 miliónov) je jeho. Zároveň je jeho 60 % masternodov, a preto je dôvera v miešanie mincí a ich zabezpečenie anonymity predmetom diskusií.

Pivx

Private Instant Verified Transaction (PIVX)[108] je kryptomena s otvoreným (verejným) zdrojovým kódom a je orientovaná primárne na anonymitu. Vznikla vo februári roku 2016 a jej pôvodným názvom bol Darknet (DNET). Neskôr sa premenovala kryptomena na PIVX a zároveň za pol roka od vzniku sa zmenil protokol z proof of work na proof of stake.

Anonymita je zabezpečená pomocou funkcie Zerocoin[109]. Keď sa funkcia používa, tak odosielateľa mincí skrýva a nezobrazuje sa v peňaženke adresa. V marci 2019 bol Zerocoin hacknutý a Pivx v nadväznosti na to prestal Zerocoin používať.[110] To znamená, že vývojári

---

[107] ALZA. *Dash*. [online]. Dostupné na internete: < https://www.alza.sk/dash#aktualny-kurz-cena >

[108] Viac informácií na: https://pivx.org/wp-content/uploads/2019/05/PIVX-White-Paper-Sept-2018.pdf

[109] Viac informácií na: http://zerocoin.org/media/pdf/ZerocoinOakland.pdf

[110] Viac informácií na: https://pivx.org/faq-on-zerocoin-and-pivx/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

znefunkčnili aj ZPiv na používanie anonymných transakcií. Vývojári potvrdili, že samotný systém Pivx-u nebol nijako ohrozený.

Tým, že je Pivx založený na proof of stake, tak sa poplatky za transakcie pohybujú na úrovni desiatok eurocentov. Podobne ako pri kryptomene Dash, je potrebné mať na prevádzku tzv. masternodes určité množstvo mincí, presnejšie 10 000, danú sumu mať zamknutú a peňaženku online. Masternodes majú na starosti mixovanie transakcií podľa ich dostupnosti. Zároveň zaisťujú demokratický princíp celého projektu, a to hlasovanie o zmenách v projekte. Masternodes majú na rozdiel od Staking nodes relatívne vyššiu odmenu. Pivx je nastavený tak, že každých 60 sekúnd je vytvorených 5 PIV. Odmena sa delí na tri časti. Na marketing a ďalší vývoj projektu ide fixných 10 %. Zvyšných 90 % ide masternodes alebo staking uzlom. Záleží od toho, koľko ich je v tom čase online.

Pivx napriek tomu, že sa orientuje na anonymitu, má aj svoje slabiny. Rovnako má blockchainový vyhľadávač, v ktorom je vidieť, koľko má tá ktorá adresa mincí. V prípade Monera to nie je možné.

Zcash

Kryptomena Zcash[111] vznikla v roku 2016, avšak jej počiatky sa datujú o tri roky skôr, keď bola forkom Bitcoinu pod názvom Zerocoin. V roku 2014 pôvodní zakladatelia začali spolupracovať s kryptografmi na MIT a Tel Aviv University. Spolupráca priniesla pokrok v oblasti anonymity a premenovanie na Zerocash. Kryptomena sa premenovala zo Zerocoin na Zcash a oficiálne spustenie nastalo v októbri 2016.

V prípade anonymných transakcií využíva kryptomena tzv. zero-knowledge proof (zk-SNARKs), ktorý skrýva odosielateľa, prijímateľa, ale aj sumu, ktorá je posielaná. Zároveň funguje aj

[111] Viac informácií na: https://whitepaperdatabase.com/zcash-zec-whitepaper/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

transparentná funkcia. To je bežné posielanie, ako napríklad Bitcoinov, kde je zobrazená adresa oboch strán a suma. Problémom je, že len malé percento transakcií je anonymných a väčšina transakcií je bez anonymity. Množstvo mincí je fixne dané na 21 miliónov a vyťažené by mali byť do roku 2032. Rovnako aj pri Zcash funguje halving, teda delenie odmeny za vyťaženie bloku, a to každé 4 roky. Vyťaženie bloku je nastavené na každých 2,5 minúty a v súčasnosti je odmena nastavená na 12,5 mincí za vyťaženie bloku.

Verge

Je to kryptomena[112], ktorá sa zameriava na anonymitu a rýchlosť transakcií. Na rozdiel napríklad od Dashu, je plne decentralizovaná a jej zdrojový kód je verejný. Nestojí za ním žiadna spoločnosť či osoba alebo komunita. V počiatkoch nevznikla ani prostredníctvom ICO.

Verge vznikol v roku 2014 pod názvom DogeCoinDark. Neskôr v roku 2016 sa premenoval len na Doge. Dnes je známy pod menom Verge a kryptomena má označenie XVG. Verge na zabezpečenie anonymity využíva niekoľko technológií či postupov.

Servery medzi sebou štandardne na internete komunikujú cez poskytovateľa internetových služieb (z angl. Internet Service Provider), ktorý funguje pri komunikácii ako tretia strana. Na to, aby mohli byť správy posielané cez internet, musia mať počítače špecifický identifikátor, ktorý sa nazýva IP adresa. Toto umožňuje poskytovateľom internetových služieb (ISP) zhromaždiť súkromné informácie, ako napríklad lokáciu IP adries, čo narúša anonymitu užívateľov.

Verge proti narušeniu anonymity využíva Tor a I2P, ktoré využívajú tzv. Onion router, čo je softvér na anonymizáciu IP adries. Názov Onion vychádza z toho, že jednotlivé pakety sú

[112] Viac informácií na: https://whitepaper.io/document/12/verge-whitepaper

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zabalené do viacerých vrstiev, pripomínajúcich vrstvenie cibule, a poslané cez viacero uzlov. Tým majú správy viackrát zmenenú IP adresu. To sťažuje dohľadanie transakcie.

I2P je skratka pre „Invisible Internet Project“ a predstavuje riešenie anonymizácie. Zatiaľ čo Tor umožňuje svojim používateľom pripojiť sa k bežnému internetu anonymne, I2P sa zameriava na uľahčenie bezpečného a anonymného vnútorného spojenia medzi používateľmi v sieti I2P. To sa často označuje ako „Darknet“. I2P v podstate vytvára svoju vlastnú súkromnú sieť v rámci internetu.

Funguje to tak, že vytvára dva oddelené tunely pre prichádzajúce a odchádzajúce správy a šifruje jednu správu do dvoch rôznych zväzkov. Predstavte si, že máte jednu poštovú schránku pre listy, ktoré ste posielali, a druhú pre listy, ktoré ste dostali. V kombinácii s dynamickým smerovaním, ktoré zakrýva IP adresy všetkých, riešenie I2P sťažuje dešifrovanie správ, aj keď ich niekto zachytí.

Zároveň vďaka Wraith protokolu je možné vyberať si medzi privátnou alebo bežnou transakciou. Bežné transakcie zabezpečujú rýchlosť a transparentnosť.

6.3. Trhoviská

Niektoré kryptomenové projekty, snažiace sa o čo najvyššiu anonymitu svojich užívateľov, začali postupom času integrovať digitálne trhoviská priamo do svojich blockchainových platforiem.

OpenBazaar

V apríli 2014 v Toronte vznikol projekt pod názvom Dark Market. Stál za ním Amir Taaki s malým tímom vývojárov, ktorý spravili proof of concept pre decentralizovaný trh. Vytvorený produkt bol úplne peer-to-peer, teda bez prostredníka, ktorý by akokoľvek zasahoval do výmeny na trhu.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Neskôr sa projekt rozdelil a vznikol dnešný OpenBazaar, pretože sa nechceli venovať len darknet trhu, teda čiernemu trhu. Brian Hoffman spolu s Amirom odhalili prvú verziu softvéru v septembri 2014. Na projekte pracovali niekoľko mesiacov aj s malým tímom vývojárov. OpenBazaar predstavili aj v Bruseli na Európskom stretnutí vývojárov softvérov s otvoreným zdrojový kódom v roku 2015. Tam získali uznanie a po ňom sa rozhodli pracovať na projekte na plný úväzok.

Myšlienka trhu bez povolenia bola silná a ľudia z celého sveta sa pripojili k autorom projektu, aby pomohli vytvoriť tento softvér s otvoreným zdrojom. V septembri tento tím vydal prvú testovaciu verziu softvéru. V priebehu niekoľkých nasledujúcich mesiacov tím pokračoval vo vylepšovaní softvéru a dostal povzbudivú odpoveď od komunity Bitcoinov. Začiatkom roku 2015 navštívili v Bruseli FOSSDEM (európske stretnutie vývojárov softvéru s otvoreným zdrojovým kódom) a predstavili projekt nadšenému publiku. Brian a niekoľko základných členov tímu sa rozhodli, že je čas zmeniť projekt z čiastočného, dobrovoľníckeho úsilia na serióznu, dobre financovanú kampaň, ktorá prinesie voľný obchod.

Neskôr založili aj spoločnosť OB1, kde získali jeden milión dolárov od Union Square Ventures a Andreessen Horowitz na rozvoj projektu. Neskôr dostali ďalšie tri milióny dolárov, po tom ako spustili projekt v apríli 2016 a ľudia začali na OpenBazaar predávať a nakupovať.

OpenBazaar je v súčasnosti decentralizovaným trhoviskom, ktoré neukladá osobné dáta a nepredáva ich tretím stranám, čo sa môže diať v prípade bežne používaných e-shopov. Na OpenBazaar sa neplatia poplatky a nevyžaduje sa založenie účtu a obchod prebieha len medzi dvoma stranami. Platí sa výhradne Bitcoinom.

V prípade, že chce predávajúci predať napríklad stoličku na OpenBazaar, tak si musí stiahnuť klienta do svojho PC. Následne vytvorí listing, kde bude stolička s jej cenou a opisom, avšak môže tam mať aj ďalšie veci na predaj. Ten nahrá na OpenBazaar. V prípade, že nájde kupcu, tak sa vytvorí kontrakt. V rámci neho kupca pošle Bitcoiny do escrow kontraktu, ten zadrží

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

prostriedky až kým kupec nie je s poslaným predmetom spokojný a potvrdí spokojnosť. Následne escrow kontrakt uvoľní prostriedky predávajúcemu.

V prípade reklamácie alebo problémov sú na OpenBazaar tretie strany, ktoré sa nazývajú Moderátori. Tí sa v prípade vyžiadania môžu zapojiť do escrow kontraktu, kde v rámci multisig transakcie, ktorá si vyžaduje dve a viac potvrdení, môžu potvrdiť či má kupujúci pravdu alebo nie.[113]

Particl

Je to decentralizovaná platforma (trhovisko) s otvoreným zdrojovým kódom. Je prispôsobená na prácu s akoukoľvek kryptomenou. Zároveň umožňuje použitie decentralizovaných aplikácií (Dapps) aj v rámci peňaženky. Cieľom projektu je spájať všetko decentralizované alebo spojené s kryptomenami na jednu platformu, a to na marketplace „trhovisko".

Projekt vznikol v roku 2017 a je nasledovníkom iného projektu pod názvom ShadowProject. Projekt má oficiálne sídlo vo Švajčiarsku v meste Zug a bol založený Paulom Schmitzerom a Rynom Matheeom. Samotný projekt zastrešuje Particl Foundation. Nadácia sa nevenuje len projektu, ale aj ostatným decentralizovaným technológiám a softvéru. Projekt má svoj utility token Particl (PART), ktorý je potrebný pre fungovanie na platforme, a to na Dapps (voľby alebo komunikácia prostredníctvom aplikácií, teda messaging).

PART vznikol prostredníctvom ICO na jar v roku 2017, keď projekt vyzbieral prostredníctvom emisie 750-tisíc dolárov. Samotný projekt zastrešuje Particl Foundation.

---

[113] Viac informácií na: https://openbazaar.org/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Trhovisko (Open Marketplace) využíva niekoľko technológií na zabezpečenie anonymity a bezpečnosti:

- Transakcie na trhovisku: Nákupy a predaje na trhu sú všetky súkromné. Transakcie sa uskutočňujú kombináciou súkromných protokolov CT a RingCT.
- Komunikácia: Komunikácia nie je v súčasnosti integrovaná do Open Marketplace, ale keď bude, bude šifrovaná a bezpečná. Particl používa protokol SMSG na bezpečné a súkromné odovzdávanie správ medzi uzlami (nodami).
- Sieťová identita (IP adresa): Aj keď táto funkcia nie je v predvolenom nastavení povolená (z bezpečnostných dôvodov), môže byť Open Marketplace ľahko presmerovaný tak, aby fungoval výlučne cez sieť Tor. Zároveň Particl pracuje na výskume aj iných protokolov anonymizácie.
- Meta údaje: Všetok obsah nahraný na marketplace (trhovisko), napríklad zoznam s obrázkami, je úplne zbavený všetkých svojich metaúdajov skôr, ako sa prenesie cez sieť Particl. Tak sa chránia používatelia pred únikom osobných údajov.
- Nahrávanie obsahu: všetok obsah, ktorý bol nahratý na trhovisko (open marketplace) je šifrovaný a nemožno ho vysledovať späť k používateľovi.
- Escrow: Decentralizovaný escrow systém funguje bez zásahu akejkoľvek tretej strany. To znamená, že žiadna iná strana, než strany daného obchodu, nemôže čítať predošlé diskusie týkajúce sa obchodu.

Particl používa escrow založený na teórii hier (Mutually Assured Destruction). Používa BIP 65 opcode na uzamknutie prostriedkov na zabezpečenej multi-signature adrese, kým transakciu nepodpíšu kupujúci aj predávajúci.

Obe strany iniciujú escrow transakciu uložením rovnakého vkladu, ktorý symbolizuje virtuálne podanie ruky. Tento bezpečnostný vklad môže byť v rôznej výške, ak sa obidve strany

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

dohodnú, medzi 0 a 100 % kúpnej ceny položky, ale optimálne je, keď sa poistný vklad rovná 100 % kúpnej ceny položky.

Prostriedky potom zostanú v escrow inteligentnej zmluve a nebudú uvoľnené, kým obidve nepotvrdia, že transakcia bola úspešne dokončená. Až potom, čo obe strany potvrdia uvoľnenie finančných prostriedkov, dostane predajca platbu za svoju ponuku. Obe strany tiež dostanú prostriedky zo svojej kaucie v plnej výške, bez akýchkoľvek poplatkov.

Zároveň má escrow kontrakt nastavený výpovedný čas, ktorý beží na vopred určenú dobu (ktorá sa môže predĺžiť, ak sa obidve strany dohodnú). Po uplynutí času už nie je možné uvoľniť prostriedky, čím sa transakcia stane stratovou pre obe strany. Tým sa zabráni úmyselnému predlžovaniu procesu.

6.4. Regulácia kryptomien

Regulácia kryptomien je témou, ktorá súvisí s kryptomenami od začiatku. Satoshi Nakamoto vytvoril prvú kryptomenu Bitcoin, ako alternatívu voči tradičným peniazom. Bitcoin mal od začiatku slúžiť ako alternatíva, nad ktorou by nemal nikto moc a nikto by ju nemohol regulovať. To vyplýva zo samotného nastavenia Bitcoinu a jeho blockchainu.

Po 10 rokoch sa situácia mení a vzniká potreba kryptomeny v nejakej miere regulovať. Dôvodom je to, že povedomie a používanie kryptomien sa vo svete pomaly zvyšuje. Prirodzene vzniká potreba štátov chrániť finančný trh. Problémom je, že kryptomeny nezasahujú len do finančnej oblasti, či oblastí peňazí, ale technológia blockchain sa dá uplatniť aj v mnohých iných oblastiach. A preto nie je možné zaradiť kryptomeny pod existujúcu reguláciu, ale je potrebné ich špecificky v niektorých oblastiach vymedziť.

Z toho dôvodu aj po 10 rokoch nepanuje vo svete zhoda ako sa legislatívne voči kryptomenám postaviť. Dokonca ani na poli Európskej únie. V nasledujúcej kapitole si ukážeme jednotlivé

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

legislatívne prístupy, či už v Spojených štátoch amerických (USA), v Európe, alebo na Slovensku.

6.4.1. Regulácia kryptomien v Spojených štátoch amerických

V rámci jednotlivých štátov USA je postoj k regulovaniu kryptomien nejednotný. V princípe záleží na jednotlivých regulátoroch, inštitúciách, aké majú právomoci. Na základe toho regulujú trh s kryptomenami.

V prvom rade sa vzťahuje na kryptomeny a obchodovanie s nimi Anti Money Laundering Regime (AMLR), teda regulácia proti praniu špinavých peňazí. Sem spadá napríklad overovanie identity používateľov kryptomenových búrz. To znamená, že nemôžete anonymne obchodovať na kryptomenových burzách, prípadne môžete obchodovať len malé sumy. Oblasť AMLR patrí pod Financial Crimes Enforcement Network (FCEN), a legislatíva sa týka všetkých inštitúcií, ktoré poskytujú zámenu kryptomien.

Ďalšou organizáciou je Securities and Exchange Commission (SEC), ktorá reguluje finančný trh, presnejšie burzy a obchodovanie s cennými papiermi. Pri súčasnom znení zákona považuje SEC všetky kryptomeny za cenné papiere až dovtedy, kým vývojári danej kryptomeny nepreukážu odlišné vlastnosti danej kryptomeny. Z toho dôvodu burzy a zmenárne podliehajú pod právomoci SEC a musia spĺňať nimi požadované regulácie.

Commodity Futures Trading Commision (CFTC) je organizácia, ktorá sa venuje burzovým či neburzovým derivátovým obchodom. Pod CFTC spadajú všetci, ktorí poskytujú nejaký typ derivátov napojených na kryptomeny. V súčasnosti napríklad burzy ako Chicago Board Options Exchange (CBOE) alebo Chicago Mercantile Exchange Group (CME Group). Obe obchodujú Bitcoin futures kontrakty.

Poslednou organizáciou, ktorej právomoc sa týka aj kryptomien, je Internal Revenue Service (IRS). Organizácia spravuje daňový systém Spojených štátov amerických. V roku 2014 IRS

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

vydala stanovisko ku kryptomenám, kde kryptomeny považuje za majetok. V tom zmysle sa zdaňuje kapitálový výnos z transakcie alebo predaja kryptomien. A to môže byť predaj z kryptomeny na FIAT alebo z kryptomeny na inú kryptomenu.

6.4.2. Regulácia kryptomien v Európskej únii

V rámci EÚ panuje zhoda len čo sa týka dane z pridanej hodnoty (DPH) a dane z príjmu, v rámci ktorej je Bitcoin vyňatý. O DPH rozhodol v minulosti Európsky súdny dvor. Existujú dva prípady, kedy sú kryptomeny od DPH oslobodené. Prvý prípad sa týka kryptomenových búrz. V prípade, že sa poskytuje zámena kryptomien či FIAT-u, tak sú tieto transakcie považované za službu za odplatu.[114] Druhý prípad sa týka ťažby kryptomien. V tomto prípade nebolo dokázané spojenie medzi službou a odplatou. To znamená medzi vyťažením kryptomeny a ťažením kryptomeny.[115]

V ostatných oblastiach, tak ako aj v Spojených štátoch amerických, ani v Európe nie je zhoda v oblasti kryptomien. Prvou legislatívou, ktorá sa týkala kryptomien, bola štvrtá smernica Anti Money Laundering Directive (AMLD). Smernica sa týka hlavne zmenární, teda kryptomenových búrz a iných služieb. Rovnako aj peňaženiek. V rámci smernice sú tieto platformy povinné mať politiky a postupy, ktoré zabezpečia prevenciu a detekciu podozrivých operácií, ktoré by mohli byť spojené s praním špinavých peňazí či terorizmom.[116]

Európska komisia rovnako vydala akčný plán, ktorý sa venuje inováciám v oblasti finančných služieb na vytvorenie inovatívnejšieho a konkurencieschopnejšieho finančného trhu

---

[114] Tento prípad je možné súdne napadnúť, a to preto, že oslobodenie sa vzťahuje za transakcie, avšak väčšina činnosti na burze súvisí s obchodovaním za účelom zisku.

[115] Rovnako sa považuje za spornú oblasť. Dôvodom je existencia pool miningu. V tom prípade je výnos v určitej miere istý, pretože sa rozpočítava na počet členov a poskytnutý výpočtový výkon.

[116] Návrh bol predložený v júli 2016 a schválený koncom januára 2018.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

v Európskej únii. Okrem iného sú súčasťou tohto plánu aj finančné inovácie, inak nazývané Fintech. Do Fintechu patrí blockchain, umelá inteligencia (AI) a rôzne služby súvisiace s cloudami. Rovnako v tom čase bola založená platforma EU Blockchain Observatory and Forum. Do platformy sú zapojené členské štáty EÚ. Účelom platformy je sledovať trendy a kľúčové udalosti v rámci blockchainu.[117]

Členské štáty Európskej únie majú možnosť samé si regulovať ostatné oblasti v rámci kryptomien. To znamená, že každý členský štát pristupuje ku kryptomenám odlišným spôsobom.

6.4.3. Regulácia kryptomien v Číne[118]

Čínsky päťročný plán zverejnený v roku 2016 označil blockchain za „strategickú technológiu" a žiadal intenzívnejší výskum a vývoj v tejto oblasti. Čínsky prezident Xi Jinping vyzval k technickým inováciám v „novej generácii technológií predstavovanej umelou inteligenciou, kvantovými informáciami, mobilnou komunikáciou, internetom vecí a blockchainom."

Ministerstvo obchodu navrhlo riešenia založené na blockchaine v rôznych oblastiach od podávania správ o úveroch a riadení dodávateľského reťazca, cez elektronický obchod a finančný priemysel. Napríklad, daňový úrad skúma pilotný projekt, ktorý by za účelom overenia platby vkladal daňové doklady na blockchain. Na druhej strane sa na kryptomeny nazerá negatívne a predpokladá sa, že by mohli spôsobiť finančnú či sociálnu nestabilitu.

Čínska regulácia kryptomien, konkrétne Bitcoinu, existuje od roku 2013, kedy vyšlo Oznámenie o prevencii Bitcoinových rizík.

---

[117] Akčný plán bol publikovaný v marci 2018

[118] Viac informácií na: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/china

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Účelom tohto oznámenia je znížiť riziko vo finančnom sektore, a to tým, že „Bitcoin“ sa nepovažuje za „menu“, keďže existuje iba jedna oficiálna mena Renminbi.

V oznámení sa ďalej uvádza, že finančné a platobné inštitúcie nemôžu používať Bitcoin na vyjadrenie ceny za výrobky alebo služby, kupovať ho a ani predávať. Rovnako nemôžu obchodovať s Bitcoinami na burze, uzatvárať poistenie súvisiace s Bitcoinom, priamo alebo nepriamo poskytovať ďalšie služby súvisiace s Bitcoinami, vrátane obchodovania, zúčtovania či platobného vyrovnania.

Táto reštrikcia vznikla z dôvodu, že Bitcoin sa považuje za prostriedok na pranie špinavých peňazí, obchodovanie s drogami, pašovanie, nezákonné získavanie finančných prostriedkov a iné nezákonné a trestné činnosti. Zároveň sa predpokladá, že niektorí používatelia kryptomien môžu byť jednoducho špekulanti alebo malí investori a môžu byť nevzdelaní, pokiaľ ide o riziká spojené s využívaním kryptomien ako investície.

V prvej polovici roku 2017 dosiahli kryptomeny vrchol v popularite, a to aj v rámci Číny v prípade Initial Coin Offering (ICO). V prvej polovici roku 2017 bolo viac ako 65 ICO, pričom podľa odhadov čínski investori v prvej polovici toho roku investovali najmenej 2,6 miliardy RMB (takmer 400 miliónov USD). To spôsobilo dvojaké riziká. A to nekontrolovateľný únik kapitálu z Číny a hrozbu hospodárskej destabilizácie zo strany neskúsených maloobchodných investorov, ktorí stratili značné sumy peňazí v špekulatívnych ICO, ktoré boli často podvodom.

V septembri 2017 čínske úrady zakročili, a to so Správou o prevencii rizík ICO. V Správe sa zakazuje všetka činnosť ICO v Číne ako neoprávnené a nezákonné verejné získavanie finančných prostriedkov. Správou sa tiež všetky zámeny kryptomien v Číne stávajú nezákonnými. Žiadna z takzvaných tokenových finančných a obchodných platforiem sa nemôže zapojiť do výmenných služieb medzi akýmkoľvek zákonným platidlom a tokenmi alebo medzi virtuálnymi menami, ani sa nesmie zapojiť do predaja tokenov alebo virtuálnych mien pre seba alebo ako centrálna protistrana, alebo poskytovať nejaké služby s tým spojené.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Vo februári 2019 čínska Správa pre kybernetickú bezpečnosť implementovala Reguláciu správy blokchainovych informačných služieb (Blockchain Information Service Management Regulations; BISMR), ktorými sa ustanovil právny rámec na prevádzkovanie podnikania založeného na blockchaine.

Podľa BISMR sa podniky poskytujúce služby založené na blockchaine musia registrovať u regulátorov a musia vlastniť skutočné mená a totožnosť ich používateľov. Spoločnosti, ktoré majú založené podnikanie na blockchaine, sú povinné monitorovať používanie blockchainu na nezákonné účely, zastaviť nezákonné používanie, odstrániť nezákonný obsah, nahlásiť nezákonné činnosti orgánom a na požiadanie im poskytnúť záznamy.

Regulácia predaja kryptomien

Všeobecne platí, že prenos Bitcoinov, kryptomien alebo tokenov medzi dvoma súkromnými osobami nie je nezákonný a nie je osobitne regulovaný. Napríklad individuálny vlastník Bitcoinu (BTC) sa môže dohodnúť s vlastníkom Ripple (XRP) na prevode určitého množstva BTC na vlastníka Ripple výmenou za vopred dohodnutú hodnotu RMB alebo za dohodnutú hodnotu XRP.

Tu treba zdôrazniť, že kryptomena sa nemá používať na platenie ako náhrada národnej meny. To znamená, že je nezákonné predajcovi jabĺk zaplatiť v Bitcoine miesto RMB.

Zdanenie

V súčasnosti neexistujú žiadne osobitné daňové zákony alebo nariadenia, ktoré by sa vzťahovali na kryptomeny, čím tvoria šedú zónu ekonomiky. Za normálnych okolností by daňový úrad neváhal uvaliť dane na akýkoľvek druh príjmu. Kryptomeny sú však v ojedinelej situácii, pretože banky a finančné inštitúcie majú zakázané ponúkať služby súvisiace s kryptomenami, ako aj výmenu kryptomien. Daňový úrad Číny nemá kapacitu ani infraštruktúru na monitorovanie výnosov z obchodovania s kryptomenami.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Zákaz prevodu peňazí do zahraničia

Čína vykonáva prísne kontroly kapitálu zamerané na obmedzenie množstva odlivu kapitálu z Číny do iných krajín prostredníctvom devíz. Jednotlivci majú obmedzenie na prepravu alebo odosielanie až do 50 000 dolárov mimo Číny za rok, prevody firiem do zahraničia sú dôkladne preskúmané a musia spĺňať súhlas Čínskej štátnej správy devíz. Pri kryptomenách hrozí destabilizácia tohto systému kontroly kapitálu tým, že sa jednotlivcom umožní prevod peňazí do zahraničia. Každé použitie kryptomeny na prevod viac ako 50 000 dolárov na hlavu z územia Číny sa bude pravdepodobne považovať za porušenie individuálnych obmedzení devízových prevodov.

6.4.4. Regulácia kryptomien v Singapure[119]

Singapur sa bežne označuje ako jeden z rajov pre kryptomeny, najmä vďaka vyváženému právnemu a regulačnému režimu, ktorý podporuje Singapurská menová autorita (Monetary Authority of Singapore - MAS). Prístupom MAS, ktorý je centrálnou bankou a regulátorom finančného trhu, je regulovať finančný trh, ale len v takej miere, aby to neprekážalo inováciám.

Vláda legislatívne nedefinovala virtuálnu menu (používa sa zameniteľne s „kryptomena“ alebo „token“ alebo „minca“, pokiaľ nie je uvedené inak), namiesto toho definícia obsahuje viacero možností:

- nejde o menu alebo legálnu ponuku vydanú niektorou z vlád
- je ako prostriedok platby za tovar alebo služby niekomu, kto je ochotný ju prijať ako spôsob platby, a je prostriedkom na vykonávanie platieb
- je vykázaná ako majetok a osobný majetok, pričom s ňou obchoduje čoraz viac ľudí.

[119] Viac informácií na: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/singapore

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Vláda podporuje najmä rozvoj technológie blockchain, ale tvrdí, že tento pozitívny postoj neznamená, že nevyhnutne podporuje kryptomeny. Podľa vlády nie sú kryptomeny jedinou aplikáciou technológie blockchain. Vláda okrem iného pracuje aj na tzv. projekte Ubin.

Projekt Ubin, ktorý je podporovaný MAS, je zameraný na vytvorenie digitálneho tokenu, teda singapurského dolára na blockchaine kryptomeny Ethereum. Každý token je krytý ekvivalentným množstvom singapurských dolárov, ktoré vlastní vláda, tak by nemal mať token vplyv na celkovú ponuku peňazí. Zámerom projektu je zlacniť a zefektívniť finančné transakcie.

Samotná virtuálna mena nie je v Singapure regulovaná. Okolnosti a činnosti spojené s virtuálnou menou určujú, či bude regulovaná podľa zákona o cenných papieroch alebo podľa iných právnych predpisov.

Pri analýze charakteru tokenu je kľúčovým rozdielom v porovnaní s ostatnými jurisdikciami to, že sa nebude považovať automaticky za bezpečný. Namiesto toho sa vyžaduje hĺbková analýza, či spadá do rámca zákona o cenných papieroch. Keď áno, tak z toho následne plynú ostatné zákonné požiadavky.

ICO ako cenné papiere

Niektoré tokeny sa môžu podobať cenným papierom a preto je na mieste otázka, či sa na ICO vzťahujú singapurské právne predpisy o cenných papieroch. Dôsledky sú dôležité, pretože existujú ďalšie zákony a nariadenia, upravujúce vydávanie cenných papierov pre verejnosť, ako napríklad registrácia prospektu. V konečnom dôsledku sa môže ICO predražiť a zároveň bude administratívne náročnejšie.

Ponuku alebo vydanie digitálnych tokenov v Singapure reguluje MAS, ak digitálne tokeny predstavujú produkty regulované podľa zákona o cenných papieroch.

Regulácia predaja virtuálnych mien

Predaj virtuálnych mien môže nastať prostredníctvom:

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- Súkromného predaja – Môže k tomu dôjsť pred ICO alebo v rámci predaja a nákupu v kontexte novo vytvoreného tokenu. Spravidla ide o súkromné dohody. Ak sa však token považuje za cenný papier v rámci SFA, je potrebné požiadať o licencie.
- ICO – Niektoré tokeny sa môžu podobať cenným papierom a preto je na mieste otázka, či sa na ICO vzťahujú predpisy v rámci regulácie cenných papierov. Pre vývojárov to je dôležitá otázka, pretože existujú ďalšie zákony a nariadenia upravujúce vydávanie cenných papierov pre verejnosť, ako napríklad registrácia prospektu. V konečnom dôsledku sa môže ICO predražiť a zároveň bude administratívne náročnejšie. Ponuku alebo vydanie digitálnych tokenov v Singapure reguluje MAS ak tokeny spadajú pod zákon o cenných papieroch.
- Obchodovaním – Neexistujú žiadne predpisy pre malých investorov, ktoré by osobitne upravovali obchodovanie s kryptomenami. MAS napriek tomu vydal vyhlásenie, v ktorom odporúča verejnosti, aby konala s mimoriadnou opatrnosťou, ak sa rozhodne niekto investovať do kryptomien.

Zdanenie

Príjmy za tovar alebo služby využívajúce virtuálne meny – Podniky, ktoré sa rozhodnú akceptovať virtuálne meny ako protihodnotu za tovar alebo služby, podliehajú bežným pravidlám podľa zákona o dani z príjmov. Napríklad, ak podnik akceptuje platbu v Bitcoine, bude sa to považovať za to isté ako keby akceptoval národnú menu.

Daň z kapitálových výnosov

V Singapure neexistujú dane z kapitálových výnosov, a preto tieto zisky nepodliehajú dani. Jednotlivci alebo podniky, ktoré nakupujú a predávajú virtuálne meny v rámci svojej bežnej činnosti ,sa však zdaňujú zo zisku získaného z obchodovania s virtuálnou menou. Zisky získané podnikmi, ktoré ťažia a obchodujú s virtuálnymi menami výmenou za peniaze podliehajú dani, pretože sa to považuje za príjem. To, či zisky z obchodovania virtuálnych mien podliehajú dani

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

z kapitálových výnosov, závisí od skutočností a okolností každého prípadu. Pri určovaní, či sú zisky zdaniteľné, sa berú do úvahy faktory ako účel, frekvencia transakcií a obdobie držby.

Daň z výnosov pri ICO

V súčasnej legislatívnej podobe je to nejasné. Podľa dohody je v Singapure príjem zdaniteľný ak:

- je zhromaždený v rámci Singapuru alebo získaný zo Singapuru
- ak ide o príjem pochádzajúci zo zahraničia, ale smeruje do Singapuru. Situácia v bode, v ktorom sa uvádza, že príjmy z obchodovania, alebo podnikania vykonávané daňovníkom sú zdaniteľné (pretože subjekt, ktorý sa obvykle používa na ICO, je registrovaný v Singapure - daňový poplatník). Keďže situácia stále nie je jasná, niektorí daňovníci preto považujú príjem pochádzajúci mimo Singapuru (t. j. v prípade, keď je kupujúci tokenov mimo Singapuru), za nepodliehajúci dani. Z tohto dôvodu niektoré podmienky ICO stanovujú, že Singapurčania nesmú kupovať tokeny.

Daň z tovaru a služieb pri predaji virtuálnych mien

Predaj kryptomien podlieha dani z pridanej hodnoty, a to podľa zákona o tovaroch a službách. Ak sa však predaj tokenov týka kupujúcich, ktorí nemajú žiadne spojenie so Singapurom, je možné to považovať za medzinárodné poskytovanie služieb, ktoré má podľa zákona nulovú daňovú sadzbu. Súčasná sadzba dane z pridanej hodnoty je 7 %. Očakáva sa, že sa zvýši na 9 % v období medzi 2021 a 2025.

Ťažba

V súčasnosti v Singapure neexistujú žiadne predpisy, ktoré by špecificky upravovali ťažbu kryptomien. Zisky získané ťažiarmi, ktorí ťažia a následne kryptomeny predávajú, podliehajú dani. Súčasná sadzba podnikovej dane je 17 % zo zisku. Keďže ťažba sa považuje za prácu, pri

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

cudzincovi je potrebné pracovné povolenie, aby mohol pracovať v Singapure. Podniky, ktoré zamestnávajú baníkov, musia navyše dodržiavať zákony týkajúce sa zákonníka práce.

6.4.5. Regulácia kryptomien vo Švajčiarsku a na Malte

Švajčiarsko a Malta sa označujú za krajiny, ktoré majú legislatívu nastavenú priaznivo, a tým lákajú spoločnosti, ktoré podnikajú s kryptomenami.

Vo Švajčiarsku v roku 2017 začal kantón Zug a municipalita Chiasso kantónu Ticino akceptovať platbu Bitcoinom za mestské služby či dane. Municipalita Zug je v súčasnosti označovaná ako Crypto valley, a to preto, že v kantóne množstvo spoločností z oblasti kryptomien sídli.

V roku 2018 vydal Švajčiarsky regulátor finančného trhu, Swiss Financial Market Supervisory Authority (FINMA), usmernenie k Initial Coin Offering (ICO). FINMA v rámci usmernenia delí tokeny na tri typy.

- Payment tokeny – slúžia na platenie. To znamená, že ich účelom je prenos hodnoty. Tokeny podliehajú regulácii, ktorá sa týka prania špinavých peňazí, či boja proti terorizmu.
- Utility tokeny – špeciálne tokeny, ktoré fungujú v rámci vnútorného ekosystému kryptomeny. Väčšinou slúžia na prístup ku konkrétnej službe, ktorá je v ponuke danej kryptomeny či projektu.
- Asset tokeny – reprezentujú pohľadávku alebo záväzok. Tieto tokeny sú zo strany FINMA posudzované rovnako ako cenné papiere, teda akcie alebo dlhopisy. Z toho vyplývajú aj legislatívne požiadavky ako v prípade cenných papierov.

Kryptoburzy a zmenárne spadajú pod Anti Money Laundering Act, z čoho plynú rôzne požiadavky. V rámci Švajčiarska je zisk z obchodovania s kryptomenami predmetom zdanenia,

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

avšak každý kantón za to zodpovedá samostatne. ICO, ktoré v budúcnosti garantujú výnos, sú tak povinné mať bankovú licenciu.

6.4.6. Situácia na Malte

Malta[120] je prvou krajinou, kde parlament schválil reguláciu kryptomien. Parlament schválil v júli 2018 tri návrhy zákona s vplyvom na kryptomeny:

1. Malta Digital Innovation Authority Act – zriaďuje úrad, ktorého úlohou je monitorovať trh firiem, ktoré podnikajú v oblasti kryptomien. Následne je úlohou úradu certifikovať vyvinutý softvér zo strany spoločností a zabezpečiť tak transparentnosť. Certifikát poskytuje používateľom softvérov istotu, či už z právneho alebo technologického hľadiska. V súčasnosti je riaditeľom Stephen McCarthy.

2. Innovative Technological Arrangement and Services Act – zákon stanovuje rámec v ktorom môžu fungovať Innovative Technology Arrangements (technologické dohody) a Services (ITAS; služby) týkajúce sa kryptomien či blockchain technológií. Tie sú vymáhané vyššie spomínaným úradom. Zákon zároveň stanovuje podmienky certifikácie a auditu napríklad inteligentných zmlúv, kryptomenových búrz či decentralizovaných autonómnych organizácií.

3. Virtual Financial Asset Act (VFA) – Slúži ako právny rámec pre regulátorov a stanovuje podmienky, ako majú narábať s poskytovateľmi peňaženiek, burzami, či inými službami spojenými s kryptomenami. Zároveň stanovuje, ako majú regulačné orgány nahliadať na STO či ICO a čo je potrebné od nich na začiatku fungovania projektu vyžadovať.

---

[120] Viac informácií na: https://www.welcome-center-malta.com/blockchain-services-in-malta/ico-crypto-regulation-in-malta/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Malta zároveň zaviedla štyri typy licencií podľa úrovne kompetencií.

1. Držitelia licencie prvého stupňa môžu prijímať alebo posielať obchodné príkazy, poskytovať investičné poradenstvo v súvislosti s virtuálnymi finančnými aktívami (virtual financial assets) a rovnako umiestňovať tieto aktíva.

2. Držitelia licencie druhého stupňa môžu okrem predošlého zároveň spravovať klientove peniaze, avšak nemôžu ovládať burzu alebo obchodovať na vlastný účet.

3. Držitelia licencie tretieho stupňa môžu robiť to, čo držitelia licencie druhého stupňa, avšak nemôžu ovládať burzu.

4. Držitelia licencie štvrtého stupňa môžu ovládať burzu a zároveň spravovať privátne kľúče jej používateľov. V princípe môžu vykonávať činnosti spojené s prevádzkou kryptomenovej burzy.

Poplatky súvisiace s jednotlivými licenciami uvádzame nižšie v nasledujúcej tabuľke.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tabuľka 8: Licenčné poplatky podľa úrovne kompetencií

Druh poplatku	Prvý stupeň licencie	Druhý stupeň licencie	Tretí stupeň licencie	Štvrtý stupeň licencie
Za vydanie	3 000 eur	5 000 eur	7 000 eur	12 000 eur
Za dohľad (ročný)	2 750 eur (za tržby do výšky 50 000 eur)	4 500 eur (za tržby do výšky 250 000 eur)	6 000 eur (za tržby do výšky 250 000 eur)	25 000 eur (za tržby do výšky 1 mil. eur)
Za tranžu	350 eur (v objeme od 50-tis do 1 mil. eur)	400 eur (v objeme od 250-tis do 5 mil. eur)	400 eur (v objeme od 250-tis do 50 mil. eur)	2 500 eur (v objeme od 1 mil. do 1 mld. eur)

Zdroj:Vlastné spracovanie

6.4.7. Regulácia kryptomien na Slovensku

V roku 2018 bolo na Slovensku novelizovaných niekoľko zákonov, ktoré upravujú obchodovanie a zdaňovanie kryptomien a rovnako narábanie s nimi v rámci účtovníctva.

Začiatkom októbra 2018 vstúpila do platnosti novela zákona č. 213/2018 Z. z. o dani z poistenia a o zmene a doplnení niektorých zákonov, v ktorej sa ustanovujú aj zmeny zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov a jeho doplnenie o oceňovanie virtuálnej meny reálnou hodnotou. Novela upravuje aj zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, v ktorom tiež zakotvuje pojmy týkajúce sa kryptomien a spôsobu ich zdaňovania.

Podľa Metodického usmernenia je kryptomena: „digitálny nositeľ hodnoty, ktorý nie je vydaný ani garantovaný centrálnou bankou ani orgánom verejnej moci, ani nie je nevyhnutne

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

naviazaný na zákonné platidlo a nemá právny status meny, resp. peňazí, avšak je akceptovaný niektorými fyzickými alebo právnickými osobami ako platobný prostriedok a ktorý je možné prevádzať, uchovávať alebo s ním elektronicky obchodovať.“

Zároveň sa kryptomeny nepovažujú legislatívne za elektronické peniaze, keďže elektronické peniaze sa len uchovávajú elektronicky. Medzi elektronické peniaze alebo nosiče sa zaraďujú kreditné a debetné karty.

Zdaňovanie na Slovensku

Príjem, ktorý plynie z predaja virtuálnej meny, sa považuje za predmet dane. To znamená, že je považovaný za zdaniteľný príjem. Za predaj kryptomeny sa považuje výmena virtuálnej meny za majetok, alebo výmena za inú virtuálnu menu, národnú menu či za poskytované služby.

Zjednodušene to znamená, že zdaniteľný príjem je zisk z predaja kryptomeny pri výmene za službu, národnú menu, alebo za inú virtuálnu menu. V prípade, keď vlastník kryptomeny ju len drží vo svojej peňaženke a nevykonáva žiadne transakcie, tak k zdaňovaniu nedochádza. Daňovníkom je podnikateľ a rovnako aj nepodnikateľ.

V prípade ťaženia kryptomien podnikateľom či nepodnikateľom, ktorý si nakúpi potrebné zariadenia na to, aby sa mohol podieľať na ťažbe, rovnako platí, že príjem sa zdaňuje až v momente zámeny. A to či už na inú virtuálnu menu, národnú menu, majetok, či výmenou za službu. Príjem sa v tomto prípade zahŕňa do základu dane v zdaňovacom období realizácie predaja tej ktorej kryptomeny. V prípade nadobudnutia kryptomeny formou mzdy či platbou za tovar sa považuje takéto nadobudnutie za zdaniteľný príjem podobne ako v eurách.

V prípade virtuálnych mien si môže daňovník znížiť zdaniteľné príjmy o preukázateľné vynaložené výdavky na dosiahnutie tohto typu príjmov. Dôležité je poznamenať, že si ich môže

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

priznať len do výšky zdaniteľného príjmu. To znamená, že nemôže dosiahnuť daňovú stratu. V tomto prípade sa neprihliada o ktorý typ kryptomeny išlo a berie sa do úvahy úhrn ako celok.

V prípade fyzických osôb, ak je základ dane daňovníka nižší ako 35 268,06 €, tak sadzba dane z príjmov fyzickej osoby je 19 %. V prípade, že je väčší, tak sadzba dane je 25 %. Zároveň podlieha tento príjem aj zdravotnému poisteniu vo výške 14 %.

Pri právnickej osobe pri zisťovaní základu dane, resp. daňovej straty, daňovník vychádza z výsledku hospodárenia zisteného v účtovníctve alebo z rozdielu príjmov a výdavkov. Tento výsledok hospodárenia sa následne transformuje na základ dane prostredníctvom § 17 až § 29 zákona o dani z príjmov.

Miesto virtuálnych mien v právnom systéme SR

Podľa správy NBS[121] z augusta 2019, ktorá sa venuje aj virtuálnym menám, zatiaľ v žiadnej z krajín EÚ nebola zavedená regulácia, ktorá by sa venovala len tejto oblasti. Zároveň krajiny presne nedefinujú kryptomeny.

Podľa NBS skôr spadajú pod existujúcu formuláciu: „nehmotných predmetov majetkových práv, najčastejšie zhmotnených práv, na ktoré sa aplikuje režim ako na veci. Právna úprava niektorých krajín teda umožňuje zhmotnenie práv, pričom následne môžu byť predmetom vlastníctva a prevodu, resp. prechodu, tak ako v prípade iných typov osobného vlastníctva. Viaceré krajiny takisto uplatňujú na určité práva režim ako na veci, niektoré z týchto krajín však považujú za veci, ktoré možno vlastniť, iba hmotné predmety.“[122]

---

[121] Viac informácií na: https://www.nbs.sk/_img/Documents/_PUBLIK_NBS_FSR/Biatec/Rok2019/04-2019/biatec_04Aug_WEB.pdf?fbclid=IwAR2ENJhEBYKvLvuXniBGFe4YQkj1wtt7PjCYYLp0VcTxHSeXtILnKDEQqW8

[122] Tamtiež str. 3

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Podľa NBS: „Právna úprava Slovenskej republiky v tejto súvislosti ustanovuje, že predmetom občianskoprávnych vzťahov sú veci, živé zvieratá, a pokiaľ to ich povaha pripúšťa, práva alebo iné majetkové hodnoty.“[123] Aj keď definícia pojmu vec nie je ustanovená, tak právna teória a prax hovorí o veci v spojitosti s hmotným a ovládateľným predmetom. Z toho dôvodu nie je možné považovať kryptoaktíva za vec.

V súčasnosti nie sú v slovenskej legislatíve kryptoaktíva explicitne upravené a preto: „do úvahy prichádza ich kvalifikácia ako práv (nároky s nimi spojené môžu mať napríklad charakter pohľadávky) alebo iných majetkových hodnôt (keďže kryptoaktíva sú nositeľmi informácií a s nimi súvisiace aplikačné riešenia predstavujú databázy a algoritmy).“[124]

NBS zdôrazňuje, že ICO či STO, aj keď sa v niektorých prípadoch vlastnosťami podobajú na IPO či na trh cenných papierov, tak ich nemožno považovať za totožné. Zároveň aj kryptoburzy, kde sa následne kryptoaktíva obchodujú, nie sú v súčasnosti burzami cenných papierov, keďže nie sú robustne regulované podľa platného regulačného rámca MiFiD II. „V Slovenskej republike nie sú dohliadané príslušným orgánom zodpovedným za výkon dohľadu nad finančným trhom.“[125]

Napriek tomu môže byť prevádzkovateľ dohliadaný, ak poskytované služby majú presah na regulované finančné služby, ako napríklad platobné služby podľa PSD2. Napriek tomu jadro činnosti týchto platforiem nepodlieha regulačnému rámcu. Túto situáciu čiastočne zmení transpozícia piatej smernice o boji proti praniu špinavých peňazí (AMLD5) do právneho poriadku Slovenskej republiky.

---

[123] Tamtiež str. 3

[124] Tamtiež str. 3

[125] Tamtiež str. 4

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Z transpozície budú plynúť nové povinnosti: „povinnosť registrovať sa v zozname vedenom príslušným štátnym orgánom. Identickú povinnosť budú mať aj custodian wallet providers, t. j. prevádzkovatelia služieb správy (virtuálnych) peňaženiek. Zastávame názor, že uvedená povinnosť je odrazovým mostíkom pre nastavenie takých kontrolných mechanizmov v pôsobnosti štátu, ktoré umožnia identifikovanie a najmä predchádzanie aktivitám súvisiacim s legalizáciou príjmov z trestnej činnosti.“[126]

Podľa NBS sa diskusia o regulovaní kryptomien zintenzívnila po tom, čo Facebook oznámil svoj projekt Libra. Dovtedy kryptomeny neboli považované za systémové riziko pre finančné trhy. Na medzinárodnej úrovni nedošlo k dohode v oblasti regulácie, avšak NBS spomína, že niektoré krajiny zvolili jeden z nasledujúcich prístupov:

- „Uplatňovanie existujúcich regulačných rámcov, t. j. ich interpretácia vo vzťahu ku kryptoaktívam a s nimi spojeným aktivitám bez ďalšieho doplnenia týchto rámcov.
- Úprava existujúcich regulačných rámcov s cieľom pokryť novú podstatu kryptoaktív alebo nové aktivity, ktoré nie je možné pokryť súčasnými rámcami, a tak reagovať na nové riziká, ktoré kryptoaktíva prinášajú.
- Zavedenie nových osobitných regulácií – vytvorenie nových predpisov, osobitne upravujúcich kryptoaktíva a s nimi spojené aktivity.
- Zavedenie osobitných regulačných režimov – t. j. ustanovenie špeciálneho režimu pre FinTech aktivity a FinTech spoločnosti, ktorých kryptoaktíva a s nimi spojené aktivity sú podmnožinou, a tým vytvorenie špeciálneho režimu mimo štandardnej regulácie finančného trhu.“[127]

---

[126] Tamtiež str. 4

[127] Tamtiež str. 5

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Možná regulácia na Slovensku

Podľa NBS je regulácia kryptomien predmetom úvah aj na Slovensku už dlhší čas. Dôvodom je plynúca neistota firiem, ktoré chcú v tejto oblasti podnikať. Akčný plán digitálnej transformácie Slovenska 2019-2022 obsahuje aj úlohu analyzovať využiteľnosť tokenizácie aktív. V zmysle využitia tokenizácie ako nového kanálu na prílev finančných prostriedkov do reálnej ekonomiky.

Podľa NBS nie je zmysluplné vytvárať nový osobitný regulačný rámec. Podľa NBS by sa malo Slovensko zapájať do kreovania legislatívy na úrovni EÚ. Podľa NBS na úrovni EÚ sa definuje najmä terminológia a taxonómia. Naopak, očakáva sa, že EÚ určitú časť regulácie prenechá na členské štáty, aby si ju definovali samé. A to najmä v oblasti civilného práva či úpravy vlastníctva.

Podľa NBS delenie na spomínané payment, ulity a asset tokeny by sa malo zaviesť aj na Slovensku, a to preto, že toto delenie prebrali aj niektoré štáty z EÚ. Investičné tokeny by mali byť podľa NBS regulované podobne ako cenné papiere, a to z hľadiska ochrany investorov či pravidiel činnosti. Preto bude potrebné zmeniť zákon o cenných papieroch.

Zároveň by sa primárne mala regulovať aktivita na kryptomenovom trhu. To znamená primárny a sekundárny trh, tak ako to robí väčšina členských štátov. NBS zároveň poukazuje na potrebu zostavenia prospektu v rámci ICO aj pod hranicu 1 milióna eur. Práve v prípade akcií nie je potrebné zostavovať a zverejňovať prospekt, keď celkový objem verejnej ponuky je pod 1 milión eur. Zároveň centrálna banka poukazuje na to, že bude potrebné regulovať aj sprostredkovateľov, poradcov či brokerov na tomto trhu. Tu by sa rovnako mala využiť existujúca regulácia trhu cenných papierov.

V závere NBS spomína, že by sa kvôli decentralizovanej odlišnej evidencii investičných tokenov malo rozmýšľať aj o technologickom audite. NBS ako príklad uvádza právnu úpravu Malty, kde

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

boli upravené požiadavky na osoby vydávajúce tokeny a zároveň bol vytvorený aj osobitný orgán dohľadu, Malta Digital Innovation Authority. Na Slovensku by túto činnosť mohla zastrešovať NBS alebo novo vytvorený orgán dohľadu.

6.5. Zhrnutie

Napriek tomu, že sa vlády a štáty snažia zasahovať do šedej ekonomiky, ktorá vzniká prostredníctvom kryptomien, môžu to robiť len v obmedzenej miere. Vždy, keď uzatvoria jeden darknet, tak vzápätí vznikne iný. Na prvý pohľad by sa mohlo zdať, že kryptomeny sú nevyhnutnou súčasťou čiernych trhov, avšak opak je pravdou a len malé percento kryptomien sa využíva na nelegálnu činnosť.

Budúcnosť kryptomien bude závisieť aj od regulačného rámca. V súčasnosti na poli Európskej únie neexistuje jednotný rámec, ktorý by definoval a reguloval kryptomeny. Každý štát má reguláciu definovanú v inej miere, niektoré štáty viac reštriktívne, iné voľnejšie. Aj keď sú kryptomeny decentralizované a nezávislé od rozhodnutí napríklad politikov, tak stále do určitej miery môžu zlé či dobré rozhodnutia ovplyvniť používanie a záujem o kryptomeny.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

7. PRÍKLADY EXISTUJÚCICH A PLÁNOVANÝCH PROJEKTOV

V nasledujúcej kapitole uvádzame prehľad a príklady jednotlivých projektov privátneho, ako aj verejného sektora. Dôraz je kladený hlavne na už existujúce projekty, ale v niektorých prípadoch sa projekty nachádzajú v počiatočnej fáze vývoja, takže sa dajú považovať za plánované. Projektov implementujúcich blockchain technológiu je pomerne veľa. Mnohé z nich sú stále v štádiu vývoja a často neexistuje dostatok infromácií súvisiacich s implementáciou samotných technológií. Taktiež, mnoho blockchain projektov uvádza vo svojich marketingových materiáloch že využívajú blockchain, aj keď v skutočnosti to tak často krát nie je. Do tejto kategórie môžu často spadať aj projekty, ktoré vyvíjajú produkt za využitia klasických technológií a databáz s jediným rozdielom, že implementujú do svojho interného prostredia aplikácie kryptografický token. Tokenizáciu a jej rozdelenie sme analyzovali v kapitolách vyššie. V tejto kapitole sa teda sústreďujeme na využitie a aplikácie technológie blockchain, ktoré sa považujú vo všeobecnosti za overené.

7.1. Privátny sektor

Viacero aplikácií či protokolov ktoré analyzujeme v tejto kapitole sú často na rozmedzí privátneho a verejného sektora, resp. majú potenciálne dopad na obidva sektory. Napriek tomu sa snažíme rozdeliť projekty podľa týchto dvoch kategórií, a to typicky podľa toho, v ktorom odvetví majú potenciálne primárny dopad.

7.1.1. Stabilné kryptomeny

Volatilita kryptomien býva často kritizovaná nielen laickou verejnosťou, ale aj viacerými odborníkmi. Na trhu kryptomien v súčasnosti funguje už niekoľko rôznych kryptomien, ktoré technologicky fungujú ako ktorákoľvek decentralizovaná kryptomena, avšak s tým rozdielom, že ich hodnota je krytá reálnym aktívom, alebo košom aktív. Jedným z prvých takýchto

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

projektov bol napríklad Digix[128], ktorý kryl každý vydaný token jedným gramom zlata. Ďalším podobným projektom je Tether[129]. Tether je jedna z najznámejších kryptomien, nakoľko sa dlhodobo drží medzi najväčšími kryptomenami v rebríčku podľa trhovej kapitalizácie. Tether bol jednou z prvých kryptomien, ktoré boli naviazané na americký dolár. Napriek pomerne dlhotrvajúcemu obdobiu obáv, či firma naozaj disponuje dostatočnými rezervami na svojich bankových účtoch, sa Tether používa už niekoľko rokov na rôznych svetových burzách. Dá sa predpokladať že množstvo, ako aj celková trhová kapitalizácia stabilných a aktívami krytých kryptomien, bude rásť v čase aj naďalej.

V súčasnosti sa stále viac hovorí aj o vytváraní digitálnych mien národnými centrálnymi bankami. Vyvrcholením tohto trendu v roku 2019 bolo oznámenie o pláne vytvoriť národnú digitálnu menu Čínskou národnou bankou[130], ktorá oznámila, že spustí novú digitálnu menu už začiatkom roka 2020. Zatiaľ nie sú známe ešte technické detaily implementácie, ale je pravdepodobné, že národné banky v iných krajinách budú nasledovať tento trend a budeme vidieť obdobu národných mien v digitálnej forme na blockchaine čím ďalej tým viac.

Projekt Libra[131]

V júni roku 2019 bol oznámený projekt od sociálnej siete Facebook pod menom Libra. V tom čase boli zverejnené White paper, popis Libra Association, Libra Reserve a technická dokumentácia Libra blockchainu a k tomu zdrojový kód na webe GitHub, kde sa združujú vývojári z celého sveta.

---

[128] Viac informácií na: https://digix.global/dgd/
[129] Viac informácií na: https://tether.to/
[130] Viac informácií na: https://www.cnbc.com/2019/11/12/china-could-launch-digital-currency-in-next-2-3-months-investor-says.html
[131] Viac informácií na: https://www.alza.sk/libra-facebook >

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Projekt je spravovaný práve asociáciou Libra, ktorá sídli vo Švajčiarsku. Cieľom projektu je vytvoriť kryptomenu, ktorá bude stabilná, dostupná, s nízkou infláciou a hlavne dostupná na celom svete. Nejedná sa o kryptomenu ako Bitcoin alebo Litecoin či Ethereum, ale o Stablecoin, ktorý je naviazaný na určité aktíva.

Členmi Libra Association bolo zo začiatku 27 spoločností. Väčšina z nich boli známe spoločnosti z finančného sveta. Medzi nimi Visa, Mastecard, Uber, PayPal, Spotify, Vodafone, Lyft, Coinbase či Xapo alebo Coinbase. Ide primárne o spoločnosti, ktoré majú sídlo v Spojených štátoch Amerických.

Podmienkou členstva v asociácii je investícia vo výške 10 miliónov dolárov. Libra má za cieľ do jedného roka mať 100 členov a vyzbierať aspoň miliardu dolárov. Asociácia má hlavné slovo v rámci smerovania projektu. Aj keď je zdrojový kód na GitHub, tak pravdepodobne nebude môcť hocikto do neho prispievať. Zároveň asociácia rozhoduje o Libra Reserve. To je kôš aktív, ktoré predstavujú Libra coin.

Hodnota digitálnej meny Libra je viazaná na hodnotu koša aktív, ktorými je krytá. Prirovnať sa dá ku Špeciálnym právam čerpania (Special Drawning Rights), ktoré spravuje Medzinárodný menový fond (MMF). Libra bude krytá hlavne likvidnými aktívami, ktoré tam vložia členovia Libra Association. Presnejšie to budú aktíva ako dlhopisy či vklady. Stabilita Libry by mala byť porovnateľná s národnými menami. Členovia asociácie dostanú investičné tokeny, ktoré im budú generovať výnos z aktív (napríklad úrok zo štátnych dlhopisov).

Bežní používatelia sa ku Libre dostanú pravdepodobne prostredníctvom burzy Coinbase, ktorá je členom asociácie. Ambíciou, ktorá je spomínaná aj vo White paperi, je stať sa menou, ktorá bude prístupná aj ľudom bez bankového účtu, ktorí vlastnia mobilné telefóny. Takých je na svete podľa štatistík 1,7 miliardy.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Facebook by mal po spustení projektu integrovať peňaženku Calibra do svojich existujúcich služieb ako WhatsApp alebo Instagram. Facebook tak integruje E-commerce služby do svojich aplikácií, pričom z transakcií by si bral určité percento poplatkov.

Podľa kritikov nie je Libra tradičnou kryptomenou, a to preto, že jej blockchain nie je dostatočne decentralizovaný. O stave účtovnej knihy, teda prebehnutých transakcií budú rozhodovať len vopred určené strany a nebude to voľne prístupné každému, tak ako pri Bitcoine. Facebook deklaruje, že určitú centralizáciu udržiava kvôli tomu, aby transakcie mohli byť rýchlejšie potvrdzované, avšak v budúcnosti plánuje postupnú decentralizáciu.

Libra je predmetom kritiky aj kvôli obavám, či bude po spustení projektu zachovaná ochrana dát súvisiacich s transakciami užívateľov. Existujú obavy, najmä v súvislosti so škandálmi z rokov 2013 a 2015, že by dáta o platbách boli prepojené s identitou na Facebooku a následne zneužité. V prvom prípade sa jednalo o Snowdena, ktorý tvrdil, že Facebook sa zúčastňoval programu PRISM. V roku 2015 to je v súvislosti s analýzou dát Cambridge Analytica. Na popretie týchto obáv vytvoril Facebook spoločnosť Calibra.

Libra od svojho vzniku musí dokazovať pred regulátormi, že nebude zneužívať užívateľské dáta a že nebude ohrozením pre stabilitu menového systému. Nekončiace otázky od regulátorov v poslednom období znepokojili niektorých z asociácie. Partneri ako Mastercard, Visa, Ebay alebo PayPal či Stripe už z projektu vystúpili, avšak deklarovali, že sa časom môžu vrátiť.

7.1.2. Decentralizovaný finančný systém

Maker Dao a Dai

Dai je algoritmicky kontrolovaná stabilná kryptomena, ktorá je naviazaná na americký dolár. Mechanizmus peggingu je zabezpečený pomocou sady smart kontraktov, ako aj

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

decentralizovanou autonómnou organizáciou Maker DAO[132], ktorej členovia (držitelia MKR tokenu) majú právo a možnosť hlasovať o spravovaní, pravidlách, a podmienkach pri ktorých je možné emitovať Dai. Dai je v princípe emitovaný v rámci procesu pôžičiek, ktoré môže vykonať ktokoľvek, kto vloží do smart kontraktov kolaterál vo forme Etherov. Zaujímavosťou je, že od novembra 2019[133] je možné vkladať kolaterál aj vo forme iných kryptomien. Je nutné dodať, že technická náročnosť takéhoto procesu je pomerne vysoká, a teda je nepravdepodobné, že sa v blízkej budúcnosti tento spôsob pôžičiek rozšíri v rámci širokej verejnosti. Napriek tomu je objem kryptomeny Dai na trhu v novembri 2019[134] vo výške viac než 100 miliónov dolárov. Zároveň je nutné dodať, že chápanie mechanizmu pôžičiek a emitovania kryptomeny Dai nie je nevyhnutné k tomu, aby užívateľ mohol používať Dai ako akúkoľvek inú kryptomenu, keďže je obchodovateľná na trhu. Ktokoľvek, kto má kryptomenovú peňaženku kompatibilnú s Ethereum, môže vlastniť Dai. Z technologického hľadiska sa jedná o štandardný ERC-20 token, takže je pomerne ľahko integrovateľný naprieč rôznymi aplikáciami. Mechanizmus pegu je dosiahnutý vďaka systému, ktorý poskytuje motiváciu pre účastníkov voľného trhu na udržiavanie viazanosti cenovej hladiny na americký dolár. Celý systém tak funguje bez centrálnej autority, ktorá by tento kurz musela udržiavať pomocou monetárnych operácií. Dá sa povedať, že rola „centrálnej banky“ je v tomto prípade distribuovaná medzi Maker DAO, a teda držiteľov MKR tokenov. Napriek tomu, že výmenný kurz Dai sa mierne mení v čase v rozmedzí pár centov, osciluje okolo hranice jedného dolára, a teda jedna jednotka kryptomeny Dai sa efektívne rovná hodnote jedného dolára. Členovia Maker DAO taktiež rozhodujú o „úrokovej miere“, teda výške poplatku za sprostredkovanie pôžičky Dai. Tento poplatok je platený vo forme MKR tokenu.

---

[132] Viac informácií na: https://makerdao.com/en/whitepaper/#overview-of-the-dai-stablecoin-system

[133] Viac informácií na: https://www.coindesk.com/makerdaos-multi-collateral-dai-token-is-launching-nov-18

[134] Viac informácií na: https://coinmarketcap.com/currencies/dai/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Celý mechanizmus emitovania Dai je pomerne komplexný a technologicky náročný proces. V prvom rade je nevyhnutné vykonať obalenie (z angl. wrapping) Etheru. Toto má za následok, že Ether získa funkcionalitu štandardného ERC-20 tokenu označeného ako WETH. Následne treba WETH token konvertovať na PETH token (z angl. Pooled Ether), čo v princípe znamená, že obalený Ether sa vloží do fondu Etherov, ktoré tvoria kolaterál pre pôžičky Dai. Pomocou PETH tokenu sa následne dá vytvoriť CDP (Collateralized Debt Position), ktoré uzamkne PETH v smart kontrakte a umožňuje vytlačenie nových jednotiek kryptomeny Dai. Vytlačením Daiu sa užívateľovi zvyšuje pomer dlhu v rámci CDP. Nový Dai môže byť vytlačený len do výšky 60 % z hodnoty kolaterálu vo forme PETH tokenov (ktoré sa hodnotou rovnajú Etheru). V momente, kedy je nový Dai vytlačený, môže sa používať či obchodovať rovnako ako akýkoľvek iný ERC-20 token.

Ako sme spomenuli vyššie, väčšina užívateľov nebude podstupovať tento technicky náročný proces. Avšak, z hľadiska užívateľov, ktorí tak vykonajú, existuje niekoľko dôvodov prečo tak môžu robiť. Prvým z nich je potreba pôžičky ako takej. Pre užívateľov, ktorí majú určitý kapitál vo forme Etheru, ktorý nechcú predávať za eurá či doláre, je pôžička vo forme Dai veľmi dobrým riešením, nakoľko nemusia Ether predávať, ale ho len vložia ako kolaterál do smart kontraktu. Druhým dôvodom môže byť, že veria, že Ether porastie na hodnote a chcú nakúpiť Ethery na páku. Ether, ktorý majú, vložia do smart kontraktov a vytlačia nové Dai tokeny. Tie následne zamenia na burze za eurá, ktoré potom investujú opäť do Etheru. Je nutné dodať, že celý tento proces môže fungovať bez účasti tretích strán či finančných prostredníkov. Tretí dôvod môže byť daný samotným mechanizmom pegu, ktorý ráta s trhovými silami. Ak nastane situácia, že dopyt po Dai tokene dvíha jeho cenu nad úroveň jedného dolára, užívateľ má ekonomickú motiváciu vytvoriť Dai tokeny a okamžite ich predať na burze so ziskom. Jednoducho povedané, ak je trhová cena Dai nad úrovňou jedného dolára, účastníci trhu majú motiváciu vytvárať viacej tokenov Dai, a teda zvyšovať jeho zásobu a ponuku na trhu. Toto prispieva k nájdeniu rovnováhy na trhu. Naopak, ak trhová hodnota Dai klesá pod úroveň jedného dolára, užívatelia, ktorí majú pôžičky, majú šancu splatiť ich dlh lacnejšie. Toto je dané

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

tým, že ich dlh je denominovaný v Dai tokenoch. Ak napríklad klesne cena Dai na 99 centov, dlžníci majú možnosť splatiť pôžičku s 1 % zľavou a ušetriť tak. Splatením pôžičky sa zároveň spália Dai tokeny, ktoré si užívateľ požičal, a teda klesne ich zásoba ako aj ponuka na trhu. To opäť napomáha k vyrovnaniu cenovej hladiny na úroveň jedného dolára. Týmto spôsobom je zachovaný peg mechanizmus na americký dolár. Dai funguje od začiatku roka 2018, a tento systém sa ukázal byť odolný aj voči obrovským prepadom ceny Etheru ako aj celého trhu počas roku 2018.

Proces získania pôžičky vo forme stabilnej kryptomeny Dai z pohľadu užívateľa[135]:

1. Vloženie kryptomeny Ether do kryptomenovej peňaženky (napr. Metamask).

2. Vykonanie tzv. obalenia Etherov a vytvorenie tokenu WETH.

3. Výmena WETH za PETH (Pooled Ether).

4. Vytvorenie CDP(z angl. Collateralised Debt Position), ktoré reprezentuje samotnú pôžičku.

5. Uzamknutie kolaterálu vo forme PETH.

6. Vytlačenie nových mincí Dai v maximálnej výške 60 % z uzamknutého kolaterálu.

7. Výmena kryptomeny Dai za Bitcoin, Ether či eurá alebo doláre prostredníctvom búrz.

Proces platenia pôžičky vo forme kryptomeny Dai:

1. Získanie tokenu MKR na burze (napr. Oasis DEX).

---

[135] Viac informácií na: https://blockonomi.com/how-to-take-out-a-loan-with-maker-dai/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2. Vrátenie kryptomeny Dai do smart kontraktu a splatenie poplatku za pôžičku v tokene MKR.

3. Zrušenie pôžičky CDP.

4. Odomknutie PETH a získanie Etherov.

5. Výmena PETH za WETH.

6. Odbalenie WETH a konverzia na ETH.

0x/AirSwap – 0x[136] ako aj Airswap[137] sú protokoly vo forme smart kontraktov, fungujúce ako decentralizované burzy. Vývojári ich môžu implementovať do svojich decentralizovaných aplikácií, ktoré tak môžu fungovať ako užívateľské rozhranie pre prístup k týmto protokolom.

Augur/Gnosis – Augur[138] aj Gnosis[139] sú dva najznámejšie decentralizované predikčné trhy, ktoré umožňujú vytváranie stávok na akékoľvek udalosti v rámci, ale aj nad rámec politického, spoločenského či športového spektra. Ktokoľvek taktiež môže participovať na týchto stávkach a realizovať monetárny benefit, ak dokáže predpovedať udalosti správne. Celá mechanika stávok a odmeňovania je maximálne transparentná, nakoľko je realizovaná cez smart kontrakty.

Dy/dx – Dy/dx[140] je algoritmus fungujúci ako smart kontrakt na Ethereum sieti, ktorý podobne ako 0x protokol umožňuje obchodovanie aktív v decentralizovanej forme. Na rozdiel od

---

[136] Viac informácií na: https://0x.org/

[137] Viac informácií na: https://www.airswap.io/

[138]Viac informácií na: https://www.augur.net/

[139]Viac informácií na: https://gnosis.io/

[140] Viac informácií na: https://gnosis.io/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

decentralizovaných búrz poskytuje aj možnosť vytvárania finančných derivátov v podobe štandardných ERC-20 tokenov.

{Set} Protocol – {Set}Protocol[141] poskytuje možnosť vytvárať deriváty vo forme kolateralizovaných košov, skladajúcich sa z akýchkoľvek tokenizovaných aktív v podobe ERC-20 tokenov.

Uniswap – Uniswap[142] je jeden z najpoužívanejších smart kontraktov poskytujúcich funkcionalitu decentralizovanej burzy. Na rozdiel od 0x protokolu či AirSwapu, žiaden nemá vlastný token.

Dharma – Dharma[143] je protokol, ktorý umožňuje tokenizáciu dlhových inštrumentov vo forme ERC-20 tokenov bez toho, aby bola v celom procese zahrnutá tretia strana vo forme inštitúcie.

7.1.3. Logistika - Tradelens

Prvým významným projektom, ktorý implementoval blockchain na účely sledovania tovaru v rámci logistických reťazcov bol Tradelens, ktorý v marci roku 2017 dodalo IBM pre prvotného objednávateľa, spoločnosť Maersk, jedného z najväčších prevádzkovateľov lodnej dopravy[144]. Maersk sa tak stal prvým účastníkom tohto logistického blockchainu a taktiež prevádzkuje svoj vlastný uzol v sieti. Nakoľko je blockchain definovaný ako sieť uzlov, Tradelens sa ním skutočne stal až spustením o rok neskôr a príchodom ďalších 94 účastníkov (napr. ďalšie firmy lodnej, leteckej, cestnej dopravy, veľkoobchodu, colné úrady, bezpečnostné firmy), pričom väčšina

[141]Viac informácií na: https://www.tokensets.com/

[142]Viac informácií na: https://uniswap.io/

[143] Viac informácií na: https://www.dharma.io/

[144] Viac informácií na: https://www-03.ibm.com/press/us/en/pressrelease/51712.wss

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

týchto organizácií taktiež prevádzkuje vlastný uzol v sieti[145]. Dnes má Tradelens niekoľko sto účastníkov na čele s ďalšími dvoma lodnými prepravcami, švajčiarskou firmou Mediterranean Shipping Company (MSC) a francúzskou CMA-CGM, ktoré majú najväčší počet lodí a lodných kontajnerov na svete hneď po Maersk. Práve tieto kontajnery, ako aj ich obsah, sú teraz dohľadateľné na Tradelens blockchaine aj s „papierovou" stopou. Dokopy je tak zaznamenaná polovica celkového objemu kontajnerovej prepravy na svete.

TradeLens je digitálna platforma, ktorá umožňuje podnikom a organizáciám v dodávateľskom reťazci prístup k údajov o preprave, ktorý je transparentnejší a umožňuje efektívnejší svetový obchod. Systém sleduje produkt v reálnom čase a zaznamenáva jeho postup. Zároveň, údaje, ktoré sa ukladajú do blockchainu, sú taktiež šifrované. Tradelens umožňuje taktiež integráciu do rôznych aplikácií či platforiem, ktoré ponúkajú spoločnosti. Cieľom projektu je kompenzovať alebo úplne vyriešiť problémy, ako:

- Nejednotné údaje a nepresné zdieľanie informácií v dodávateľských reťazcoch.
- „Slepé miesta" organizácií, ktoré sa zúčastňujú dodávateľských procesov.
- Príliš veľa manuálnych, časovo náročných procesov, ktoré zvyšujú náklady a predlžujú dodávacie lehoty.
- Neefektívne postupy zúčtovania, ktoré sa zneužívajú na podvody.

Tradelens teda znižuje náklady na administratívu, presun a overovanie dokumentácie, zvyšuje transparentnosť presunu a evidencie kontajnerov a obsahu. Vytvára tak dôveru v predtým komplikovanej sieti častých aj zriedkavých obchodných stykov. Následne sa tak zvyšuje aj rýchlosť lodnej dopravy a dodávateľského reťazca. Platforma je škálovateľná pre budúce

[145]Viac informácií na: https://www.computerworld.com/article/3298522/ibm-maersk-launch-blockchain-based-shipping-platform-with-94-early-adopters.html

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

potreby či integrácie, nakoľko vlastnícke práva nemá jediná organizácia, ale celé konzorcium. Tieto benefity teda využívajú všetky účastnícke strany rovnako.

Z technologického hľadiska je Tradelens postavený na platforme Hyperledger Fabric, jedného z viacerých otvorených protokolov v rámci konzorcia Hyperledger[146], ktoré je spravované Linux Foundation[147], a zahŕňa stovky členských organizácií, ktoré sa podieľajú na vývoji otvorených protokolov.

Príklad využitie Tradelens v lodnej doprave

Ako vyzerá implementácia a využitie platformy Tradelens na konkrétnom príklade v lodnej doprave si ukážeme v nasledujúcej časti. Príklad realizácie bude pojednávať o distribúcií kvetov od pestovateľa a exportéra v Malajzii cez lodnú, až koncovú dopravu k predajcovi, importérovi v Nemecku.

Dianie tohto zjednodušeného príkladného procesu zahŕňa päť tranzitných bodov, či záznamov a tri kľúčové aspekty, finančné prevody a potrebné tlačivá:

1. Akreditív – list vyjadrenia dôvery exportérov.
2. Nákladný list – Dopravná inšpekcia
3. Rastlinolekársky Certifikát – po ktorom prebieha finančné vysporiadanie.

Tieto záznamy zaručujú decentralizovanú a sieťou autorizovanú a validovanú verziu pravdy, dostupnú všetkým dotknutým stranám. Validačné uzly sú u všetkých medzinárodných dopravcov, dotknutej Berlínskej banky a prístavnými úradmi miest Kelang a Hamburg. Ich výber a počet je založený na algoritme v závislosti od typu dopravy a obsahu. Tieto sú známe

[146] Viac informácií na: https://www.hyperledger.org/

[147] Viac informácií na: https://www.linuxfoundation.org/about/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

pred začiatkom procesu. Preto je ich počet, oproti verejným blockchainom, vymedzený na počet zmluvných a dotknutých strán.

Náhľad do informácií o predmete a procese je rovnomerne vymedzený pre všetkých účastníkov. Tými sú: realizujúci dopravca, Malajský pestovateľ, Berlínsky importér, ich Malajské a Berlínske banky, Berlínsky Colný Úrad a prístavné autority oboch strán.

Obrázok 12: Interface Tradelens aplikácie

Zdroj: IBM Research Youtube[148]

Proces začne, keď Berlínska banka vytvorí pre importéra a exportéra akreditívum, vyplnením v TradeFinance portáli, alebo z ich vlastného systému cez API. Tento dokument garantuje exportérom v budúcnosti vyplatenie importérom pred tým, než produkt-kvety odošle. Špecifikuje strany transakcie, objem a obsah a cenu. Už túto transakciu validujú spomenuté uzly. Akonáhle je validované akreditívum zhliadnuté všetkými stranami, je ich interakcia

[148]Viac informácií na: https://www.youtube.com/watch?v=r0LsnzAe1Yg

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

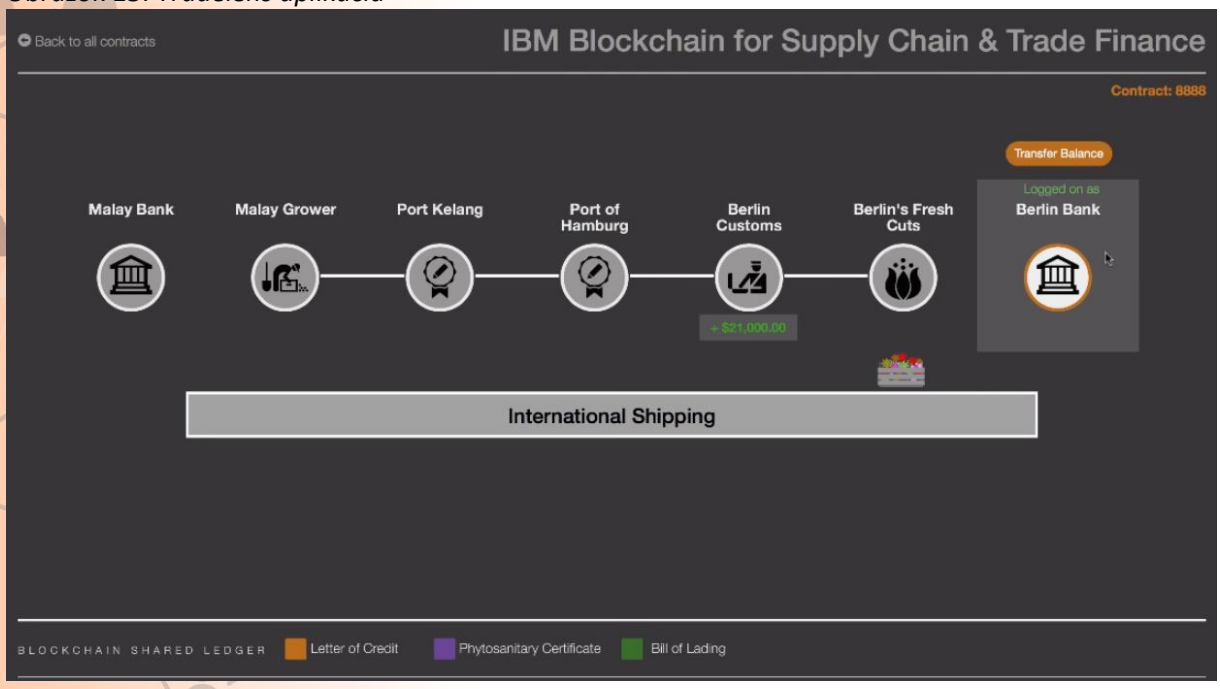
s dokumentom, v tomto prípade prečítanie, zaznamenaná do blockchainu. Keď je exportér-pestovateľ pripravený odovzdať obsah doprave, vytvorí auto-vyplňujúcu prihlášku pre Rastlinolekársky úrad na vytvorenie Rastlinolekárskeho certifikátu. Tu sa mimo blockchain deje aj fyzická kontrola úradmi. Výsledok daný úradom tvorí ďalšiu transakciu, ktorú validujú spomenuté uzly. Exportér, v tomto prípade malajský pestovateľ, vidí iba nutné informácie, ako napríklad kedy a či vôbec boli certifikáty udelené. Akreditíva sú vecou bánk a importéra, teda pokiaľ je táto transakcia validovaná blockchainom, exportér ich hlbšie detaily nevidí.

Následne sa kvety naložia do kontajnerov a dopravca vydáva nákladný list ako potvrdenie. Výsledok daný dopravcom tvorí ďalšiu transakciu, ktorú validujú spomenuté uzly. Autority Kelangského prístavu potvrdzujú spustenie dopravy a kontajnery sa nakladajú na loď, ktorá sa plaví do Hamburgu. Autority Hamburgského prístavu potvrdzujú prijatie kontajnerov. Berlínske Colné úrady vykonajú inšpekciu kontajnerov. Po úspešnej inšpekcii, vykonanej pomocou smart kontraktu, sa uskutoční finančný prevod na úhradu colných poplatkov a cestní dopravcovia potvrdia nakládku kontajnerov. Keď sú kvety doručené, a potvrdí to aj importér, smart kontrakt spustí vykonanie finančného prevodu na úhradu dopravy, ako aj za produkt samotný. Všetky dokumentácie a potvrdzovanie strán, spomenuté v tomto odstavci, sú taktiež validované spomenutými uzlami.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Obrázok 13: Tradelens aplikácia



Zdroj: IBM Research Youtube[149]

Keďže je tento typ súkromného blockchainu dostupný iba pre účastníkov s povoleným prístupom, ktorý je determinovaný členstvom v konzorciu, je nutné konštatovať, že oproti verejným otvoreným blockchainom sa jedná o pomerne centralizovanú infraštruktúru. Na druhej strane, toto riešenie predstavuje výrazný posun oproti predchádzajúcemu stavu a taktiež výrazne zvyšuje úroveň dôvery v hodnovernosť záznamov ako takých.

Tradelens spustený v júli roku 2017, ako mnoho ďalších s týmto alebo blízkym účelom (FoodTrust pre potraviny 2018 a Everledger pre Diamandy 2017), je postavený na platforme Hyperledger Fabric, alebo Everledger, ktoré sú založené na architektúre projektu Hyperledger.

[149] Viac informácií na: https://www.youtube.com/watch?v=r0LsnzAe1Yg

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tento projekt vznikol vo februári roku 2016 ako projekt nadácie otvorených zdrojových kódov Linux Foundation. Tá vznikla v roku 2000 na spoluprácu, implementáciu a podporu otvorených štandardov, správy a zdroja kódu pre tvorbu softvéru. Firma IBM je prémiovým členom ako mnoho ďalších veľkých IT firiem.

7.1.4. Virtuálna realita

Sektor virtuálnej reality je napriek ranému štádiu odvetvia pomerne aktívny v implementácii technológie blockchain prostredníctvom viacerých firiem, ktoré využívajú túto technológiu na sledovanie vlastníctva digitálnych predmetov vo virtuálnom priestore. Tento princíp je veľmi podobný tomu, ktorý sa snažia aplikovať rôzne firmy v rámci logistických procesov a sledovania životného cyklu produktov. Zatiaľ čo v logistike je takáto aplikácia pomerne náročná pre už spomínané bariéry fyzického sveta, vo virtuálnej realite sa digitálne predmety sledujú omnoho ľahšie a presnejšie. Už od počiatku berú do úvahy blockchainové platformy, konkrétne Ethereum, ako akýsi štandardný komunikačný protokol využívaný naprieč viacerými virtuálnymi svetmi. V súčasnosti je na trhu už niekoľko takýchto svetov, ktoré využívajú Ethereum na presun a zaznamenávanie vlastníctva predmetov.

Jedným z takých projektov je napríklad Decentraland[150], ktorý je virtuálna 3D platforma s vlastnou internou kryptomenou MANA, ktorá je vydaná na platforme Ethereum. Užívatelia môžu vďaka nej nakupovať virtuálne pozemky, stavať na nich a využívať ich podobne ako pozemky v reálnom fyzickom svete.

Ďalším významným projektom v tejto sfére je napríklad Somnium Space[151], ktorý na jeseň roku 2019 uskutočnil dokonca emisiu a predaj virtuálnych pozemkov. Tieto pozemky mali z technického hľadiska formu tzv. ERC-721 tokenu, ktorý je typický pre unikátne digitálne predmety a umožňuje každému takémuto predmetu vytvoriť unikátnu identitu pomocou

[150] Viac informácií na: https://decentraland.org/
[151] Viac informácií na: https://www.somniumspace.com/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

špecifických atribútov. Sektor virtuálnej reality je síce len v začiatkoch, no je veľmi pravdepodobné, že jeho užívateľská základňa bude rapídne rásť v blízkej budúcnosti a bude presahovať z herného priemyslu do mnohých ďalších. S rastúcim počtom ľudí využívajúcich produkty virtuálnej reality sa dá teda očakávať aj čím ďalej tým vyššia adopcia otvorených blockchainov ako Ethereum či Bitcoin, ktoré sa pravdepodobne stanú komunikačným štandardom, ktorý bude spájať mnoho virtuálnych svetov. To bude mať za následok možnosť vzájomnej komunikácie týchto svetov, a ako aj vyššiu likviditu ich interných digitálnych predmetov, a tak vytvorenie kompletne nového trhu.

7.1.5. Herný priemysel a digitálne predmety (NFT)

Aplikácie z herného či zábavného priemyslu sú typicky ťažnou silou viacerých významných technológií. Inak tomu nie je ani v blockchaine. Práve herný priemysel ako prvý implementoval blockchain na sledovanie životného cyklu digitálnych predmetov prostredníctvom tzv. unikátnych tokenov (z angl. Non-fungible tokens). Tie sú v podstate jedinečnou reprezentáciou aktíva alebo tovaru vo forme virtuálneho tokenu. Prostredníctvom kryptografie sa preukazuje vlastníctvo a pravosť aktíva. Napríklad virtuálne umelecké dielo, kde je umelecké dielo tokenizované, je dokázané vlastníctvom tokenu, ktoré je zapísané na blockchaine.

NFT sú jedinečné a nemôžu byť nahradené inou položkou. Takéto tokeny, ktoré nie sú uložené centralizovane, otvárajú do budúcnosti mnoho možností, ako digitalizovať aktíva. Od čiastočného vlastníctva, po viazanie celých reálnych aktív do digitálnych tokenov. Hlavnou výhodou je, že vlastníctvo nie je registrované len jednou entitou, ktorej treba veriť, ale obrovskou sieťou, ako Ethereum, ktoré má mohutnejšiu infraštruktúru ako akákoľvek organizácia.

Zameniteľnosť existuje v kryptomenách prakticky od začiatku, keďže každý novo vyťažený Bitcoin je rovnaký ako ten predchádzajúci. Napriek tomu v prípade Bitcoinu to už nie je celkom pravda, pretože existujú v rámci neho tokeny, ktoré sú na čiernej listine a to preto, že boli

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

používané na ilegálne alebo nelegálne aktivity, ako sú napríklad darknety alebo terorizmus. Z toho dôvodu nezameniteľné tokeny majú väčší potenciál v niektorých prípadoch.

Koncept NFT sa dostal do povedomia hlavne prostredníctvom projektu CryptoKitties na konci roku 2017, kedy sa niektoré kitties dokonca predali za stovky tisíc dolárov. Hoci protokoly a štandardy existujú mimo siete Ethereum pre NFT, primárnym štandardom, ktorý umožňuje ich vytváranie a výmenu, je štandard ERC-721. Podrobnejšie k dispozícii na Ethereum Github Wiki, štandard ERC-721 sa stal chrbticou pre tvorbu, vydávanie a obchodovanie s NFT.

V poslednej dobe však tím za platformou Enjin navrhol nový štandard tokenov, štandard ERC-1155, ktorý je navrhnutý ako vylepšenie oproti pôvodnému štandardu ERC-721. Konkrétne štandard umožňuje, aby token kontraktu obsahoval tak zameniteľné, ako aj nezameniteľné tokeny, čo predtým nebolo možné. Okrem toho ERC-1155 umožňuje implementovať viacero rôznych NFT do tej istej transakcie a vytvára tak oveľa efektívnejší proces výmeny NFT prostredníctvom distribuovaného trhu.

Typy NFT

DFT vytvárajú nedostatok určitého majetku. Zatiaľ čo spočiatku to bolo populárne iba pri virtuálnych aktívach, ako sú napríklad CryptoKitties a podobné aplikácie na iné jedinečné zberateľské predmety, potenciálne aplikácie NFT sa výrazne rozšírili, a to nielen v digitálnej oblasti.

V poslednej dobe čím ďalej tým viac narastá prienik herného priemyslu s kryptomenami, najmä v oblasti nehmotných aktív, ktoré zaznamenali väčšie pokroky. Platforma WAX od spoločnosti OpSkins umožňuje používateľom obchodovať s NFT na decentralizovanom trhu a dokonca si vytvárať vlastné virtuálne obchody. Spoločnosť WAX nedávno dokonca zverejnila plán výmeny fyzického tovaru prostredníctvom svojho trhu, ktorý je priamo spojený s nezameniteľným tokenom.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Mnoho súčasných implementácií NFT sa zameriava konkrétne na obchodovanie s rôznymi predmetmi hry, ako sú prispôsobené zbrane alebo brnenie v streleckých hrách prvej osoby, ako je Counter-Strike. Obchodovanie s týmito aktívami je v súčasnosti hlavným zameraním distribuovaných búrz, ako je WAX, a zameranie sa na NFT sa v tejto fáze týka predovšetkým herného priemyslu. Stále však dochádza k ďalšiemu vývoju, ktorý by mal rozšíriť ich uplatnenie.

Pojmy ako frakčné vlastníctvo niečoho, ako napríklad vzácneho umeleckého diela vo fyzickom svete, je rovnako možnosťou. Digitálne aktívum sa potom môže predať na menšie fragmenty skupine vlastníkov, ktorí budú zisková, keď sa niečo predá neskôr. Dostanú odmenu, ktorá bude korelovať s ich zlomkovým podielom na digitálnom majetku. Tento proces je možné uplatniť aj na trhu komerčných nehnuteľností. Nedávno vznikajúce platformy sa tiež zameriavajú na využitie blockchainu na poskytnutie pôvodu umeleckých diel vytvorením a udržiavaním reťazca vlastníctva konkrétnych umeleckých diel.

CryptoKitties

CryptoKitties je hra na blockchaine Etherea, ktorá umožňuje hráčom nakupovať, zbierať, rozmnožovať a predávať virtuálne mačky. Je to jeden z prvých pokusov o nasadenie technológie blockchain pre rekreáciu a voľný čas. Popularita hry v decembri 2017 preťažila sieť Ethereum a spôsobila, že dosiahla najvyšší počet transakcií a výrazne ju spomalila.

CryptoKitties nie je kryptomena. Namiesto toho je na blockchine Etherea ako non-fungible token (NFT) jedinečný pre každý obrázok virtuálnych mačiek. Každá CryptoKitty je jedinečná a vlastnená používateľom, overená prostredníctvom blockchainu a jej hodnota sa môže zhodnotiť alebo znehodnotiť na základe trhu. CryptoKitties sa nedajú replikovať a nemôžu byť prenášané bez súhlasu užívateľa. Vývojári v tomto prípade nemajú žiadnu právomoc. Používatelia môžu interagovať so svojimi CryptoKitties a môžu ich kupovať, predávať a chovať

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

(rozmnožovať). Spoločnosť vydala niektoré umelecké diela pod novou licenciou „Nifty“, ktorá umožňuje hráčom používať ich obrázok CryptoKitty.

Testovacia verzia CryptoKitties bola predstavená v ETH Waterloo 19. októbra 2017, na Ethereum hackathone. Od 2. decembra 2017 sa Genesis, prvá a najpredávanejšia mačka, predala v za 246,9255 ETH, čo bolo ekvivalentom viac ako 100-tisíc dolárov.

Virtuálne mačky sú rozmnožiteľné a nesú jedinečné číslo a 256-bitový genóm s DNA a rôznymi vlastnosťami (cattributes), ktoré sa môžu preniesť na potomstvo. Od rodičov k potomkom sa dá preniesť niekoľko znakov. Pre každú mačku existuje celkom 12 atribútov vrátane vzoru, tvaru úst, kožušiny, tvaru oka, základnej farby, farby očí či iných vlastností.

20. marca 2018 bolo oznámené, že spoločnosť CryptoKitties sa zmení na spoločnosť Dapper Labs a získa 12 miliónov dolárov od niekoľkých špičkových spoločností rizikového kapitálu a investičných anjelov.

V máji 2018 spoločnosť CryptoKitties uviedla na trh prvú celebritu značky CryptoKitty s americkým profesionálnym basketbalovým hráčom Stephenom Currym. V rámci partnerstva dostal Curry tri CryptoKitties so špeciálnymi snímkami, z ktorých prvú dal na dražbu. Spoločnosť neskôr aukciu pozastavila a tvrdila, že Stephen Curry nebol až v takej miere zahrnutý do projektu, ako sa pôvodne myslelo. Spoločnosť bola neskôr za to žalovaná. Súd rozhodol v prospech spoločnosti.

V októbri 2018 spoločnosť CryptoKitties dosiahla míľnik v miliónoch chovaných mačiek s objemom 3,2 milióna transakcií na základe svojich inteligentných zmlúv. V novembri 2018 spoločnosť Dapper Labs, ktorá bola vyradená z Axiom Zen ako vývojárska spoločnosť CryptoKitties, získala ďalších 15 miliónov dolárov v ďalšom kole vedenom Venrockom. V tomto kole spoločnosť zdvojnásobila svoje ohodnotenie.

Gamedex

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Gamedex[152] je platforma pre digitálne zberateľské karty a hry, v ktorých môžu byť aj použité. Na rozdiel od tradičných zberateľských predmetov (napríklad karty na bejzbal alebo Pokémon), pravosť týchto kariet môže byť preukázaná. Nemôžu byť falšované alebo znovu vytlačené. Platforma je podobná platforme Steam, ale týka sa digitálnych zberateľských kartových hier, pri ktorých sú jednotlivci schopní vytvárať a hrať.

Gamadex prevádzkuje systém, kde sa tokeny kupujú za ether, zároveň umožňuje predaj digitálnych kariet v kamenných obchodoch pomocou QR kódov. Projekt Gamadex v počiatkoch vyzbieral približne 800-tisíc dolárov.

CryptoPunks

CryptoPunks[153] je jeden z prvých projektov svojho druhu. Jedná sa o kolekciu 10 000 unikátnych digitálnych postavičiek. Žiadne z nich si nie sú úplne podobné a každá z nich môže byť oficiálne vlastnená len jednou osobou na blockchaine Etherea. Pôvodne ich mohol bezplatne získať ktokoľvek s peňaženkou Ethereum, avšak všetkých 10 000 bolo rýchlo predaných. Teraz sa dajú zakúpiť na sekundárnom trhu, ktorý je tiež zabudovaný do blockchainu. Prostredníctvom tohto trhu môžete nakupovať, ponúkať a ponúkať postavičky na predaj.

Na zakúpenie obrázkov je potrebné mať nainštalované rozšírenie Metamask. Zároveň vlastniť kryptomenu Ether, za ktorú sa dajú obrázky nakúpiť na trhu.

---

[152] Viac informácií na: https://www.gamedex.co/

[153] Viac informácií na: https://www.larvalabs.com/cryptopunks

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

CryptoPunks sú umelecké obrázky s rozmermi 24 x 24 pixelov generované algoritmom. Každý obrázok má svoju vlastnú stránku profilu, ktorá zobrazuje jeho atribúty, ako aj stav ich vlastníctva či históriu predaja. Celkové doterajšie predaje sú na úrovni 250-tisíc dolárov.

Budúcnosť NFT

Budúce využitie NFT bude pravdepodobne realitou na rôznych trhoch. S rastúcou digitalizáciou vecí a internetom sa objavujú praktické použitia technológie blockchainu. A s tým práve bude súvisieť aj tokenizácia aktív.

Môžu to byť rôzne predmety z reality, napríklad a aj tenisky. Pokiaľ by to bol zberateľský alebo historický kus, tak to môže byť tokenizované na blockchaine. Následne by sa to mohlo ďalej predávať. Spomínaná spoločnosť WAX by mohla umožniť výmenu fyzického tovaru za virtuálnu položku, ako je napríklad hra. Certifikácia, softvérové licencie a vlastníctvo nehnuteľností majú potenciál fungovať ako NFT. Tradičnejšie aktíva, ako sú dlhopisy, akcie a drahé kovy, by sa mohli tokenizovať alebo zoskupiť do skupín, tak sa stane systém efektívnejším pre finančné inštitúcie. Pomerne slabá škálovateľnosť a vysoké náklady systému sú zatiaľ prekážkou, no do budúcna budú pravdepodobne mitigované.

Jedným z najpozoruhodnejších projektov v oblasti tokenizovaných aktív je nedávne spustenie programu Liquid Assets spoločnosťou Blockstream. Program umožňuje výmenu a tokenizáciu širokého spektra aktív, od finančných nástrojov, po objekty v reálnom svete.

Blockstream je už dlho v popredí inovácií v kryptomenovom priestore a za nimi stojí vysoko rešpektovaný tím. Spojenie digitálnych aktív v rámci Bitcoinových side chainov je úspechom a významným krokom vo vývoji v NFT.

V rámci privátneho sektora existuje mnoho blockchainových platforiem, ako aj projektov, ktoré sú aplikovateľné v rôznych odvetviach. V nasledujúcej tabuľke sa snažíme zmapovať tie najvýznamnejšie iniciatívy, platformy a projekty v rámci privátneho sektoru.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tabuľka 9: Blockchain projekty naprieč odvetviami v privátnom sektore

Odvetvie	Účely	Projekty
Platby	Medzinárodné / medzibankové / medzi-inštitučné prevody, podmienené / záväzné platby	Bitcoin*, Litecoin*, Ripple*, Stellar*, NANO, NEM
Bankovníctvo, pôžičky (súkromné, anonymné)	Sporenie, finančné produkty s úrokom, pôžičky, pôžičky kryptomeny krytej národnou menou,	dYdX, Celsius, Dharma, Compound, Bitshares, OmiseGo
Kyberbezpečnosť	Decentralizované úložisko informácií, internet, bezpečnejšie prevody a surfovanie internetom	MaidSafe, Abra, Enigma
Dodávateľský reťazec / Logistika	Pôvod, záznam pohybu a aktuálny stav produktov, logistický monitoring, bezpečnosť potravín / spotrebiteľa	Tradelens, FR8, Provenance, Fluent, Block Verify, Decent (SK)*, 0x
Predpovede a hazard	Stávkovanie bez stávkovej kancelárie či sprostredkovateľa, decentralizovaný a autonómny algoritmus pre rozhodovanie / automatizovaný výkon zmluvných podmienok,	Augur*, Gnosis, Bethereum (SK)
Internet vecí	Autonómny výkon transakcie pomocou senzorov a čipov, autonómna platba vozidlom	Innogy* (SK), IOTA, ZF, UBS, Walton
Poisťovníctvo	Poistné produkty na činnosť / imanie vo fyzickom svete, vychádzajúce zo zjednodušeného dokladovania poistnej udalosti blockchainom	Etherisc, Tierion, B3i
Zdieľaná ekonomika	Zdieľaná taxi služba a preprava iných druhov	Arcadecity, LA ZOOZ
Cloud/virtuálne úložisko	Svetový superpočítač/decentralizovaná výpočtová sila, priame sprostredkovanie a permanentné uchovanie informácií a obrazového obsahu	Golem, StorJ, Strat, Decent (SK)*

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Charita	Transparentné poukázanie fin. prostriedkov strane v núdzi bez prostredníkov	BitGive, DarujKlik.sk (SK)*
Hlasovanie/Voľby	Nezmeniteľné záznamy hlasovania, ochrana hlasovania voči hackingu či mazaniu, petície	FollowMyVote, Democracy Earth
Sociálny a dôchodkový systém (ich nahrádzanie súkromným sektorom)	Súkromné dôchodkové sporenie, univerzálny základný príjem občana, decentralizovaná, bezpečná a autonómna výplata podpory / dávok / príspevkov	Circles, GovCoin
Zdravotníctvo	Zdravotná karta, ochrana zdravotných informácií a ich prenos medzi zdravotníckymi zariadeniami, dokladovanie predpisu / receptu liekov	Gem, Tierion, Aetna
Distribučná sieť elektrickej energie	Pôvod, záznam užívania a sporenia, či produkcie elektrickej energie a s tým spojené finančné vysporiadanie	Innogy* (SK), WePower, TransactiveGrid, Power Ledger
Hudobný priemysel	Predaj a kúpa hudby medzi interpretom a poslucháčom bez prostredníkov	UJO music, MyCelia
Maloobchod	Online trhovisko bez prostredníkov či tretej strany	OpenBazaar, OB1
Reality	Decentralizovaný a autonómny algoritmus vykonávajúci prevod nehnuteľnosti a finančných prostriedkov na základe zmluvných podmienok, stavebné pôžičky	UbitQuity, RealT
Monetizácia online obsahu	Mikrotransakcie, prepitné za služby, príspevky či sponzoring tvorcov internetového obsahu	BNS, Steemit, Brave/BAT
Účtovníctvo a audit	Decentralizovaný a autonómny algoritmus (Smartcontract) vykonávajúci zaraďovanie položiek a manažment účtovníctva	Nightfall

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Aero/Moto priemysel a výroba	Pôvod, záznam pohybu a aktuálny stav súčiastok leteckého či auto priemyslu, monitoring ich životnosti	3IPK (SK),
Monitoring finančnej kriminality	Forenzná analýza a vyšetrovanie finančnej kriminality	Chainalysis, Elliptic, Blockseer,
Virtuálna Realita	Kúpa a užívanie virtuálneho priestoru vo virtuálnom prostredí	Decentraland, Somnium Space
Decentralizované aplikácie	Tvorba decentralizovaných blockchain-aplikácií	Dfinity, EOS, Cardano, Lisk, Ethereum, Tron

*Ako platforma sa dá zaradiť pod viacero účelov vo viacerých odvetviach
(SK) - Slovenská firma

7.2. Verejný Sektor

V rámci verejného sektora sa dá na blockchain nahliadať ako dostribuovanú databázu, ktorá ma potenciál nahradiť centrálnu autoritu, ktorá spravuje systém, do ktorého sa zapisujú rôzne dáta a záznamy. Tieto záznamy môžu súvisieť v princípe s čímkoľvek. Ako príklad môžeme uviesť prevod nehnuteľností, vydávanie a overovanie rôznych listín, zaznamenanie zdravotných údajov a podobne. Namiesto jednej zodpovednej centrálnej autority či orgánu zodpovedného za správu systému, je možné garantovať integritu dát distribuovanou otvorenou databázou, do ktorej môže mať prístup ktokoľvek, a ktorá má zároveň otvorený a sprístupnený zdrojový kód, aby verejnosť mohla audiovať princípy, na ktorých systém funguje. Z obáv o únik citlivých osobných či iných informácií sa niektoré inštitúcie rozhodli implementovať privátne blockchainy. Prístup do nich je riadený centrálnou autoritou či skupinou autorít, avšak vývoj vo svete verejných blockchainov pomerne výrazne napreduje a dá sa domnievať, že čoskoro aj verejné a auditovateľné blockchainové systémy budú schopné uchovať citlive informácie, tak aby boli prístupne len vybraným entitám. V nasledujúcej časti analyzujeme vybrané konkrétne aplikácie blockchainu vo verejnom sektore.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

7.2.1. Univerzitné diplomy

Jedným z možných použití technológie blockchain je, že môže slúžiť ako decentralizované trvalé nemenné úložisko rôznych druhov informácií alebo aktív. Vytváranie a vydávanie rôznych digitálnych certifikátov je s blockchainom relatívne jednoduché. Napríklad sa vytvorí digitálny súbor PDF, ktorý obsahuje informácie, ako sú meno študenta, titul, rok ukončenia štúdia, názov univerzity, dátum vydania atď.

Následne sa digitálny súbor podpisuje pomocou súkromného kľúča, ku ktorému má prístup iba vydávajúca inštitúcia. Podpis sa pripojí k samotnému certifikátu. Ďalej sa vytvorí haš dokumentu pomocou algoritmu SHA-256, ktorý sa dá použiť na overenie, či nikto neporušil obsah digitálneho súboru. Nakoniec sa súkromný kľúč znova použije na vytvorenie záznamu v blockchaine, čo znamená, že v tomto prípade certifikát sa vydáva študentovi v daný deň. To umožňuje overiť, komu bol certifikát vydaný a kým bol vydaný. Zároveň je možné overiť aj obsah samotného certifikátu - všetko iba prostredníctvom napríklad Bitcoinového blockchainu a nie je potrebné sa obracať na vydávajúcu inštitúciu.

Univerzita v Nikózii sa stala prvou univerzitou na svete, ktorá vydávala akademické osvedčenia, ktorých pravosť sa dá overiť prostredníctvom Bitcoinového blockchainu. Tieto certifikáty sa vydávajú od roku 2015 študentom, ktorí úspešne ukončili alebo sa zúčastnili na DFIN-511 (Úvod do digitálnych mien), čo je prvý univerzitný kurz ponúkaný na tému kryptomeny. Od roku 2017 začala UNIC vydávať všetky univerzitné diplomy na Bitcoinovom blockchaine pomocou vlastnej technológie, ktorá sa vyvinula ako open-source.

7.2.2. Voľby prostredníctvom blockchainu154

[154] Viac informácií na:. https://medium.com/bpfoundation/election-voting-blockchain-case-studies-18321c379529>

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Jedným z najčastejšie diskutovaných využití blockchainu v rámci verejného sektora sú voľby. Voľby sú v mnoho štátoch stále manuálnym papierovým procesom. Už samotná digitalizácia tohto procesu by výrazne zvýšila efektívnosť a presnosť volieb, a zároveň by mohla zvýšiť dôveru vo výsledky volieb ako takých. Ak by sa voľby konali prostredníctvom softvéru, ktorý zapisuje dáta do verejného blockchainu, ktorý je mnoho odolnejší proti hackerským útokom, ako aj zneužitiu dát centrálnou autoritou, mohlo by to výrazne zvýšiť bezpečnosť takýchto dát, nakoľko by bolo ťažšie ich manipulovať. V niektorých krajinách sa s takýmto nastavením volieb už dlhšiu dobu experimentuje a taktiež existuje niekoľko nezávislých projektov a platforiem, ktorá budujú softvérové systémy slúžiace na tento účel.

Voatz

Dňa 6. novembra 2018 americký štát Západná Virgínia použil Voatz[155] mobilnú hlasovaciu aplikáciu založenú na blockchaine, aby umožnila zahraničným voličom (aktívnych vojakov) hlasovať v amerických priebežných voľbách. Bolo to prvé použitie technológie blockchain vo federálnych voľbách v USA. Voatz je startup založený v roku 2015, ktorý umožňuje občanom hlasovať vo všetkých druhoch volieb prostredníctvom smartfónov. V januári 2018 spoločnosť získala prostredníctvom seed financovania 2,2 milióna dolárov.

Aplikácia Voatz sa spolieha na blockchain, a teda na vytvorenie nemenného záznamu odovzdaných hlasov, spolieha sa aj na softvér na detekciu škodlivého malvéru a na biometriu, ktorá ma pomôcť autentifikácii a identifikácii. Aby voliči mohli odovzdať hlasovacie lístky, musia sa najprv zaregistrovať prostredníctvom aplikácie odovzdaním fotky vodičského preukazu alebo iného identifikačného preukazu. Aplikácia následne bude požadovať odoslanie krátkeho videa s ich tvárou. Technológia rozpoznávania tváre, ktorú používa iPhone alebo

[155] Viac informácií na: https://voatz.com/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Android, porovnáva nahraté video s fotkou z identifikačného preukazu. Osobné údaje na identifikačnom preukaze zase porovnáva s databázou voličov v Západnej Virgínii. Po dokončení overenia si voliči môžu vybrať a predložiť svoj hlasovací lístok pomocou odtlačku prsta alebo rozpoznaním tváre. Okrem používania technológie na overovanie má spoločnosť tiež pracovníkov na kontrolu predložených informácií manuálne. Všetky údaje umožňujúce identifikáciu osôb sa vymažú po hlasovaní.

Hlasy sú uložené na blockchaine - databáze, ktorá je distribuovaná a uložená na 16 rôznych miestach a kde sú záznamy zabezpečené pomocou algoritmov – neskôr sú odomknuté úradníkmi pri kontrole, keď sa voľby uzatvoria. Keď volič odovzdá svoj hlas, pošle sa potvrdzovací e-mail schránke, ktorá je určená volebnej komisii a rovnako sa pošle e-mail aj voličovi. To slúži ako mechanizmus auditu a záloha. Voliči môžu tento doklad skontrolovať a overiť a v prípade akýchkoľvek nezrovnalostí informovať úradníkov. Aplikácia funguje iba na vopred určených smartfónoch, ktoré spĺňajú bezpečnostné štandardy a majú najnovšie aktualizácie softvéru. Ak softvér na detekciu škodlivého malvéru zistí potenciálne nebezpečenstvo, aplikácia zabráni používateľom v jej otvorení. Akákoľvek podozrivá aktivita je označená na kontrolu ľuďmi. Voliči, ktorí sa nechcú zúčastniť alebo nie sú oprávnení hlasovať pomocou smartfónu, sa môžu rozhodnúť hlasovať tradičnými metódami.

Pred voľbami v polovici obdobia uskutočnil štát Západná Virgínia obmedzené voľby s 13 voličmi zo šiestich rôznych krajín v máji 2018 v tzv. primárkach. Výsledky pilotov skontrolovalo niekoľko spoločností venujúcich sa bezpečnosti, ktoré skonštatovali, že systém je bezpečný.

Po úspechu prvého testu štát Virginia rozšíril projekt na prezidentské voľby v novembri 2018. Do druhého testu bolo vybraných 25 z 55 štátov. Zúčastnilo sa na ňom 144 voličov z 31 krajín.

Spoločnosť aj štát Západnej Virgínie boli s výsledkom spokojní. Voliť mohli aj vojaci mimo svojho domova. Systém spoločnosti Voatz bol však neskôr kritizovaný a to preto, že Voatz je súkromná spoločnosť, ktorá má príliš veľkú moc nad tým, kto a ako blockchain udržuje. Systém

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Voatz je postavený na báze blockchainu HyperLedger, ktorý vytvorila spoločnosť IBM a ktorý je teraz podporovaný nadáciou Linux. Každý, kto sa chce zapojiť do systému, či už volič alebo audítor, musí byť overený. V rámci pilotu v Západnej Virgínii sa malo použiť 4 až 16 overovacích uzlov rozdelených medzi viacerých poskytovateľov cloudu, z ktorých každý je geograficky distribuovaný. Overovatelia blockchainu v systéme Voatz sú preverenými stranami. Medzi stakeholderov patrí samotný Voatz, volební úradníci, nestranní audítori a politici. V budúcnosti môže štátny tajomník alebo nezávislá štátna volebná rada zvýšiť počet uzlov a určiť, ktoré organizácie (napr. politické strany, univerzity, médiá, mimovládne organizácie, neziskové organizácie, audítori, atď.) sa môžu zapojiť do siete ako overovatelia.

Votem

Mobilné hlasovanie[156] založené na blockchaine sa používa aj na hlasovanie mimo politických volieb, ako napríklad hlasovanie akcionárov za uznesenia predstavenstva spoločnosti na výročných valných zhromaždeniach. Zároveň sa umožnilo hlasovať aj za interpretov, ktorí sa mali umiestniť v Rock and Roll Hall of Fame. Hlasovanie v roku 2016 pomocou online hlasovacieho systému (ktoré nepoužívalo blockchain) bolo hacknuté a negatívne ovplyvnilo dôveryhodnosť a integritu hlasovania. V roku 2017 sa už použila aplikácia Votem, ktorá používa blockchain. Spoločnosť Votem informovala, že spracovala viac ako 1,8 milióna hlasov bez podvodov, kompromisov, útokov alebo hackerských útokov akéhokoľvek druhu, čo je zatiaľ najviac hlasov pri online hlasovaní pomocou blockchainu. Fanúšikovia hlasovali zo všetkých 50 štátov a viac ako 100 rôznych krajín, pričom 60 percent hlasov pochádzalo z telefónov.

Spoločnosť Smartmatic-Cybernetica

---

[156] Viac informácií na: https://www.votem.com/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

V marci 2016 spoločnosť Smartmatic-Cybernetica uskutočnila ako prvá na svete voľby online pomocou súkromného blockchainu pre snemovňu republikánskej strany v Utahu (GOP) na hlasovanie o prezidentských kandidátoch. Táto platforma umožnila 24 486 voličom odovzdať svoje hlasovacie lístky zo 45 rôznych krajín pomocou svojho počítača, tabletu alebo smartfónu. Používatelia sa museli prihlásiť pred voľbami do systému online. Najprv strana overila svoje členstvo v GOP a identifikáciu štátneho voliča a potom dala týmto používateľom šifrované identifikačné číslo, s ktorým mohli hlasovať. Voľby boli úspešné z viacerých hľadísk - účasť voličov bola vysoká a strana nezistila žiadne obavy, týkajúce sa bezpečnosti, ani problémy s presnosťou hlasovania.

Napriek tomu sa objavili voliči, ktorí nedokázali pochopiť systém alebo boli zmätení, nevedeli, ako sa prihlásiť či odovzdať hlas vo voľbách. Podľa vývojárov sú tieto obavy prehnané.

V máji 2018 spoločnosť Smartmatic-Cybernetica použila blockchain aj v referende v nórskom Finnmarki. Regionálne referendum zorganizovalo 19 miestnych orgánov z okresu Finnmark, aby konzultovalo s občanmi, či sa majú spojiť so susednou oblasťou Troms. S cieľom uľahčiť účasť a informovať voličov bol systém TIVI (systém Smartmatic-Cybernetica) plne integrovaný do systému ID-Porten. Jedná sa o službu jednotného prihlasovania, ktorá sa používa na prístup k nórskym verejným elektronickým službám. Voliči používali na prístup do systému štandardné webové prehliadače na svojich počítačoch, tabletoch alebo telefónoch. Elektronické hlasovacie karty boli prostredníctvom SMS poslané voličom. Upozornili ich, že hlasovali a informovali o prijatí svojho online hlasovania. Napriek možnosti hlasovania online alebo tradične papierovo, vo volebných miestnostiach bolo 85,5 % všetkých hlasov odovzdaných online. Podľa spoločnosti to je preto, že online hlasovanie je rozhodujúce pre zapojenie voličov vzhľadom na stále mobilnejších a rozptýlenejších voličov.

Napriek úspechu nie je spoločnosť Smartmatic-Cybernetica presvedčená, že blockchain je potrebný na online hlasovanie. Spoločnosť Smartmatic-Cybernetica poskytuje od roku 2005

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

v Estónsku technológiu bez blockchainu pre internetové hlasovanie. Firma poskytuje technológie a riešenia elektronického hlasovania po celom svete od roku 2000. Smartmatic-Cybernetica verí, že online hlasovanie je možné aj bez blockchainu a v prípade blockchainu si systémy vyžadujú ešte ďalší audit a analýzu.

Pokiaľ ide o výkon a škálovateľnosť, mnohé verejné blockchainy sú pomalé a nepoužiteľné pre rozsiahle parlamentné voľby. Verejný charakter mnohých blockchainov vyvoláva problémy týkajúce sa anonymity voličov a súkromia, ktoré sú základnými vlastnosťami demokratického procesu.

Okrem toho čisto decentralizovaná forma blockchainov je v rozpore s modelom riadenia volieb, v ktorom sú orgány pre riadenie volieb zodpovedné za potvrdzovanie výsledkov volieb a overovanie integrity konečných výsledkov.

Blockchain sám o sebe len slabo prispieva k bezpečnosti online hlasovacieho procesu. Kľúčové sú detaily implementácie. Na dosiahnutie bezpečného a preukázateľného online hlasovania je potrebné množstvo ďalších procesov a technológií. Napríklad overiteľné šifrovanie medzi koncovými bodmi. Napriek tomu spoločnosť priznáva, že prebiehajúci výskum vyrieši mnohé problémy súvisiace s výkonnosťou a súkromím v ranom štádiu. S postupujúcim vývojom technológie bude zohrávať čoraz dôležitejšiu úlohu vo voľbách.

7.3. E-governence – príklad z Estónska

V nasledujúcej časti podrobne analyzujeme smart riešenia v rámci e-governance v Estónsku. Estónsko je jednou z krajín, ktorá je najďalej v oblasti efektívneho verejného sektora. Vyznačuje sa nízkou byrokratickou záťažou, vysokou efektivitou, automatizáciou procesov a digitalizáciou záznamov. Napriek tomu, že nie všetky nižšie uvedené nevyhnutne využívajú blockchain, uvádzame ich, nakoľko nielenže využívajú iné alternatívne riešenia

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

a kryptografické protokoly, ale slúžia aj ako skvelý príklad zvyšovania efektivity procesov v štátnej správe.

Digitálna Identita

V Estónsku má každý obyvateľ tzv. digitálnu identitu a krajina má v súčasnosti najrozvinutejší národný systém preukazov na svete. Okrem toho, že slúži ako identifikačný preukaz s fotografiou, tak slúži aj ako prístup ku všetkým elektronickým službám v Estónsku.

„V Estónsku sa každá osoba môže bezpečne identifikovať a poskytnúť digitálny podpis pomocou svojho preukazu totožnosti, mobilnej identifikácie alebo Smart-ID a tým používať elektronické služby. Čip na preukaze totožnosti obsahuje údaje, ktoré zabezpečuje 2048-bitové šifrovanie. Preukaz totožnosti sa pravidelne používa ako cestovný doklad pre občanov Estónska na cestovanie v rámci EÚ, ako karta zdravotného poistenia, prostriedok na identifikáciu pri prihlasovaní na bankové účty, digitálny podpis, i-Voting, prostriedok na prezeranie zdravotných záznamov, podávanie daňových priznaní a pod.“[157]

V súčasnosti má 98 % obyvateľov Estónska tento preukaz, pričom pravidelne ho využíva 67 %. Okrem počítača je možné používať aj mobil ako prístup k elektronickým službám a na digitálny podpis dokumentov. Systém nevyžaduje špeciálnu čítačku kariet, ale používateľ si musí vybaviť špeciálnu SIM kartu do mobilného telefónu. Súkromné kľúče spolu s aplikáciou poskytujúcou autentifikačné a podpisové funkcie sú uložené na SIM karte. Mobilnú identifikáciu využíva 12,2 % obyvateľov. „Mobilnú identifikáciu využíva 12,2 % obyvateľov. Smart-ID je pohodlná mobilná aplikácia, ktorá funguje ako identifikačné riešenie pre každého, kto nemá v inteligentnom zariadení (smartfón, tablet) SIM kartu, ale musí online bezpečne preukázať

[157] ERNST & YOUNG. Štúdia možností a potenciálu technológie „blockchain“ pri zlepšovaní eGovernment riešení. Str. 59 [online]. Dostupné na internete: < https://www.vicepremier.gov.sk/wp-content/uploads/2019/06/UPPVII-blockchain-studia-v2_3-20190318.pdf?fbclid=IwAR27kbeDLast6ljL6Sm9NI44BjF1duSKYf5U2OcYyoqxkPozizrJTP0CrA4 >

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

svoju identitu. Pomocou Smart-ID je možné prihlásiť sa do elektronických služieb finančného sektora a potvrdiť transakcie, zmluvy a pod. K vykonaniu transakcie prostredníctvom Smart-ID postačuje 5 kilobajtov. Technológia blockchain zabezpečuje integritu údajov.“[158]

Elektronická rezidencia v Estónsku

Od roku 2014 umožňuje Estónsko komukoľvek na svete požiadať o získanie prístupu k digitálnej identite a stať sa e-rezidentom.

„Elektronický identifikačný doklad vydávaný e-rezidentom umožňuje držiteľom komerčné aktivity s verejným a súkromným sektorom, t. j. e-rezidenti majú prístup k podnikateľskému prostrediu EÚ a môžu využívať verejné elektronické služby prostredníctvom svojej digitálnej identity. Tento doklad nepredstavuje občianstvo v jeho tradičnom zmysle a nie je cestovným dokladom. V mnohých ohľadoch je však medzinárodným „pasom“ do virtuálneho sveta.“[159]

Elektronická rezidencia je významnou zmenou aj vzhľadom na skutočnosť, že prostredníctvom technológie blockchain môžu elektronickí rezidenti využívať notárske služby. Aplikácia blockchain technológie má potenciál zásadne zmeniť spôsob, akým sú údaje o identite overované a kontrolované.

Zahraničie využíva elektronickú rezidenciu najmä na založenie podnikania online, a to s možnosťou neskoršieho rozšírenia do celého sveta. Spoločnosť je možné založiť z akéhokoľvek miesta za 24 hodín. Následne môže požiadať o podnikateľský bankový účet a zabezpečiť bezpečné elektronické bankovníctvo, zabezpečiť si prístup k poskytovateľom medzinárodných platobných služieb, digitálne podpisovať a zasielať dokumenty a priznávať

[158] Tamtiež str.58

[159] Tamtiež str. 59

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

dane online. Elektronickí rezidenti obdržia digitálnu Identifikačnú kartu s PIN kódmi, kvôli autentifikácii a digitálnym popisom. Tieto podpisy sú právne ekvivalentné rukopisnému podpisu v rámci Estónska, ako aj u partnerov z celého sveta, ktorí túto formu podpisu akceptujú. O Residency zatiaľ požiadalo 50 tisíc ľudí zo 160 krajín sveta.

Obchodný register

Estónske centrum registrov a informačných systémov vytvorilo ako jeden z prvých registrov práve obchodný register. Služba je založená na databáze oddelení registrov okresných súdov a zobrazovaní údajov všetkých právnických osôb registrovaných v Estónsku v reálnom čase. Pre prezeranie údajov je potrebný len doklad totožnosti.

Register umožňuje prehľadávanie:

- prezeranie všeobecných údajov o spoločnosti a daňových nedoplatkov
- vyhľadávanie podľa mena
- kódu v obchodnom registri
- sídla, oblasti činností a pod.
- prezeranie výročných správ, stanov, osobných a obchodných záväzkov, monitorovanie spracovania údajov
- zaznamenávanie zmien spoločností v reálnom čase
- overenie obchodných a podnikateľských zákazov prislúchajúcich k jednotlivým osobám
- vizualizovanie vzťahov medzi rôznymi spoločnosťami a osobami, súčasné a bývalé vzťahy medzi spoločnosťami

Technológia blockchain pomáha zaistiť, kedy došlo k zmene informácií o spoločnosti v registri a aký bol dôvod zmeny.

Elektronický systém súdnictva

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

V roku 2006 bol v Estónsku spustený informačný systém súdnictva pre všetky typy prípadov. To znamená od prvého stupňa, cez druhý stupeň, až po najvyšší súd.

Informačný systém umožňuje:

- registráciu súdnych prípadov
- registráciu vypočutí
- registráciu rozsudkov
- automatické prideľovanie prípadov sudcom
- vytvorenie predvolania
- uverejnenie rozsudkov
- zber metaúdajov

Systém umožňuje vyhľadávanie na základe kľúčových slov, či upomienok. Systém umožňuje aj sledovanie dĺžky jednotlivých fáz konania. Blockchain umožňuje podobne ako pri predchádzajúcich registroch vyhľadávanie kto, kedy a ako zmenil údaje.

Elektronické voľby

Estónsko sa v roku 2005 stalo prvou krajinou, kde sa pri celoštátnych voľbách využil elektronický systém. V roku 2007 bol tento systém využitý na celoštátne parlamentné voľby. Volič hlasuje jednoducho cez webové rozhranie v čase volieb. Do systému sa prihlasuje pomocou elektronického dokladu totožnosti. Identita voliča sa odstráni predtým, ako sa hlasovací lístok dostane k Národnej volebnej komisii pre počítanie, čím sa zabezpečí jeho anonymita. Estónske riešenie umožňuje voličom prihlásiť sa a hlasovať toľkokrát, koľko chcú počas stanoveného obdobia pred hlasovaním. Keďže každé ďalšie hlasovanie voliča zruší to posledné, volič má do uzavretia stanoveného obdobia vždy možnosť zmeniť svoj hlas. Podľa štatistík bolo v posledných estónskych voľbách ušetrených 11 000 pracovných dní. Technológia blockchain sa využíva na odhalenie prípadnej manipulácie s hlasovaním.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

E-health

V Estónsku disponujú zdravotnými údajmi samotní pacienti. Od roku 2008 sú dostupné zdravotné údaje online. Skoro všetky zdravotnícke údaje už sú v súčasnosti digitalizované a blockchain sa používa na zabezpečenie integrity dát. Pacienti majú v systéme prístup ku svojim údajom, výsledkom, histórii vyšetrení. Lekári majú rovnako ako pacienti prístup k týmto záznamom. Systém šetrí náklady na administratívu a zároveň je efektívnejší v správe údajov pacientov a zároveň efektívnejšie dokáže riešiť problémy pacientov. „Podľa štatútu zdravotného IS je zriaďovateľom estónskeho národného zdravotného IS Ministerstvo sociálnych vecí a autorizovaným prevádzkovateľom estónska nadácia eHealth. Zdravotný IS je databáza, ktorá je súčasťou štátneho informačného systému.“[160]

Kataster nehnuteľností

Využívanie služby je podmienené, podobne ako pri obchodnom registri, elektronickým dokladom identity alebo aj prostredníctvom online bankovníctva.

Služba umožňuje vyhľadanie či overenie:

- všeobecných údajov
- veľkosti
- vlastníkov
- obmedzení a zaťažení nehnuteľností hypotékami

---

[160] ERNST & YOUNG. Štúdia možností a potenciálu technológie „blockchain“ pri zlepšovaní eGovernment riešení. Str.55 [online]. Dostupné na internete: < https://www.vicepremier.gov.sk/wp-content/uploads/2019/06/UPPVII-blockchain-studia-v2_3-20190318.pdf?fbclid=IwAR27kbeDLast6ljL6Sm9NI44BjF1duSKYf5U2OcYyoqxkPozizrJTP0CrA4 >

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

S katastrom nehnuteľností v Estónsku je možné uzavrieť zmluvu a registrovať sa v systéme, a to v prípade, že väčšie spoločnosti či agentúry potrebujú údaje čerpať denne. Všetky údaje vydané katastrom sú použiteľné na právne účely. Technológia blockchain pomáha zistiť, kto, kedy a ako zmenil údaje o nehnuteľnostiach v e-katastri nehnuteľností.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ZÁVER

Tento dokument analyzuje technologické a filozofické princípy súvisiace s krypto-technológiami, primárne s kryptomenami a blockchainom. Podrobne rozoberá fungovanie jednotlivých technológií založených na kryptografii a decentralizovaných systémoch, ako aj ich aplikáciu v rôznych odvetviach v rámci súkromného, ako aj verejného sektora. Analyzujeme súčasný stav vývoja rôznych kryptografických, kryptomenových či blockchainových protokolov, ako aj ich predpokladané smerovanie z technologického hľadiska. Zároveň analyzujeme ich vplyv na rôzne ekonomické procesy v rámci podnikateľského prostredia, štátneho sektoru, ale aj šedej ekonomiky. V rámci našej analýzy sme dospeli k nasledujúcim záverom:

- Pojem kryptomeny sa dá považovať za pomerne mylný, nakoľko väčšina technológií, ktoré sa skrývajú pod týmto termínom, má za cieľ byť viac než alternatíva k peniazom, či platobný nástroj.
- Bitcoin samotný môže byť analyzovaný z viacerých hľadísk ako digitálna mena, platobný nástroj, alternatíva k FIAT peniazom, digitálna komodita, investičné aktívum, či globálna databáza, garantujúca nemeniteľnosť dát.
- V prípade komplexnejších platforiem na smart kontrakty, ako Ethereum a iné, sa ich definovanie či analýza komplikuje ešte viac, nakoľko sa dajú považovať za globálny počítač v rámci ktorého sa dá spúšťať v princípe akúkoľvek aplikáciu.
- Najväčší prínos Blockchainu ako technológie spočíva v možnosti koordinovať sieť tisícok pseudo-anonymných serverov distribuovaných po celom svete, bez prítomnosti centrálnej autority, a zároveň poskytovať vysokú garanciu nemeniteľnosti dát v systéme.
- Technologické vlastnosti blockchainu sa však taktiež líšia naprieč rôznymi implementáciami.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- Dá sa predpokladať, že niektoré z verejných blockchain sietí, ako Bitcoin či Ethereum, sa v budúcnosti stanú podkladovým komunikačným štandardom pre webovú infraštruktúru.
- Na blockchain sa dá nazerať aj ako na distribuovanú databázu vhodnú pre širokú paletu aplikácií naprieč rôznymi odvetviami v súkromnom či verejnom sektore.
- Blockchain má potenciál výrazne zvýšiť efektivitu, automatizáciu a transparentnosť procesov, avšak podobný efekt sa dá dosiahnuť aj inými nástrojmi či centralizovanými riešeniami.
- Blockchain má zmysel aplikovať hlavne v prípadoch, kedy je cieľom eliminovať rolu centrálnej autority, dohliadajúcu na určitý systém, a nahradiť ju distribuovaným protokolom.
- Kryptomeny v súčasnosti stále predstavujú najrozšírenejšiu aplikáciu blockchain technológie, a pravdepodobne budú mať aj najväčší vplyv na právne či ekonomické systémy krajín.
- Zatiaľ čo kryptomeny neposkytujú dokonalú anonymitu užívateľom, využitie niektorých protokolov dokáže výrazne sťažiť vystopovanie identity užívateľa.
- Napriek väčšej anonymite kryptomien oproti klasickým platobným systémom, sa v rámci šedej ekonomiky v drvivej väčšine prípadov používajú národné meny, ako eurá či doláre.
- Napriek tomu sa dá očakávať v budúcnosti rastúci trend využívania anonymizačných techník a nástrojov, ktorých obmedzenie sa bude veľmi ťažko vymáhať.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

BIBLIOGRAFIA

1. 0X. [online]. Dostupné na internete: <https://0x.org/>
2. 1ML. Real-Time Lightning Network Statistics [online]. Dostupné na internete: <https://1ml.com/statistics>
3. ABRAHAM CH. 2018. The Origin Story of the Initial Coin Offering (ICO) Token Sale History. Newconomy [online]. Dostupné na internete: <https://newconomy.media/news/the-origin-story-of-the-initial-coin-offering-ico-token-sale-history>
4. AIRSWAP[online]. Dostupné na internete: <https://www.airswap.io/>
5. ALONSO K., 2018. Zero to Monero: First Edition a technical guide to a private digital currency; for beginners, amateurs, and experts [online]. Dostupné na internete:<https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf>
6. ALZA. *Monero* [online]. Dostupné na internete: <https://www.alza.sk/monero>
7. ANTONOPOULOS A. 2017 : Mastering Bitcoin: Programming the Open Blockchain, 2nd edition, Sebastopol: O'Reilly Media ISBN: 978-1491954386
8. ANTONOPOULOS A., Wood G. 2019: Mastering Ethereum: Building Smart Contracts and DApps, Sebastopol: O'Reilly Media. ISBN 978-1491971949
9. ATZORI M,. 2015. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? [online]. [cit. 17.9.2019.] Dostupné na internete: <http://dx.doi.org/10.2139/ssrn.2709713>
10. AUGUR [online]. Dostupné na internete: <https://www.augur.net/>
11. BACK A, CORALLO M, DASHRJ L., 2014. et al. Enabling Blockchain Innovations with Pegged Sidechains. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://blockstream.com/sidechains.pdf >
12. BACK A. 2002. Hashcash- A Denial Of Service Counter-Measure [online]. Dostupné na internete:<https://nakamotoinstitute.org/static/docs/hashcash.pdf>
13. BACK A., CORALLO M., DASHRJ L., FRIEDENBACH M., MAXWELL G., MILLER A.,POELSTRA A. ,TIMÓN J., and WUILLE P. 2014. Enabling Blockchain Innovations with Pegged Sidechains [online]. [cit. 15.9.2019.] Dostupné na internete: <https://blockstream.com/sidechains.pdf>
14. BACON J., MICHELS J., MILLARD CH., SINGH J .2017. Blockchain Demystified. Queen Mary School of Law Legal Studies Research Paper No. 268/2017. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://ssrn.com/abstract=3091218>
15. BARAN P. 1964. On distributed communications: I. Introduction to distributed communications networks. [online]. [cit. 17.9.2019.] Dostupné na internete:

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

<https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf>
16. BITCOIN CASH[online]. Dostupné na internete:<https://www.bitcoincash.org/>
17. BITCOIN WIKI. Base58Check encoding [online]. Dostupné na internete: <https://en.bitcoin.it/wiki/Base58Check_encoding>
18. BITCOIN WIKI. Secp256k1 [online]. Dostupné na internete: <https://en.bitcoin.it/wiki/Secp256k1>
19. BITMEX RESEARCH. 2019. The Schnorr Signature & Taproot Softfork Proposal [online]. Dostupné na internete: <https://blog.bitmex.com/the-schnorr-signature-taproot-softfork-proposal/>
20. BITSHARES [online]. Dostupné na internete:<https://bitshares.org/>
21. BLACKLOCK J., LEI S., Blockchain & Cryptocurrency Regulation 2020 China. [online]. Dostupné na internete: <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/china >
22. BLOCKCHAIN APP FACTORY. Art Token Development [online]. Dostupné na internete:<https://www.blockchainappfactory.com/art-tokenization>
23. Blockonomi:Taproot. [online]. [cit. 17.9.2019.] Dostupné na internete <https://blockonomi.com/bitcoin-taproot/>
24. BLOCKSTACK [online]. Dostupné na internete:<https://blockstack.org/>
25. BLOCKSTREAM. Liquid [online]. Dostupné na internete:<https://blockstream.com/liquid/>
26. BONNEAU J, MILLER A, CLARK J et al. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. [online]. [cit. 17.9.2019.] Dostupné na internete <https://wws.princeton.edu/system/files/research/documents/Felten_SoK.pdf.>
27. BOS J, HALDERMAN J, HENINGER N, MOORE J, NAEHRIG M, WUSTROW E. Elliptic curve cryptography in practice. In 18th International Conference, FC 2014. Springer Berlin Heidelberg, 2014. 157–175.
28. BRITTO J., CASTILLO A. 2013. Bitcoin Primer, Mercatus Center, George Mason University [online], [cit. 15.9.2019.] Dostupné na internete: <https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf>
29. BUIS J. 2018. How the $170 million Ethereum bug could have been prevented. Hackernoon. [online]. Dostupné na internete: <https://hackernoon.com/how-the-170-million-ethereum-bug-could-have-been-prevented-819053c3b2cb>
30. BUTERIN V. 2016. Chain Interoperability [online]. [cit. 15.9.2019.] Dostupné na internete: <http://www.r3cev.com/s/ChainInteroperability-8g6f.pdf>
31. CADWALLADR C., HARRISON E., 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian [online]. Dostupné na

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

internete: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
32. CANNELIS D. 2019. Bitcoin has nearly 100,000 nodes, but over 50 % run vulnerable code. The Next Web [online]. Dostupné na internete:<https://thenextweb.com/hardfork/2019/05/06/bitcoin-100000-nodes-vulnerable-cryptocurrency/>
33. CARDANODOCS. Ouroboros Proof Of Stake Algorithm [online]. Dostupné na internete:<https://cardanodocs.com/cardano/proof-of-stake/>
34. CATALINI C,. GANS J. 2019. Initial Coin Offerings and the Value of Crypto Tokens. MIT Sloan Research Paper No. 5347-18; Rotman School of Management Working Paper No. 3137213. [online]. [cit. 16.9.2019.] Dostupné na internete: <https://ssrn.com/abstract=3137213>
35. CERTICOM RESEARCH. 2010. SEC 2: Recommended Elliptic Curve Domain Parameters version 2.0 [online]. Dostupné na internete: <http://www.secg.org/sec2-v2.pdf>
36. CIAMBELLA F., CHONG E., Blockchain & Cryptocurrency Regulation 2020 Singapore [online]. Dostupné na internete: <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/singapore>
37. COIN DANCE. Bitcoin Nodes Summary [online]. Dostupné na internete:<https://coin.dance/nodes>
38. COINMAP[online]. Dostupné na internete: <https://coinmap.org/>
39. COINTERPARTY. [online]. Dostupné na internete: <https://counterparty.io/>
40. CONG L., ZHIGUOU. H. 2018. Blockchain Disruption and Smart Contracts [online]. [cit. 17.9.2019.] Dostupné na internete: <http://dx.doi.org/10.2139/ssrn.2985764>
41. CONNEXT. Scalable Ethereum [online]. Dostupné na internete: <https://connext.network/>
42. CONTI M. A Survey on Security and Privacy Issues of Bitcoin. [online]. [cit. 17.9.2019.] Dostupné na internete <https://arxiv.org/pdf/1706.00916.pdf. >
43. COSMOS [online]. Dostupné na internete:<https://cosmos.network/>
44. CROMAN K. et al. 2016. On Scaling Decentralized Blockchains [online], [cit. 15.9.2019.] Dostupné na internete: <http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf>
45. DASH. What is Dash? [online]. Dostupné na internete: <https://docs.dash.org/en/stable/introduction/about.html>
46. DECENT [online]. Dostupné na internete: <https://decent.ch/>
47. DECENTRALAND [online]. Dostupné na internete: <https://decentraland.org/
48. Delegated Proof-of-Stake Consensus - Bitshares. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://bitshares.org/technology/delegated-proof-of-stake-consensus>

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

49. DEVELOPERS RSK. [online]. Dostupné na internete: <https://developers.doc.rsk.co/docs/rsk-introduction>
50. DECENT [online]. Dostupné na internete: https://decent.ch/press-release/protect-what-is-yours-decents-digital-proof-securely-logs-ideas-patents-documents-and-more/ >
51. DFINITY. The Internet Computer [online]. Dostupné na internete: <https://dfinity.org/>
52. DHARMA [online]. Dostupné na internete: <https://www.dharma.io/>
53. DIFFIE W., HELLMAN M., 1976. New Directions in Cryptography [online]. Dostupné na internete: <https://ee.stanford.edu/~hellman/publications/24.pdf>
54. DIGIX GLOBAL. Digix. [online]. Dostupné na internete: < https://digix.global/dgd/>
55. DINGLEDINE R, MATHEWSON , SYVERSON P. 2004. Tor: The second-generation onion router. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://svn.torproject.org/svn/ projects/design-paper/tor-design.pdf>
56. DIRK Z., ROSS P., DOUGLAS A. 2017. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. University of Illinois Law Review, 2017-2018, Forthcoming; University of Luxembourg Law Working Paper No. 007/2017; Center for Business & Corporate Law (CBC) Working Paper 002/2017; University of Hong Kong Faculty of Law Research Paper No. 2017/020; UNSW Law Research Paper No. 17-52; European Banking Institute Working Paper Series 14. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://ssrn.com/abstract=3018214>
57. ELECTRONIC FRONTIER FOUNDATION. [online]. Dostupné na internete: <https://www.eff.org/>
58. EOS [online]. Dostupné na internete: <https://eos.io/>
59. EOS.IO Technical White Paper v2. 2018 [online]. [cit. 17.9.2019.] Dostupné na internete: <https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.80.>
60. ERNST & YOUNG. Štúdia možností a potenciálu technológie „blockchain“ prizlepšovaní eGovernment riešení. Str. 60 [online]. Dostupné na internete: <https://www.vicepremier.gov.sk/wp-content/uploads/2019/06/UPPVII-blockchain-studia-v2_3-20190318.pdf?fbclid=IwAR27kbeDLast6ljL6Sm9NI44BjF1duSKYf5U2OcYyoqxkPozizrJTP0CrA4>
61. ETHEREUM. [online]. Dostupné na internete: <https://ethereum.org/>
62. ETHHUB. Proof of Stake (PoS) [online]. Dostupné na internete: <https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/proof-of-stake/>

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

63. EUROPEAN COMISSION. European countries join Blockchain Partnership [online]. Dostupné na internete: <https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership>
64. EUROPEAN PARLIAMENT. Fighting mileage fraud on used cars [online]. Dostupné na internete: <http://www.europarl.europa.eu/news/en/headlines/society/20180525STO04312/fighting-mileage-fraud-on-used-cars>
65. EXAKING. PoW 51 % Attack Cost [online]. Dostupné na internete: <https://www.exaking.com/51>
66. FAWKES. 2019. Avalanche (AVA) — Blockchain 3.0: A Novel Metastable Consensus Protocol. Hackernoon. [online]. Dostupné na internete: <https://hackernoon.com/avalanche-ava-blockchain-3-0-a-novel-metastable-consensus-protocol-28cdc4ee8984>
67. FINNEY H. Reusable Proofs of Work. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://nakamotoinstitute.org/finney/rpow/index.html.>
68. FINNEY H., 2004. RPOW - Reusable Proofs of Work [online]. Dostupné na internete: <https://nakamotoinstitute.org/literature/rpow/>
69. FREENET PROJECT. [online]. Dostupné na internete: <https://freenetproject.org/>
70. FRIES T. 2019. AssetBlock To Tokenize $60 Million Worth Of Real Estate On Algorand [online]. Dostupné na internete: <https://thetokenist.io/assetblock-to-tokenize-60-million-worth-of-real-estate-on-algorand/>
71. GAMEDEX [online]. Dostupné na internete: < https://www.gamedex.co/ >
72. GITHUB. Awesome Lightning Network [online]. Dostupné na internete: <https://github.com/bcongdon/awesome-lightning-network>
73. GITHUB. Proof of Stake FAQ [online]. Dostupné na internete: <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#can-multi-currency-proof-of-stake-work>
74. GNOSIS [online]. Dostupné na internete: < https://gnosis.io/>
75. HEDERA HASHGRAPH [online]. Dostupné na internete: <https://www.hedera.com/>
76. https://www.cnbc.com/2019/11/12/china-could-launch-digital-currency-in-next-2-3-months-investor-says.html>
77. HUGHES E. A Cypherpunk's Manifesto [online]. Dostupné na internete: <https://www.activism.net/cypherpunk/manifesto.html>
78. HYPERLEDGER [online]. Dostupné na internete: <https://www.hyperledger.org/>
79. CHAINALYSIS [online]. Dostupné na internete: < https://www.chainalysis.com/ >

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

80. CHAUM D. Blind Signatures for Untraceable Payments [online]. Dostupné na internete: <https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF>
81. CHAUM D. Blind Signatures for Untraceable Payments. [online]. [cit. 17.9.2019.] Dostupné na internete <http://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.>
82. CHAUM D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms [online]. Dostupné na internete: <https://nakamotoinstitute.org/static/docs/untraceable-electronic-mail.pdf>
83. I2P. The invisible internet project TOR. [online]. Dostupné na internete: <https://geti2p.net/en/>
84. IBM RESEARCH. 2016. International Trade Solution on Blockchain. Youtube. [online]. Dostupné na internete: <https://www.youtube.com/watch?v=r0LsnzAe1Yg>
85. IBM., 2017. Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain [online]. Dostupné na internete: <https://www-03.ibm.com/press/us/en/pressrelease/51712.wss>
86. ICODROPS. Ethereum [online]. Dostupné na internete: <https://icodrops.com/ethereum/>
87. IOTA. [online]. Dostupné na internete: <https://www.iota.org/>
88. IPFS. A peer-to-peer hypermedia protocol designed to make the web faster, safer, and more open. [online]. Dostupné na internete: <https://ipfs.io/>
89. KARAME G., AUDROULAKI E. 2016 Bitcoin and Blockchain Security, Artech House, Inc., Norwood, MA, USA. ISBN: 978-1630810139
90. KASIREDDY P. 2017. How does Ethereum work, anyway? [online]. Dostupné na internete: <https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369>
91. KHATWANI, S. A Comprehensive Beginner's Guide to Factom Cryptocurrency. Coinsutra. [online]. <https://coinsutra.com/factom-cryptocurrency-fct>
92. KIM H., LASKOWSKI M,. 2016. Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance [online]. [cit. 17.9.2019.] Dostupné na internete: <http://dx.doi.org/10.2139/ssrn.2828369>
93. KIM CH., 2019. MakerDAO is launching a new version of its programmatic stablecoin DAI next month. Coindesk [online]. Dostupné na internete: <https://www.coindesk.com/makerdaos-multi-collateral-dai-token-is-launching-nov-18>

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

94. KRAVCHENKO P., 2019 Blockchain And Decentralized Systems, ISBN-13: 978-6177634286, Ukraine
95. LAMPORT L., SHOSTAK R., MARSHALL P., The Byzantine Generals Problem. [online]. Dostupné na internete: <https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf>
96. LAMPORT L., SHOSTAK R., PEASE M,. The byzantine generals problem. In ACM Transactions Programming Languages and Systems. Jul. 1982. Vol. 4, No. 3. 382–401.
97. LARVALABS [online]. Dostupné na internete: <https://www.larvalabs.com/cryptopunks>
98. LEARN PLASMA [online]. Dostupné na internete: <https://www.learnplasma.org/en/>
99. LIELACHER A. 2019. ETC 51 % attack – what happened and how it was stopped [online]. Dostupné na internete: <https://bravenewcoin.com/insights/etc-51-attack-what-happened-and-how-it-was-stopped>
100. LINUXFOUDNATIOn. About Linux Foundation. [online]. Dostupné na internete: <https://www.linuxfoundation.org/about/>
101. LOPP J. 2016. Bitcoin's Security Model: A Deep Dive. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://www.coindesk.com/bitcoins-security-model-deep-dive>
102. MAIDSAFE [online]. Dostupné na internete: <https://maidsafe.net/>
103. MAINELLI M., SMITH M. 2015. Sharing Ledgers for Sharing Economies: An Exploration of Mutual Distributed Ledgers (Aka Blockchain Technology) Journal of Financial Perspectives, Vol. 3, No. 3 [online]. [cit. 17.9.2019.] Dostupné na internete: <https://ssrn.com/abstract=3083963>
104. MAKER DAO., The Dai Stablecoin System [online]. Dostupné na internete: <https://makerdao.com/en/whitepaper/#overview-of-the-dai-stablecoin-system>
105. MAKER DAO[online]. Dostupné na internete: <https://makerdao.com/en/>
106. MAXWELL G. 2018. Taproot: Privacy preserving switchable scripting [online]. Dostupné na internete: <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html>
107. MAXWELL G., Confidential Transactions. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://people.xiph.org/~greg/confidential_values.txt>
108. The Invisible Internet Project (I2P). [online]. [cit. 17.9.2019.] Dostupné na internete: https://geti2p.net/en/about/intro>
109. MEARIAN L., 2018. IBM, Maersk launch blockchain-based shipping platform with 94 early adopters. Computerworld [online]. Dostupné na internete: <https://www.computerworld.com/article/3298522/ibm-maersk-launch- blockchain-based-shipping-platform-with-94-early-adopters.html>

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

110. MERKLE R. A Digital Signature Based on a Conventional Encryption Function. In Advances in Cryptology — CRYPTO '87, Lecture Notes in Computer Science. Vol. 293. 369–378. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/merkle.pdf>
111. MERKLE R.C , "Protocols for Public Key Cryptosystems," 1980 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1980, pp. 122-122. doi: 10.1109/SP.1980.10006. [online]. [cit. 17.9.2019.] Dostupné na internete: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6233691&isnumber=6233685>
112. MIERS I,. GARMAN CH., GREEN M., RUBIN A., Zerocoin: Anonymous Distributed E-Cash from Bitcoin. Baltimore, USA [online]. Dostupné na internete: <http://zerocoin.org/media/pdf/ZerocoinOakland.pdf>
113. MITRA R. 2019. What is Web 3.0? The Evolution of the Internet [online]. Dostupné na internete: <https://blockgeeks.com/guides/web-3-0/>
114. NAKAMOTO S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System [online]. Dostupné na internete: <https://nakamotoinstitute.org/bitcoin/>
115. NAKAMOTO S. 2008. Bitcoin: A Peer-toPeer Electronic Cash System [online], [cit. 15.9.2019.] Dostupné na internete: <https://bitcoin.org/bitcoin.pdf>
116. NARAYANAN A. , BONNEAU J., FELTEN E., MILLER A., GOLDFEDER S. 2016 : Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction., Princeton University Press. ISBN: 9781400884155
117. NEM [online]. Dostupné na internete: <https://nem.io/>
118. NEO [online]. Dostupné na internete: <https://neo.org/>
119. OPENTIMESTAMPS [online]. Dostupné na internete: < https://opentimestamps.org/>
120. OPENBAZAAR. [online]. Dostupné na internete: <https://openbazaar.org/>
121. OPENPGP[online]. Dostupné na internete: <https://www.openpgp.org/>
122. ORIGINSTAMP [online]. Dostupné na internete: <https://originstamp.org/home>
123. PETERS G., PANAYI E., CHAPELLE A,. 2015. Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective [online]. [cit. 17.9.2019.] Dostupné na internete: <https://ssrn.com/abstract=2646618>
124. PILKINGTON M, Blockchain Technology: Principles and Applications. 2015. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar [online]. [cit. 16.9.2019.] Dostupné na internete: <https://ssrn.com/abstract=2662660 >
125. PIVX. 2019. FAQ on Zerocoin and PIVX [online]. Dostupné na internete: <https://pivx.org/faq-on-zerocoin-and-pivx/

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

126. PLASMA. 2019. Plasma Contracts [online]. Dostupné na internete: <https://plasma.io/plasma-contracts.html>
127. POLKADOT [online]. Dostupné na internete: <https://polkadot.network/>
128. POON J, DRYJA T, 2016: The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. [online]. [cit. 17.9.2019.] Dostupné na internete <https://lightning.network/lightning-network-paper.pdf>
129. POON J, DRYJA T. 2016. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments [online]. [cit. 17.9.2019.] Dostupné na internete: <https://lightning.network/lightning-network-paper.pdf.>
130. POON J., DRYJA T. 2016. The Bitcoin Lightning Network [online], [cit. 15.9.2019.] Dostupné na internete: <https://lightning.network/lightning-network-paper.pdf>
131. POŠVANC, M., CABAJ, A., HAVRAN, T., LINDÁK, M., STANCEL, D., THURZO, A. Kryptosystémy a potenciál ich využitia v súkromnom a verejnom sektore. NADÁCIA F.A. HAYEKA 2016. s.8.
132. Proof-of-Importance. 2019. NEM: Technical ReferenceVersion 1.2.1. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf#section.7. >
133. R3 CORDA. Platform [online]. Dostupné na internete: <https://www.r3.com/platform/>
134. RADIX KNOWLEDGE BASE. Radix Platform [online]. Dostupné na internete: <https://docs.radixdlt.com/kb/learn/platform>
135. RAIDEN NETWORK [online]. Dostupné na internete:<https://raiden.network/>
136. RASKIN, M., SALEH F., YERMACK D. 2019. How Do Private Digital Currencies Affect Government Policy? [online]. [cit. 15.9.2019.] Dostupné na internete: <https://ssrn.com/abstract=>
137. ROHR J., WRIGHT A. 2018. Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets. Cardozo Legal Studies Research Paper No. 527; University of Tennessee Legal Studies Research Paper No. 338. [online]. [cit. 17.9.2019.] Dostupné na internete: <http://dx.doi.org/10.2139/ssrn.3048104>
138. RSL. Smart Contracts For Bitcoin [online]. Dostupné na internete:<https://www.rsk.co/>
139. SABERHAGEN N. 2013 CryptoNote v 2.0. [online]. [cit. 17.9.2019.] Dostupné na internete https://cryptonote.org/whitepaper.pdf.>
140. SAIFEDEAN A, 2016. Blockchain Technology: What is it Good for? [online]. [cit. 17.9.2019.] Dostupné na internete: <https://ssrn.com/abstract=2832751>
141. SHERMAN A, JAVANI F, ZHANG A and GOLASZEWSKI E, "On the Origins and Variations of Blockchain Technologies," in *IEEE Security & Privacy*, vol. 17, no. 1, pp. 72-77, Jan.-

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Feb. 2019. [online]. [cit. 17.9.2019.] Dostupné na internete <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8674176&isnumber=8674035>

142. SOMNIUMSPACE [online]. Dostupné na internete: <https://www.somniumspace.com/>
143. SOMPOLINSKY Y., LEWENBERG Y., ZOHAR A. SPECTRE: Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://eprint.iacr.org/2016/1159.pdf>
144. SOMPOLINSKY Y., ZOHAR A., PHANTOM, GHOSTDAG: Two Scalable BlockDAG protocols [online]. [cit. 17.9.2019.] Dostupné na internete: <https://eprint.iacr.org/2018/104.pdf>
145. STRONTIUM. 2018. Piwx White Paper[online]. Dostupné na internete:<https://pivx.org/wp-content/uploads/2019/05/PIVX-White-Paper-Sept-2018.pdf>
146. SZABO N. 2008. Bit Gold. In Unenumerated: An unending variety of topics. [online]. [cit. 17.9.2019.] Dostupné na internete: <https://unenumerated.blogspot.com/2005/12/bit-gold.html>
147. SZABO N. The Idea of Smart Contracts. [online]. [cit. 17.9.2019.] Dostupné na internete: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.>
148. SZABO N., 2005. Bit Gold [online]. Dostupné na internete: <https://nakamotoinstitute.org/bit-gold/>
149. TAMBANIS T., 2019. Election Voting: Blockchain Case Studies. Medium. [online]. Dostupné na internete: <https://medium.com/bpfoundation/election-voting-blockchain-case-studies-18321c379529>
150. TERENZI C. Bitcoin Inflation Rate Will Drop Under 2% in 2020; Why Does This Matter?. UseTheBitcoin [online]. Dostupné na internete: <https://usethebitcoin.com/bitcoin-inflation-rate-will-drop-under-2-in-2020-why-does-this-matter/>
151. TĚTEK J. Libra. ALZA [online]. Dostupné na internete: <https://www.alza.sk/libra-facebook>
152. TETHER. [online]. Dostupné na internete: <https://tether.to/>
153. TOKENSETS [online]. Dostupné na internete: <https://www.tokensets.com/>
154. TOR. [online]. Dostupné na internete <https://www.torproject.org/>
155. UNISWAP [online]. Dostupné na internete: <https://uniswap.io/>
156. UNIVERSITY OF CAMBRIDGE. Cambridge Bitcoin Electricity Consumption Index [online]. Dostupné na internete:<https://www.cbeci.org/>

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

157. VOATZ [online]. Dostupné na internete:< https://voatz.com/ >
158. VOTEM [online]. Dostupné na internete:< https://www.votem.com/>
159. WALCH A. 2015. The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk (March 16, 2015). 18 NYU Journal of Legislation and Public Policy 837 (2015). [online]. [cit. 17.9.2019.] Dostupné na internete: <https://ssrn.com/abstract=2579482>
160. WALKER G. Learn Me Bitcoin [online]. Dostupné na internete: <https://learnmeabitcoin.com/guide/script>
161. WELCOME CENTER MALTA. Ico & crypto regulation in Malta [online]. Dostupné na internete: <https://www.welcome-center-malta.com/blockchain-services-in-malta/ico-crypto-regulation-in-malta/>
162. WHITEPAPER. 2018. Verge Whitepaper [online]. Dostupné na internete: <https://whitepaper.io/document/12/verge-whitepaper
163. WHITEPAPERDATABASE. 2018. Zcash (ZEC)-Whitepaper [online]. Dostupné na internete: <https://whitepaperdatabase.com/zcash-zec-whitepaper/>
164. WIKIPEDIA. Crypto Wars [online]. Dostupné na internete: <https://en.wikipedia.org/wiki/Crypto_Wars>
165. WIKIPEDIA. Cypherpunk [online]. Dostupné na internete: <https://en.wikipedia.org/wiki/Cypherpunk>
166. WIKIPEDIA. Digicash. [online]. Dostupné na internete: <https://en.wikipedia.org/wiki/DigiCash>
167. WIKIPEDIA. E-gold. [online]. Dostupné na internete: <https://en.wikipedia.org/wiki/E-gold>
168. WRIGHT A., FILIPI P. 2015. Decentralized Blockchain Technology and the Rise of Lex Cryptographia [online]. [cit. 17.9.2019.] Dostupné na internete: <http://dx.doi.org/10.2139/ssrn.2580664>
169. ZCASH. [online]. Dostupné na internete: <https://z.cash/>

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk