Freeman Family

4. července 2019

EPIC CASH

EPIC SOUKROMÉ INTERNETOVÉ HOTOVOSTI

Elektronický peněžní systém Peer-to-peer

UCHOVÁVÁNÍ HODNOTY + MÉDIUM VÝMĚNY+ ZÚČTOVACÍ JEDNOTKA

1,7 miliardy dospělých nemá přístup ke globálnímu finančnímu systému, zatímco dalších 1,3 miliardy lidí je nedoceněno. Epic Cash odemkne lidský potenciál tím, že spojuje jednotlivce s globálním trhem. Rychlé, prakticky zdarma k použití a otevřené všem.

Version 7.1b

Obsah

I. Abstraktní

Epic Cash je posledním bodem cesty ke skutečné internetové hotovosti P2P, základním kamenem soukromého finančního systému. Epic měna si klade za cíl stát se nejefektivnější formou digitálních peněz na ochranu soukromí. Aby tento cíl splnil, splňuje tři hlavní funkce peněz:

1. **Hodnota** – mohou být uloženy, získány a vyměňovány později a mají předvídatelnou hodnotu při načtení;
2. **Médium výměny** – vše, co je přijato jako standard hodnoty a vyměnitelné za zboží nebo služby;
3. **Zúčtovací jednotka** – jednotka, kterou je hodnota věci započítána a porovnávána.

	$ USD	BTC	EPIC
Hodnota	✗	✓	✓
Médium výměny	✓	✗	✓
Zúčtovací jednotka	✓	✗	✓

V roce 2009 se Bitcoin objevil jako první digitální měna založená na blockchainu a spolu s ní tři definující charakteristiky, proti kterým jsou hodnoceny další kryptoměny:

- **Nespolehlivý** – nikdo není povinen důvěřovat centralizovanému subjektu nebo protistraně, aby síť fungovala;
- **Neměnnost** – transakce nelze vrátit zpět;
  a. Přepisování historie by mělo být velmi nepravděpodobné nebo obtížné;
  b. Pro nikoho kromě vlastníka soukromého klíče by nemělo být možné přesouvat prostředky spojené s tímto soukromým klíčem;
  c. Všechny transakce jsou zaznamenány v blockchainu.
- **Decentralizace** – "Blockchain jsou politicky decentralizované (Nikdo je neovládá) a architektonicky decentralizované(žádný bod selhání infrastruktury)..."[1].

Bitcoin házel nové stezky technologicky a zároveň dodržoval časově prověřené základy ve struktuře své měnové politiky. Úspěch Bitcoin je silně spjat s omezenou nabídkou v kombinaci s bezdůvěryhodným, neměnným a decentralizovaným blockchainem. Epic Cash napodobuje měnovou politiku Bitcoinu klesající inflace a omezenou nabídku, aby Epic měna mohla sloužit jako efektivní úložiště hodnoty.

Navzdory úspěchu Bitcoinu byly od svého vzniku před 10 lety odhaleny určité nedostatky. Jiné projekty se snažily tyto nedostatky překonat a my jsme zkoumali to nejlepší, co jsme použili jako výchozí point. Rozhodli jsme se, že využijeme kodebase Grin a vynikající práci několika dalších projektů, které nám pomohou zdokonalit se na těžce vyhraných úspěších a odhalených chybách předchůdců Epic Cash. Epic Cash má klíčové vlastnosti být ideální měnou:

- **Fungibility** – Hodnota dané jednotky Epic se musí vždy rovnat jiné jednotce Epic, stejně jako jeden jen nebo jüan je vždy roven a vyměnitelný jiným jenem nebo jüanem. Dosažení zastupitelnosti z velké části závisí na soukromí.
- **Škálovatelnost**– EEpic Cash udržuje prostorově efektivní blockchain, na kterém lze snadno nastavit nové uzly bez zařízení náročných na zdroje. Epic Cash blockchain je schopen alespoň dvojnásobek propustnosti Bitcoin.
- **Soukromí** – Epic Cash blockchain chrání anonymitu držitelů a uživatelů Epic tím, že chrání detaily transakcí od třetích stran a je navržen tak, aby byl jak nevystopovatelný, tak neviditelný pro sledování.
- **Rychlost** – Transakce Epic Cash jsou hladké, nepřetržité a jsou prováděny mnohem rychleji než v předchozích generacích technologie blockchainu. Zatímco Bitcoin vyžaduje šest 10-minutových bloků k dosažení úplného potvrzení transakce, Epic transakce se uskutečňují v rámci jednoho bloku potvrzení, jakmile je jeden blok vytěžen.

[1] Buterin, Vitalik, ***The Meaning of Decentralization***, 6 February, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. Soukromí

Moderní využití peněz lze chápat jako kolektivní převod zúčtovacích jednotek mezi lidmi a institucemi. Krajina peněz v libovolném okamžiku může být zmapována zodpovězením následujících otázek:

1. *Kdo ji drží a kolik drží?*
2. *Kdo obchoduje s kým a za kolik?*

Pro tradiční fiatové měny a samozřejmě i Bitcoin, můžeme na tyto otázky odpovědět. Přitom lze odhalit mnoho věcí o životech lidí, jako jsou vzorce spotřeby, vlastnictví a transakční protistrany. Docela přesné závěry lze vyvodit o zájmech a záměrech jednotlivce sledováním převodů hodnoty. Bez soukromí mohou být údaje o transakcích nebezpečnými informacemi v rukou dravých třetích stran.

Použití kryptocurrency v uplynulém desetiletí ukazuje kontinuum „soukromí“ v různých implementacích blockchainu. Měřítko ochrany osobních údajů, pokud je třeba vzít v úvahu, se pohybuje od otevřené a notoricky známé na jednom konci až po anonymní na straně druhé. Jak soukromí narůstají, jeden základní kámen kryptocurrency, bezohlednosti, degraduje. Jak dokládá úspěch analytických služeb Bitcoin blockchainu, Bitcoin se nachází spíše směrem k notoricky transparentnímu konci spektra soukromí. Uživatelé musí stále více podniknout kroky, aby zajistili, že se neúmyslně neobchodují s poškozeným Bitcoin. Řešení Epic Cash houpe jehlu směrem k anonymním a obnoví tuto základní vlastnost tím, že zajistí, že jak soukromí jednotlivce, tak soukromí transakcí jsou přizpůsobeny systému na základní úrovni.

Soukromí identity

Soukromí transakce

Soukromí identity

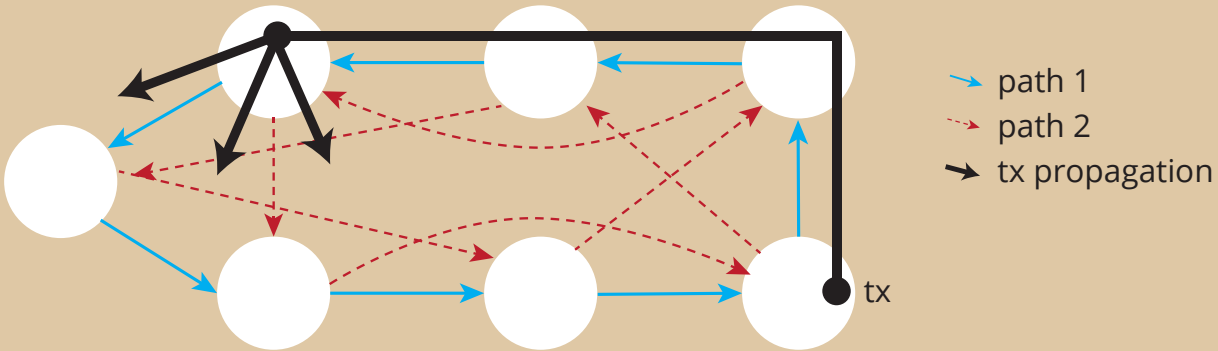
Většina kryptocurrency, jako je Bitcoin, je uložena v peněženkách, jejichž adresy odkazují na veřejné klíče odvozené od soukromých klíčů peněženky. Tyto adresy lze považovat za lokátory soukromého trezoru v digitálním světě. Blockchain Epic Cash zcela eliminuje adresy a místo toho použije jeden velký vícepodpis, ze kterého jsou všechny veřejné a soukromé klíče generovány na jedno použití.

Vzhledem k tomu, že adresy Bitcoin peněženky jsou lokátorem trezoru v digitálním světě, lze tuto peněženku vysledovat na adresu IP (Internet Protocol) vlastníka, která ukotví vlastníka k počítači na jedinečném místě v daném okamžiku. Jednoduše vysvětleno: když dojde k transakci Bitcoinu, je transakce vysílána z komunikačního centra nazývaného „node" a poté se rozšíří do jiných node nazývaných „peers". Tyto informace se pak rychle rozšíří do všech peer těchto node po sobě po celé síti. Tento proces je vhodně pojmenován „Gossip Protocol". Jednoduše řečeno, každý Bitcoin má viditelnou online pozici a fyzickou polohu, kde může být nalezen, nebo spíše vlastník Bitcoin.

Kromě odstranění adres peněženky, Epic Cash blockchain zabezpečuje soukromí identity tím, že zajišťuje, že IP adresy nelze vysledovat. Dělá to prostřednictvím integrace ***protokolu Dandelion++.*** Zlepšuje svůj předchůdce, původní protokol pampeliška, protokol pampeliška, je výsledkem pokračující práce sedmi výzkumníků v boji proti deanonymizačním útokům na blockchain. Prostřednictvím ***Dandelion++*** transakce jsou předávány přes náhodné propletené cesty, nebo „kabely", a pak se náhle rozptýlí do velké sítě uzlů, jako lusky pampeliška květina, když foukané z jejich stonku (obrázek 1). Díky tomu je téměř nemožné sledovat transakce zpět na jejich původ, a tedy jejich původní IP adresy.

Obrázek 1: *Anonymní transakce s protokol Dandelion++.*

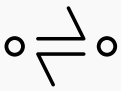
Dandelion++ předává zprávy přes jednu ze dvou vzájemně propojených cest na 4-pravidelném grafu a pak vysílá pomocí difúze. Na obrázku se transakce šíří přes modrou pevnou cestu.[3] Tento proces velmi ztěžuje sledování transakcí zpět ke zdroji, čímž se zachová soukromí.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

Soukromí transakce



Epic Cash blockchain zajišťuje soukromí transakcí tím, že zatemňuje částky a vztah odesílatele a příjemce transakce. ***Toho je dosaženo použitím myšlenek známých z Confidential Transactions (CT)*** [4] a ***CoinJoin*** [5], metody z velké části vyvinuté Gregory Maxwell (Bitcoin Core developer, spoluzakladatel a CTO společnosti Blockstream).

CT, původně vytvořený Adam Back a později rafinovaný Maxwell, pracuje tak, že transakcích na menší části prostřednictvím homomorfního šifrování, což je metoda provádění výpočtů na šifrovaných informacích, aniž by je nejprve dešifroval, aby se zachovalo soukromí. Jakmile jsou pozorovatelé rozděleni, nemohou vidět skutečné částky transakcí kvůli oslepujícím faktorům, což je systém, který hodí náhodná čísla do směsi fragmentů transakce, aby skryl hodnoty těchto fragmentů. Hodnota burzy nakonec znají pouze transakční strany, zatímco transakce je ověřena sítí potvrzením, že součet výstupních hodnot se rovná součtu vstupních hodnot a součet výstupních faktorů zaslepení se rovná součtu vstupních faktorů.

Abychom dále zkomplikovali úkolvědavých očí, všechny Epic Cash transakce jsou maskovány CT a pak smíchány dohromady, aby skryly spojení mezi transakčními stranami. To se provádí prostřednictvím druhého konceptu Maxwella, CoinJoin.

Chcete-li ilustrovat *CoinJoin* zjednodušeně, představte si, že A, B a C posílají Epic na X, Y a Z, resp. Odesláno prostřednictvím média CoinJoin, vše, co je známo, je, že odesílají A, B a C a přijímají X, Y a Z, zatímco částky transakce zůstávají neviditelné. Systém CoinJoin je zásadní pro Epic Cash prostřednictvím One-Way Aggregate Signatures (OWAS), které kombinují všechny transakce uvnitř bloku do jedné transakce.

Soukromí: Shrnutí

Epic Cash blockchain chrání soukromí jednotlivců a jejich transakcí tím, že:

- **Odstranění adres peněženky** – V digitálních trezicích v blockchain nejsou k dispozici žádné identifikátory polohy. Transakce jsou vytvářeny přímo osobně na základě peněženky k peněžence;
- ***Dandelion++ Protokol*** – **zakrývá digitální cesty transakce z IP adresy odesílatele transakce;**
- **Důvěrné transakce**– rozdělit transakce na více kusů a zavést oslepující faktory do sběru těchto kusů, aby nebylo možné znát hodnoty kusů a jiné parametry transakce;
- ***CoinJoin*** – kombinuje transakce do svazků a maskuje vztahy mezi transakčními stranami.

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.tx

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, příspěvek na fóru bitcoinů https://bitcointalk.org/index.php?topic=279249.0

III. Fungibility

Charlie Lee, tvůrce Litecoin, prohlásil, že zastupitelnost je jediná vlastnost, která chybí v Bitcoinu a Litecoinu, a přiznává, že soukromí a zastupitelnost jsou dalším bojištěm těchto coins.[6] Andreas Antonopoulos, jeden z předních světových expertů blockchainu, tvrdil, že „... zkažené mince jsou destruktivní. Pokud porušíte zastupitelnost a soukromí, porušíte currency."[7]

Zastupitelnost je majetkem sady zboží nebo aktiv, která zajišťuje, že jednotlivé jednotky této sady mají stejnou hodnotu a jsou zaměnitelné. Právě to odlišuje nejstarší formy měny od jejich předchozích směnných systémů. Bez důvěry v zastupitelnost peněz tyto peníze rychle ztrácejí svou užitečnost. Jak bude ilustrováno níže, zastupitelnost většiny kryptoměn je nejistá, zatímco architektura ochrany soukromí Epic Cash zajišťuje, že je nepropustná vůči stejným hrozbám.

Většina kryptoměn podobných Bitcoinu, podle povahy transparentních blockchainů, na kterých existují, lze ověřitelně vysledovat prostřednictvím každé peněženky, ve které byly drženy. Soukromé třetí strany i vlády sledují Bitcoin blockchain se stále sofistikovanějšími prostředky k rychlé identifikaci mincí používaných v předchozích aktivitách. To přirozeně vede k obavám, že zkažené mince mohou být jednoho dne zakázány transakce a jejich následní držitelé dobré víry budou mít ztrátu.

Dne 19. března 2018 oznámila U.S. Office of Foreign Asset Control (OFAC), že zvažuje zařazení digitálních měnových adres do seznamu Speciálně určených Nationals (SDN), což jsou subjekty, se kterými jsou osoby nebo podniky v USA zakázány obchodovat.

Ještě znepokojivější je, že OFAC nevyloučil zařazení adres, které v současné době drží zkažené mince, do seznamu SDN, což by ve skutečnosti umístilo nevinné vlastníky zkažené kryptocurrency na kriminální černou listinu kvůli příslušnosti poškozených mincí vlastněných. To přivedlo profesora právnické univerzity v New Yorku, Andrew Hinkes, k vtipku, "kiss fungibility goodbye," a že veřejnost by měla očekávat, že „prémie na čerstvě ražené coins, nebo vysledovat čisté coins...."[8].

S ohledem na tento vývoj není těžké si představit převrat na kryptoměna trhu a utrpení, nebo dokonce vyhynutí mnoha dobře zavedených kryptocurrency. Nicméně, Epic je jedním z mála kryptoměn, který se vyhýbá tomuto problému zcela kvůli silným vlastnostem ochrany osobních údajů dříve popsaným v tomto článku. Odstraněním vazby mezi identitou a vlastnictvím a vztahem mezi transformujícími se stranami nemůže být Epic nikdy přidružen k osobě nebo aktivitě. Hodnota Epic tak zůstává nezávislá na jeho uživatelích a poskytuje vysoký stupeň soukromí a bezpečnosti, které nemohou být snadno manipulovány škodlivými aktéry v trestních, finančních nebo politických arénách.

> **„...ZKAŽENÉ MINCE COINS DESTRUKTIVNÍ. POKUD PORUŠÍTE FUNGIBILITY A SOUKROMÍ, ZLOMÍTE CURRENCY."**
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. Škálovatelnost

Epic Cash je implementace blockchain MimbleWimble, která přináší pokroky v škálovatelnosti díky prostorově efektivnímu designu, který předává redundantní transakční data. Funkce Cut-Through, která je za to zodpovědná, zaručuje, že blockchain roste časem efektivnější prostor na rozdíl od většiny kryptocurrency, včetně Bitcoinu, a že nové uzly mohou být vytvořeny s minimálními investicemi do paměti a výpočetního výkonu. Tím, že zůstane prostorově efektivní, kondenzuje široce rozptýlenou síť a podporuje decentralizaci.. Navíc, zatímco každý uzel Bitcoin musí uložit celý řetězec, Epic Cash uzly jsou schopny přispět k zabezpečení sítě na základě malé podmnožiny bloků.

Většina kryptocurrency vyžaduje neomezené ukládání všech transakčních dat na jejich blockchain. Bitcoinový řetězec v současné době získává 0.1353 GB paměti každý den, zatímco řetězec Ethereum se zvyšuje ještě rychlejším tempem 0.2719 GB denně. Pokud Bitcoinův řetězec bude nadále růst současným tempem, nakonec dosáhne velikosti přibližně 6 TB v době, kdy bude jeho poslední blok odměn vytěžena v roce 2140. Ethereum do tohoto data překoná 10 TB[9]. Ve většině blockchainů bez MimbleWimble musí být transakce ověřeny uzly po celém světě. Jak se data zvyšují, tak i zátěž každého uzlu. Dokonce i při pouhých 200 GB (přibližná velikost aktuálního Bitcoinového řetězce) vyžaduje synchronizaci dat stabilní síť a schopnost vysokorychlostního čtení a zápisu disku.

V důsledku toho se mining stává stále více centralizovaným mezi velkými bazény využívajícími nákladné výpočetní zdroje. **Kdyby byla celá blockchain historie Bitcoinu uložena na Epic Cash blockchainu, vešla by do téměř o 90% méně místa.** Menší je rychlejší, protože každá transakce vyžaduje méně času na přenos a zabezpečení.

Mimblewimble řeší toto dilema úložišť inovativní metodou blokového prořezávání, označovanou jako „Cut-Through". Abychom pochopili, jak funguje Cut-Through, je nejlepší nejprve se podívat na to, jak jsou transakce a bloky složeny v blockchain MimbleWimble.

Vstupy:

Odkazy na staré výstupy;

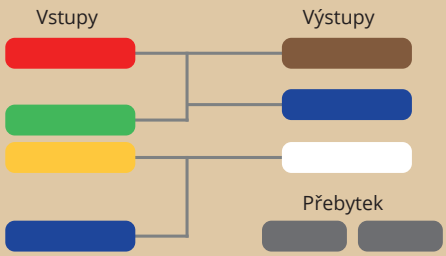
Výstupy:

Důvěrné transakční výstupy a rozsahy;

Přebytek:

Rozdíl mezi výstupy a vstupy, plus podpisy (pro autentizaci a prokázání neinflace).

Obrázek 2:
Části transakcí Mimblewimble.



[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

Všechny Epic Cash bloky obsahují:

Merkle Trees transakčních vstupů;

Merkle Trees výstupy a rozsahy transakcí;

Seznam nadbytečných hodnot a podpisů.

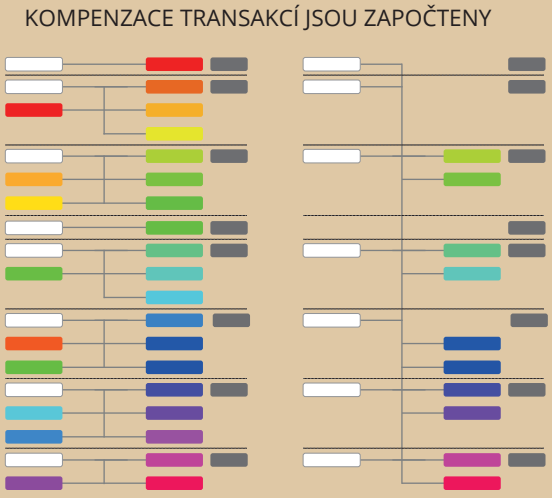
Na obrázcích 2 a 3, upravených z prezentací Andrewa Poelstry[10], vidíme nově těžený Epic reprezentovaný jako bílé vstupní buňky. Stejně barevné buňky představují výstupy s odpovídajícími spotřebovanými vstupy. S procesem Cut-Through jsou vstupy a odpovídající vyčerpané výstupy odstraněny, aby se uvolňovalo místo uvnitř bloku, což snižuje množství dat, která musí být uložena v blockchain. Zatímco transakce jsou vynechány z hlavní knihy, zbývající přebytečné jádra (pouhých 100 bajtů) trvale dokumentují, že transakce proběhly.

Když bloky budou nadále vytvářeny, použije MimbleWimble Cut-Through napříč bloky, takže v dlouhodobém horizontu zůstanou hlavičky bloku (přibližně 250 bajtů), nevyužité transakce a jádra transakcí (přibližně 100 bajtů).Grin, druhá implementace MimbleWimble, která má být zahájena, ukázala, že řetězec MimbleWimble s podobným počtem transakcí jako řetězec Bitcoin by byl téměř 10% velikosti řetězce Bitcoin[11]. Navíc velikost uzlu bude „v řádu několika GB pro řetězec velikosti bitcoin a potenciálně optimalizovatelný na několik set megabajtů."[12]

To stojí v výrazném kontrastu s Bitcoin, kde musí být celý blockchain uložen každým uzlem. Postupem času, jak efektivita prostoru Epic Cash blockchain roste vzhledem k Bitcoin blockchainu, tak i nákladová efektivita vzhledem k účasti uzlů v síti Epic Cash. Nižší bariéry k účasti pomáhají zajistit zásadní odolnost v uzlové vrstvě návrhu sítě.

Díky implementaci MimbleWimble a použití řetězového prořezávání s procesem Cut-Through nabízí Epic Cash blockchain škálovatelnost způsobem, který komunita kryptocurrency často přehlíží. Je to ten, který zachycuje podstatu Bitcoinu a podobně smýšlejících projektů: decentralizace. Bez ohledu na to, kolik transakcí za sekundu může být mince schopna zpracovat, k čemu je dobré, když ji nelze udržet širokou a rozmanitou sítí? Jsou-li požadavky na paměť takové, že validace nakonec tíhne k silným těžebním konglomerátům, pak se veškeré úsilí komunity kryptocurency o vytvoření decentralizovaného ekosystému vyloučí. Aby byla zajištěna dodatečná propustnost, je implementace vrstvy 2 ve stylu Lightning jako krátkodobý cíl v plánu vývoje Epic Cash.

Obrázek 3:
Transakce MimbleWimble před a po Cut-Through.



[10] SF Bitcoin Developers, ***MimbleWimble with Andrew Poelstra,*** 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, ***Grin Blockchain Size,*** December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, ***Introduction to Mimblewimble and Grin,*** 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Měnová politika

Měnová politika Epic Cash a Bitcoin je velmi podobná. Epic Cash cirkulující nabídka nejprve rychle expanduje a pak synchronizuje s oběžnou zásobou Bitcoin v roce 2028. Poté se zvyšuje klesajícím tempem až do dosažení maximální nabídky 21 milionů Epic v roce 2140. Epic Cash má vlastnosti stát se bezpečným úložištěm dlouhodobé hodnoty, protože oběhová zásoba je známa v každém okamžiku v průběhu svého životního cyklu emisí a vrcholí pevnou maximální zásobou. Měnová politika Epic Cash se vyznačuje následujícími čtyřmi rysy:

- Rychlé emise během prvních devíti let jeho životnosti, během nichž se má mining 20 343 750 Epic (96,875% celkové dodávky). Přesné hodnoty emisí jsou uvedeny v tomto dokumentu v části emisního programu;
- Epic cirkulující dodávky a rychlost emisí synchronizovat s těmi Bitcoin na epické Singularity kolem 24. května 2028. Po singularitě se rychlost emisí snižuje rostoucí rychlostí, zatímco oběhová zásoba roste klesající rychlostí;
- Maximální zásoba 21 milionů Epic bude dosaženo v roce 2140, přibližně ve stejnou dobu, kdy Bitcoin dosáhne maximální dodávky 21 milionů jednotek;
- Epic má 8 desetinné dělitelnosti strukturu, tak, že: 1 Epic se rovná 100 000 000 freeman (stejně jako 1 Bitcoin se rovná 100 000 000 satoshi).

Měnová politika Epic Cash je modelována podle Bitcoinu z následujících důvodů:

- Dohoda s ekonomickými základy Bitcoin, a to, že nedostatek a předvídatelnost oběhové nabídky jsou základem jeho silného uložení hodnotového majetku;
- Veřejnost je již obeznámena s modelem Bitcoinu a jeho osvědčenými výsledky za posledních deset let od jeho vzniku. Přibližně synchronizací s oběžnou zásobou Bitcoin a zrcadlením maximální struktury nabídky a dělitelnosti Bitcoin se Epic vydá cestou nejmenšího odporu vůči hromadnému přijetí.

VI. Emisní pláne

Epic Cash má celkem 33 mining epoch, z nichž každá je definována poklesem blokových odměn vzhledem k jejich předchozí době. Epic Genesis, datum těžby Epic block #1, se koná srpna 2019. Blok se těží za minutu. Prvních pět epoch produkují téměř 97% maximální nabídky Epic, což odpovídá 20 let emisí Bitcoin přibližně za devět let.

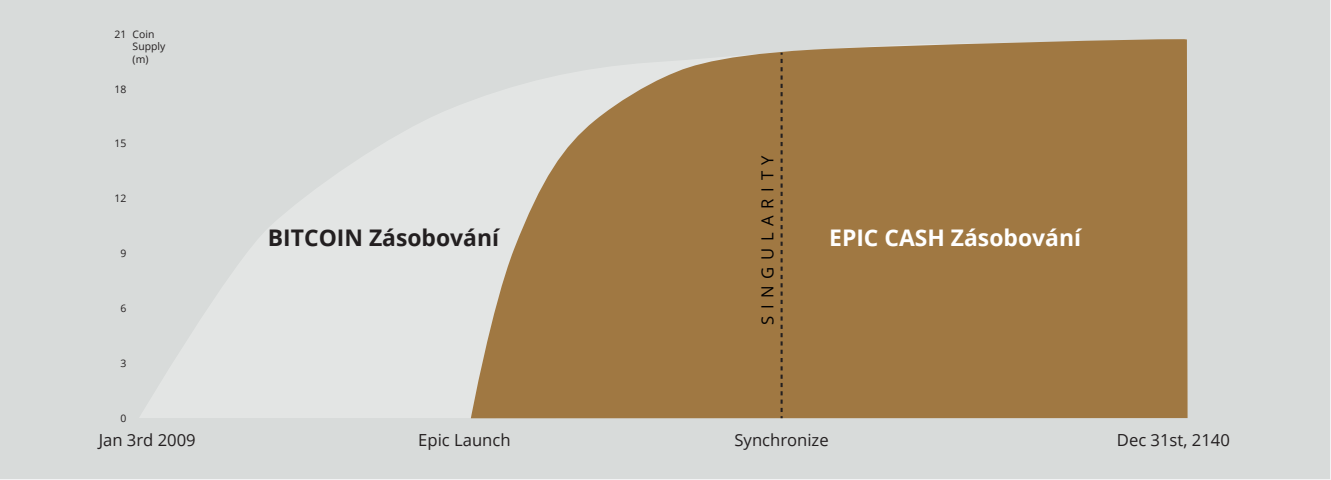
Rozpis emisí v tabulce 1 uvádí datum začátku a konce prvních sedmi těžebních období, jejich odpovídající blokové odměny a následné oběhové zásoby pro každou éru. epoch 8 až 33 nejsou zahrnuty v tabulce pro stručnost. Pro tyto éry by mělo stačit pochopit, že každá následující éra bude mít blokovou odměnu, která je poloviční výše odměny předchozí éry, přesně jako v Bitcoin. Množství Epic vyzařovaného během každé z těchto období bude součtem blokových odměn během 4 let (přibližně 1460 dní).

V epické singularitě (2028), Epic cirkulující zásoba protíná počet cirkulujících zásob Bitcoin, v tomto okamžiku Epic Cash přijímá Bitcoin blokovou odměnu a poloviční vzorec, který vidí blokové odměny klesat o polovinu každé čtyři roky. Jedinou výjimkou je, že Epic bloky se nadále těží rychlostí jedné za minutu, oproti Bitcoinu rychlosti jednoho bloku každých deset minut. Tím si Epic obíhající zásoba udržuje přibližnou paritu s oběžnou zásobou Bitcoin po zbytek jejich existence.

Tabulka 1: Rozpis emisí za prvních sedm mining epoch. Termíny jsou blízké aproximace.

Era	1	2	3	4	5	SINGULARITY	6	7
BlokOdměna	16	8	4	2	1		0.15625	0.078125
Datum zahájení	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
Datum ukončení	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
Délka (ve dnech)	334	470	601	800	1019		1460	1460
Počáteční Zásobování	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
KonecZásobování	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% maximální dodávky	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Obrázek 4: Epic a Bitcoin



VII. Mining

Epic Cash blockchain usiluje o decentralizaci tím, že přivítá širokou škálu výpočetního hardwaru. Epická těžba je zpočátku dostupná pro procesory, GPU a ASIC, a to pomocí tří příslušných algoritmů hashingu: RandomX, ProGPow a CuckatoO31+. Algoritmy mohou být triviálně vyměněny za tepla, aniž by byla ohrožena integrita řetězu.

1 RandomX a CPU

RandomX je algoritmus proof--of-Work (PoW) optimalizovaný pro všeobecné procesory. to používá randomizované spuštění programu s několika paměťovými technikami k dosažení následujících cílů:

- Prevence vývoje jednočipových ASIC;
- Minimalizujte výhodu efektivity specializovaného hardwaru oproti univerzálním procesorům.

Mining Epic s procesory vyžaduje souvislé přidělení 2 GB fyzické paměti RAM, 16 KB L1 cache, 256 KB L2 cache a 2 MB L3 cache na mining thread[13]. Zařízení se systémem Windows 10 vyžadují 8 GB nebo více paměti RAM. Časná integrace CPU v mining síti Epic Cash je vynikající příležitostí pro mnohé s pouze skromnými výpočetními prostředky, jak získat blokové odměny tím, že pomáhá zabezpečit síť Epic Cash.

2 ProgPow a GPU

Programová proof-of-work (ProGPOW) je algoritmus, který závisí na šířce pásma paměti a základním výpočtu randomizovaných matematických sekvencí, který využívá mnoha výpočetních funkcí GPU a efektivně tak zachycuje celkové náklady na energii hardwaru. Vzhledem k tomu, že ProGPOW je speciálně navržen tak, aby plně využil komoditních GPU, je obtížné a nákladné dosáhnout výrazně vyšší efektivity prostřednictvím specializovaného hardwaru. Algoritmus ProGPow tak zmírňuje pobídky pro velké skupiny ASIC k překonání grafických procesorů, jak je často vidět u mnoha jiných algoritmů PoW, jako je SHA-256 Bitcoin. GPU, i když nejsou tak převládající jako procesory, jsou stále běžně k dispozici. Díky technologickému vývoji řízenému pohonnými domy, Nvidia a AMD jsou GPU schopny paralelně zpracovávat mnoho násobků těžebních řešení nad procesory na jednotku. Je to kvůli této kombinaci všudypřítomnosti a vysokého výpočetního výkonu, že GPU poskytne páteř velké části mining činnosti během počátečních epoch, jak je uvedeno v tabulce 2.

3 CuckATOo+31 a ASIC

CuckatoO31+ je ASIC přátelská permutace algoritmu Cuckoo Cycle vyvinutý nizozemským počítačovým vědcem John Tromp. Relativní z ASIC rezistentní CuckaRoo29, CuckatoO31+ generuje náhodné bipartitní grafy a představuje horníky s úkolem najít smyčku dané délky 'N' procházející vrcholy tohoto grafu.

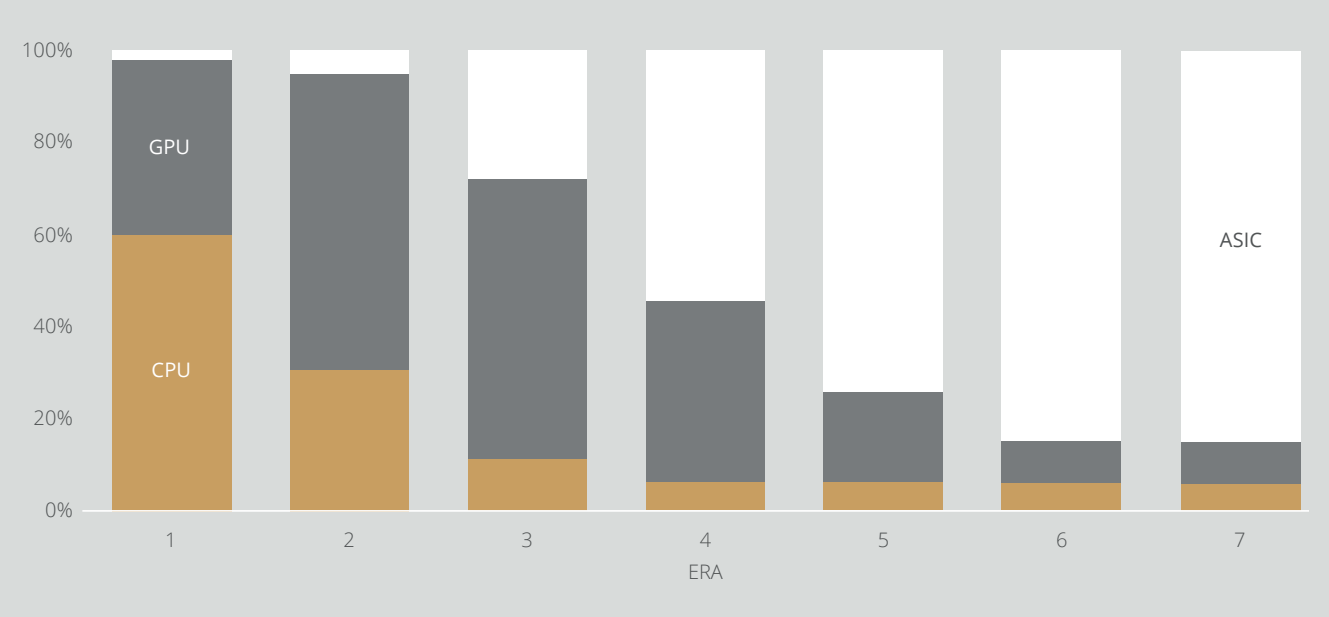
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Jedná se o úkol vázaný na paměť, což znamená, že doba řešení je vázána šířkou pásma paměti spíše než hrubým procesorem nebo rychlostí GPU. Výsledkem je, že algoritmy Cuckoo Cycle produkují méně tepla a spotřebovávají podstatně méně energie než tradiční algoritmy PoW. ASIC šetrný k Cuckatoo31+ umožňuje zlepšení efektivity oproti grafickým procesorům pomocí stovek MB SRAM a zároveň zůstává v paměti I/O.[14]. V konečném důsledku nabízejí ASIC největší potenciální úspory z rozsahu tří možností mining. V zájmu inkluzivity, ačkoli jsou jim přidělena malá část těžebních odměn vzhledem k CPU a GPU brzy, nakonec ASIC přebírají většinový podíl na odměnách mining bloků, za předpokladu, že pro CuckATOO31+ bude existovat konkurenční ekosystém výrobců zařízení.

Tabulka 2: Odděly odměn za mining pro každou éru podle tabulky 2. podléhá revizi. Přidělení budou zaměřeny na dosažení maximální decentralizace a v souladu s dlouhodobými zájmy sítě.

Era	1	2	3	4	5	6	7
Days	334	470	601	800	1019	1460	1460
CPUs	60%	30%	10%	5%	5%	5%	5%
GPUs	38%	65%	62%	40%	20%	10%	10%
ASICs	2%	5%	28%	55%	75%	85%	85%

Obrázek 5: Odděly odměn za mining pro každou éru podle tabulky 2. podléhá revizi.



[14] Le Sceller, Quentin, ***An Introduction to Grin Proof-of-Work,*** 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 Mining Příspěvky

Počínaje Epic Genesis (2019) a uzavřením na epické singularitě (2028) se během těžebního procesu přiděluje Epic, který je přesměrován jako důlní příspěvek na Nadaci EPIC Blockchain.

Nadace EPIC Blockchain se věnuje technickému rozvoji a podpoře povědomí a užitečnosti projektu Epic Cash v prvních letech svého vzniku vytvořením marketingových aktivit a rozvíjením partnerství v rámci odvětví finančních technologií.

Po singularitě převezme roli nadace EPIC Distributed Autonomous Corporation (EDAC) EPIC Distributed Autonomous Corporation (EPIC Distributed Autonomous Corporation), kterou nadace vyvine před předáním.

Nadace EPIC Blockchain je financována z procentního podílu odměn za těžbu odečtených z blokových odměn podle těchto ročních sazeb:

Table 3: Roční sazby příspěvků na těžbu nadace jako procento odměn za mining.

Rok	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% of Mining Odměn	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Závěr

Epic si klade za cíl být uznán jako „decentralizované digitální stříbro“, médium výměnného protějšku k uznávané pozici Bitcoinu coby decentralizovaného digitálního zlata. Opětovným zavedením ztracené zastupitelnosti na mnohem energeticky efektivnější a ekologicky šetrnější hardwarové páteři, Epic Cash naklání rovnováhu energie zpět ve prospěch jednotlivých uživatelů, v ostrém kontrastu s nedávnými centralizovanými trendy. Kombinace Bitcoinové ekonomie, teorie her a osvědčeného vzorce dokazování práce s nejlepšími technologiemi blockchain vede k nedůvěrné, neměnné a decentralizované měně (Epic), která je škálovatelná, zastupitelná a chrání soukromí svých uživatelů. Epic Cash blockchain je otevřený, veřejný, bez hranic a cenzuře odolný. Zachovává soukromí a bohatství svých uživatelů a odměňuje ty, kteří nasazují svůj hardware na podporu sítě prostřednictvím Mining. Každý Epic se těží do existence přes proof of work. Dodávka začíná na nulu a síť je považována za spravedlivou spuštěnou, s funkčním testnet v současné době běží.

Epic Cash fakta:

- **Mining začíná srpna 2019.**
- **Epic Cash blockchain je založen na MimbleWimble.**

  Definující vlastnosti protokolu jsou:

  1. **Cut-Through** – odstranění nadbytečných informací z blockchainu za účelem podpory efektivity vesmíru, podpory široké účasti na ověřování sítě a decentralizace správců;
  2. ***CoinJoin*** – sdružování transakcí v rámci bloku s cílem zajistit zastupitelnost kryptoměny Epic;
  3. ***Dandelion++ Protokol*** – šíření transakcí prostřednictvím komunikace mezi propojenými kanály a šíření napříč širokou sítí uzlů, které oddělují spojení mezi transakcemi a jejich původ;
  4. **Žádné adresy peněženky** – použití velkého vícenásobného podpisu k vytvoření soukromých klíčů na jedno použití pro transakční strany, čímž se zcela eliminuje potřeba adresy peněženky.

- **Měnová politika Epic Cash** je navržena tak, aby synchronizovala Epic cirkulující zásobu s oběžnou nabídkou Bitcoinu za zhruba devět let a dosáhla stejné maximální nabídky 21 milionů jednotek ve stejnou dobu jako Bitcoin, v roce 2140. This decreasingly inflationary policy guarantees transparency, predictability of supply, and scarcity, fostering the security of long-term value storage.

- **Mining**, který obsahuje procesory, GPU a ASIC prostřednictvím odpovídajících algoritmů RandomX, ProGPoW a CuckatoO31+, aby usnadnil hromadné přijetí a efektivitu sítě.

IX. Technické specifikace

Názevprojektu: Epic Cash
NázevCurrency: Epic
Doba bloku: 60 sekund
Velikost bloku: 1 MB
Počáteční Zásobování: 0
Finálová Zásobování: 21,000,000
Genesis bloku: . srpna 2019
Consensus: RandomX (CPUs), ProgPow (GPUs) a CuckAToo31+ (ASICs)

Links:

www.epic.tech

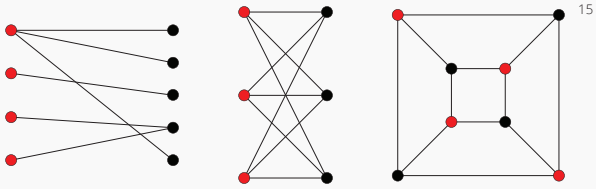
t.me/EpicCash – Telegram

t.me/EpicCashCzech

X. Slovníček

ASIC Aplikace specifické integrované obvody; čipy, které jsou určeny pro singulární účely sadu

Bipartite Graf grafických vrcholů rozložených do dvou disjunktní sady tak, že žádné dva graf vrcholy v rámci stejné sady jsou přilehlé.



Blinding Faktor náhodný prvek vložený do digitální zprávy s cílem usnadnit šifrování; sdílený tajný klíč mezi oběma stranami, který šifruje vstupy a výstupy v dané konkrétní transakci, jakož i veřejné a soukromé klíče transakčních stran[16].

Odměna blok nový Epic distribuován sítí jako odměny za výpočty provedené za účelem ověření transakcí v rámci nového bloku.

Cache hardwarovou nebo softwarovou komponentu, která ukládá data tak, aby budoucí požadavky na tato data mohly být doručovány rychleji.

Circulating Zásobování množství Epic v existenci v daném okamžiku.

CPU Central Processing Unit: počítačová komponenta odpovědná za interpretaci a provádění většiny příkazů z jiného hardwaru a softwaru počítače.

Cut-Through proces MimbleWimble blockchain, při kterém jsou odebrány vstupy a odpovídající vynaložené výstupy, aby se uvolňovalo místo uvnitř bloku, čímž se snižuje množství dat potřebných k uložení v blockchain.

Decentralization stav rozptýlení provozu a správy sítě.

Emission vytvoření nového Epic získaného horníky v bloku odměn. Epic se vytváří každých 60 sekund, protože transakce jsou potvrzeny do blockchainu

Epic Singularity bod, ve kterém se Epic cirkulující zásoba synchronizuje s oběžnou zásobou Bitcoin (květen 2028).

Přebytek(MimbleWimble) majetek zboží nebo zboží, jehož jednotlivé jednotky jsou v podstatě zaměnitelné, a každá jeho část je nerozeznatelná od jiné části.

Fungibility majetek zboží nebo zboží, jehož jednotlivé jednotky jsou v podstatě zaměnitelné, a každá jeho část je nerozeznatelná od jiné části.

Genesis (Event) těžba prvního Epic bloku a oficiální založení blockchan

GPU Graphics Processing Unit: Jednotka obsahující programovatelný logický čip (procesor) specializovaný na funkce zobrazení. Spotřebitelské GPU mohou být vhodné pro těžbu kryptoměn.

Halving (for Bitcoin) se vyskytuje každé 4 roky. Míra dodávek se po každé události na polovinu snižuje o 50%.

Hash hodnota vypočtená ze základního vstupního čísla pomocí funkce hashing.

Hashing Algorithm (funkce) matematický algoritmus, který mapuje data libovolné velikosti na hodnotu hash pevné velikosti používanou pro generování a ověřování digitálních podpisů, ověřovacích kódů zpráv (MAC) a dalších forem ověřování.

Homomorphic Encryption způsob provádění výpočtů na šifrovaných informacích bez jejich dešifrování. (v programování)

Immutability stav, ve kterém objekt nemůže být po jeho vytvoření změněn.

Input (MimbleWimble) součást transakce MimbleWimble reprezentující odesílající stranu transakce; vytvořená z výstupů předchozích transakcí.

I/O input/output; komunikace mezi systémem zpracování informací, jako je počítač, a vnějším světem, případně člověkem nebo jiným systémem zpracování informací.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction

Maximální Zásobování	množství Epic, které má být dosaženo, v tomto okamžiku se oběhová nabídka dále nezvýší (21 000 000 000 Epic).
Memory-Hard	použití velkého množství paměti RAM, aby se vyloučilo souběžné souběžné pokusy o připojení. Paměťově náročné funkce jsou algoritmy, které mají výpočetní časy primárně rozhodované dostupnou pamětí pro uložení dat. Také známé jako funkce vázané na paměť.
Merkle Tree	datová struktura používaná v aplikacích informatiky. V blockchainu umožňují Merkle stromy efektivní a bezpečné ověření obsahu ve velkokapacitě dat
MimbleWimble	protokol předložený pseudonymním přispěvatelem, který přezdívka Tom Elvis Jedusor, v chatovací místnosti pro vývojáře Bitcoin.
Multisignature	schéma digitálního podpisu, které umožňuje skupině uživatelů podepsat jeden dokument. Algoritmus vícepodpisu obvykle vytváří společný podpis, který je kompaktnější než kolekce odlišných podpisů od všech uživatelů[17].
Node	počítač, který se připojuje k síti blockchainu a rozvětví do jiných uzlů v síti, aby distribuoval informace o transakcích a blocích způsobem peer-to-peer.
One Way Aggregate Signature (OWAS)	transakční podpis složený z mnoha podpisů, který je šifrován způsobem, takže je velmi obtížné vypočítat jednotlivé podpisy, které jsou součástí agregátu
Output (MimbleWimble)	složka transakce MimbleWimble, která představuje přijetí transakce; používá se jako vstupy pro následné transakce.
Pedersen Commitment Scheme	kryptografický primitiv, který umožňuje prover zavázat se k zvolené hodnotě, aniž by odhalil jakékoli informace o této hodnotě a aniž by byl schopen zrušit závazek k hodnotě.
Soukromý klíč	soukromý klíč je malý kousek kódu, který je spárován s veřejným klíčem pro spuštění algoritmů pro šifrování a dešifrování textu. Je vytvořen jako součást kryptografie veřejného klíče během asymetrického šifrování klíčů a používá se k dešifrování a transformaci zprávy do čitelného formátu.
Proof of Work (PoW)	údaj, který je obtížně (nákladný a časově náročný) vyráběný, ale pro ostatní je snadno ověřitelný a který splňuje určité požadavky. Doklady práce se často používají při generování kryptoměna bloku.
Veřejný klíč	veřejný klíč je vytvořen v kryptografii veřejného klíče, který používá asymetrické šifrovací algoritmy. Veřejné klíče se používají k převodu zprávy do nečitelného formátu.
RAM (Random Access Memory)	čipy s rychlým přístupem pro ukládání dat ve výpočetním zařízení, kde jsou uchovávány operační systém (OS), aplikační programy a data, která jsou v současné době používána, takže je lze rychle dosáhnout procesorem zařízení.
Rangeproof	ověření závazku, které ověřuje, že součet vstupů transakce je větší než součet výstupů transakce a že všechny hodnoty transakce jsou kladné. Rozsahy zajišťují, že peněžní zásoby nebyly manipulovány.
(Digital) Podpis	standardní část protokolu blockchainu, která se používá hlavně pro zajištění transakcí a bloků transakcí, předávání informací, správu smluv a všech dalších případů, kdy je důležité zjistit a zabránit jakékoli vnější nedovolené manipulaci. Poskytují tři výhody ukládání a přenosu informací o blockchainu: • Odhalí, zda byly odesílané údaje manipulovány; • Ověřuje účast určité strany na transakci • Může to být právně závazné.
SRAM (Static Random Access Memory)	Random Access Memory (RAM) , který uchovává datové bity ve své paměti tak dlouho, dokud je dodáván napájení.
Throughput	míra transakcí za sekundu, která může být provedena daným kryptocurrency protokolem.
Trustlessness	kvalita kryptoměna sítě dodržovat pravidla protokolu bez vynucování ústřední stranou.

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA***, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPICKÉ SOUKROMÉ INTERNETOVÉ HOTOVOSTI