uPlexa

Motivujeme k využití masivní výpočetní kapacity ekosystému zařízení IoT pro zprovoznění blockchainové infrastruktury anonymních plateb s prohlížečovým rozhraním.

Omezení odpovědnosti:

Čtete verzi dokumentu White paper ze dne 26. listopadu 2018. Budoucí změny obchodních, technických a právních struktur jsou vyhrazeny. Aktuální verzi tohoto dokumentu White paper naleznete na webových stránkách uPlexa.

Obsah

Úvod a vize

uPlexa je elektronický platební systém typu peer-to-peer, který se zaměřuje na využití potenciálu konceptu IoT a dále na anonymitu používání. Systém uPlexa je založen na svém vlastním blockchainu, který využívá upravenou verzi algoritmu CryptoNight. Byl vyvinut se záměrem integrovat celkovou výpočetní kapacitu zařízení IoT (internet věcí) do jediného celku k zajišťování anonymních platebních transakcí, a to zejména pro účely poskytovatelů internetových a telekomunikačních služeb. Další prioritou je podpora anonymního elektronického obchodování. V letošním roce (2018) je ve světě provozováno více než 9 miliard zařízení IoT a pro rok 2020 se očekává překročení počtu 20 miliard zařízení.

uPlexa je podobně jako Bitcoin elektronickým platebním systémem typu peer-to-peer (p2p). uPlexa však zároveň podporuje anonymní platební transakce a ziskové těžení transakcí prostřednictvím zařízení IoT. uPlexa odolává nasazení specializovaných těžebních zařízení ASIC a klade si za cíl stát se nejziskovějším platidlem těženým provozovateli zařízení IoT s využitím určité části nevyužité výpočetní kapacity. Blockchain uPlexa bude přímo přístupný a bude možné jej těžit prostřednictvím webu bez nutnosti stahování jakýchkoli externích prostředků. Ke stažení však budou rovněž poskytnuty samostatné programy.

V prosinci roku 2017 jsme byli svědky dosud nejrozsáhlejšího přijetí kryptoměny, konkrétně měny Bitcoin. V té době Bitcoin nebyl připraven k využití takto vysokým počtem uživatelů a docházelo proto k výraznému přetížení platební sítě, což vedlo ke zpomalení doby vyřizování transakcí a k výraznému zvýšení poplatků. uPlexa tyto problémy řeší předem nasazením původního modelu NZCM (model téměř nulové zahlcení). Model NZCM staví na vysoké kapacitě hashování (klasifikace výsledků použití hashovací funkce) vzniklé koncentrací výkonu vysokého počtu zařízení IoT a zároveň na řízení četnosti mikroplateb zvyšováním poplatků pro tyto mikroplatby s růstem objemu síťových transakcí. Naopak veškeré platby, jež nebudou spadat do kategorie mikropateb, budou mít vždy poměrně nízké poplatky. Model NZCM bude rovněž používat rozhraní API uPlexa k využívání externích transakcí (transakce mimo vlastní blockchain) pro náročnější uživatele systému uPlexa. Toto je pouze několik nejpřehlednějších vrstev modelu NZCM. Další informace o modelu NZCM naleznete na straně 6.

Anonymita a soukromí patří mezi nejzávažnější témata kryptoměnových debat. uPlexa používá algoritmus CryptoNight k zajišťování nevysledovatelných soukromých transakcí. Pomocí systému uPlexa chceme zajistit anonymitu platbám směřujícím k poskytovatelům internetových a telekomunikačních služeb a elektronickému obchodování. Tohoto cíle dosáhneme vyjednáním smluv s poskytovateli připojení k internetu a dalších telekomunikačních služeb, jakož i zpřístupněním své vlastní platformy elektronického obchodování (eCommerce), a zajistíme tak podporu pro anonymní transakce a anonymní obchodníky, a zároveň (v rámci své sítě) znemožníme uchovávání a prodej osobních údajů pro marketingové účely a jakékoli jiné potenciální zneužití.

Princip činnosti – Model IoT (základní funkce)

uPlexa využívá upravenou verzi algoritmu CryptoNight k zajištění nekompromisní bezpečnosti a anonymních platebních transakcí. Při provádění vlastní analýzy výchozího algoritmu CryptoNight s ohledem na naše záměry jsme brzy zjistili, že těžení výchozího algoritmu CryptoNight prostřednictvím zařízení IoT není přímo proveditelné ani ziskové. Úpravy algoritmu ziskovost těžení prostřednictvím zařízení IoT výrazně posilují. Na rozdíl od ostatních platebních systémů bude základní komunikační kapacita naší sítě realizována miliardami již dnes provozovaných zařízení IoT.

Naším hlavním záměrem je umožnit ziskové generování takového počtu platebních jednotek uPlexa, jenž umožní částečné hrazení energie spotřebovávané dotyčným zařízením IoT, a to těžebným využitím určité části nevyužité kapacity tohoto zařízení. V průmyslově vyspělých zemích se může zdát, že nejde o významná čísla. Nicméně v rozvojových zemích – odkud pochází většina zařízení IoT – lze tato zařízení pořizovat za příznivější ceny. Věnujme pozornost například uživatelům chytrých televizorů, chytrých chladniček, chytrých automobilů a různých kapesních zařízení v jihovýchodní Asii. Pokud by uživatelé v tomto regionu mohli realizovat zisk postačující přinejmenším ke hrazení části provozních nákladů těchto zařízení, poskytlo by jim to výraznou výhodu, protože měsíční náklady na elektrickou energii často činí až 20 % jejich příjmu.

Zamýšlíme podporovat naprostou většinu zařízení IoT vývojem specializovaného softwaru uPlexa pro jednotlivá zařízení k těžbě s využitím určité části nevyužité kapacity procesoru. Podíl využití může nastavovat uživatel v mezích, které zabrání v nadměrném využití uživatelského zařízení IoT. Budou podporovány tyto typy zařízení:

- Stolní počítače a notebooky
- Mobilní telefony a tablety
- Chytré televizory
- Chytré kuchyňské spotřebiče (chladničky, trouby, kávovary, sporáky atd.)
- Chytré automobily
- Zařízení Raspberry Pi
- Servery (datová centra a serverové farmy)
- Nově zaváděné typy zařízení IoT

Princip činnosti – Poplatky a model téměř nulového zahlcení (NZCM)

V zájmu prevence výrazného zahlcení sítě a zachování extrémně nízkých poplatků jsme vytvořili model, který nazýváme termínem Near-Zero Congestion Model (NZCM - model téměř nulového zahlcení) a který zahrnuje určitý počet vrstev:

- Koncentrace potenciálu masového zavádění zařízení IoT
- Využití rozhraní uPlexa NZCM API pro externí transakce (mimo základní blockchain)
- Omezování extrémně malých mikrotransakcí
- Zvyšování poplatků pro mikrotransakce

Díky ohromnému počtu již provozovaných zařízení IoT a očekávatelnému dalšímu rozšiřování těchto zařízení se vůbec nemusíme obávat, že bychom nezískali ohromnou kapacitu k provozu našeho blockchainu. Další přednost spočívá ve skutečnosti, že pro významné účely použití systému uPlexa bude možné využívat rozhraní NZCM API a vyhnout se tak použití blockchainu pro velkou část transakcí.

Rozhraní NZCM API umožní správcům webů, vývojářům aplikací a organizacím poskytovat svým uživatelům kredit, zatímco tito uživatelé se budou na základě vlastní úvahy rozhodovat pro těžení uPlexa za účelem využívání konkrétních informačních služeb, aplikací či obchodních služeb. Pokud se uživatel rozhodne k těžení pro určitou organizaci prostřednictvím rozhraní NZCM API, bude tato organizace plnit úlohu těžebního poolu.
Těžaři těží do jedné konkrétní peněženky, například do internetového obchodu. Všechny vytěžené mince budou odesílány dotyčné organizaci a nikoli jednotlivým těžařům.
Poté bude příslušná částka uPlexa poskytnuta jako kredit jednotlivým uživatelům v rámci použití platformy prostřednictvím našeho rozhraní API, a nikoli prostřednictvím samotného blockchainu. Když tedy uživatel utratí své natěžené uPlexa na jejich platformě, transakce nemusí projít přes blockchain a bude místo toho zpracována v databázi příslušné platformy.

Účelem použití systému uPlexa jsou zejména anonymní platby poskytovatelům internetu a dalších telekomunikačních služeb, jakož i elektronické obchodování. Mikrotransakce proto mezi hlavní priority nepatří. V budoucnu se chceme zaměřit na podporu mikrotransakcí systému uPlexa a dalších systémů CryptoNight v síti CryptoNight lightning. Protože však systém uPlexa neposkytuje přímou podporu mikrotransakcí, bude stanovena minimální částka, kterou bude možné v síti uPlexa posílat (nejméně 1 uPlexa). Tuto částku bude možné kvůli případné změně finanční hodnoty platidla uPlexa změnit vytvoření alternativní verze systému (tzv. fork). Pro mikrotransakce s objemem nižším než 5 uPlexa

bude uplatňován variabilní poplatek. Posíláte-li tedy méně než 5 uPlexa v situaci, kdy je síť zahlcována mikroplatbami, dojde ke zvýšení tohoto variabilního poplatku až na dvojnásobek sazby poplatku standardní platby. Účelem tohoto opatření je prevence útoků na síť a snížení četnosti mikroplateb v síti uPlexa. uPlexa nyní není kryptoměnou, která by se zaměřovala na mikrotransakce (transakce menší než 0,15 USD).

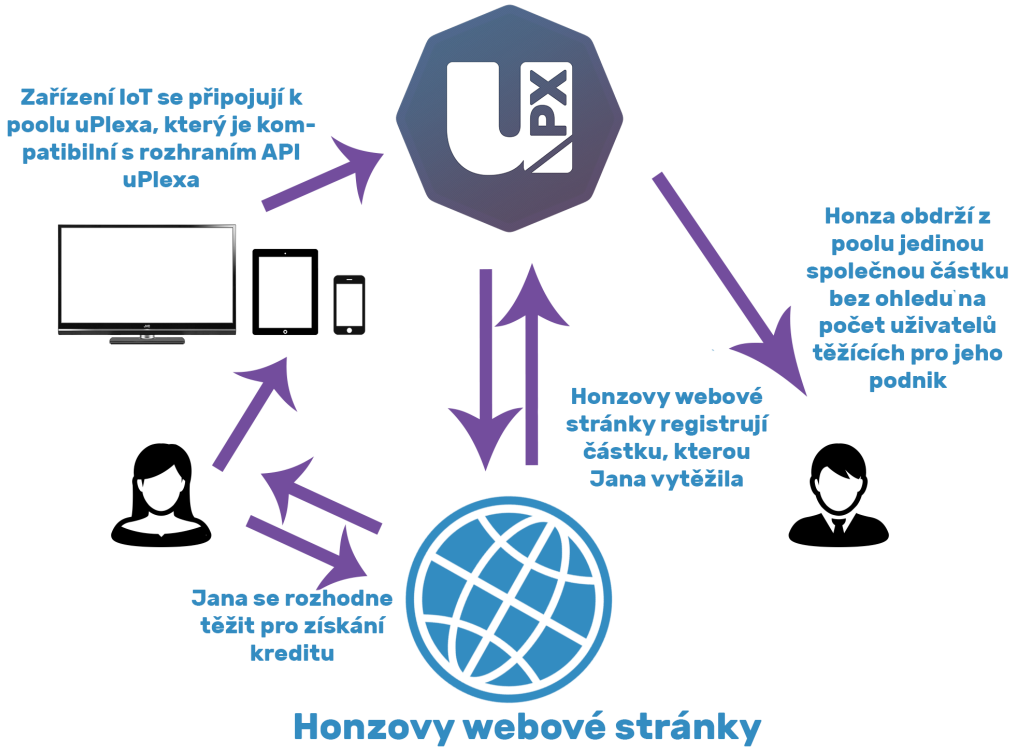
Rozhraní API pro model NZCM uPlexa

Rozhraní uPlexa API lze používat jako podporu prevence zahlcení sítě snížením počtu blockchainových transakcí, jež dále skýtá přednost snížení nákladů na poplatky pro jednotlivé podniky a projekty.

Princip činnosti

Představme si, že Honza – provozovatel webu honzuvweb.com, si přeje poskytovat kreditní systém svým uživatelům, který jim umožní nakupovat zde zboží a služby nebo poskytovat dary. Může své uživatele vyzvat k připojení jejich zařízení IoT ke své webové stránce na internetu k těžení mincí uPlexa. Na oplátku budou uživatelé odměněni kreditem webové stránky s využitím rozhraní uPlexa API. Poté co uživatelé vytěží dostatek Honzových kreditů, budou moci provést nákup nebo tyto kredity využít k získání slevy na Honzových webových stránkách.

Vytěžené mince se v rámci tohoto procesu zasílají do jediné peněženky, a to do do Honzovy peněženky. Nicméně jednotliví uživatelé a počty vyřešených hashů jsou sledovány prostřednictvím rozhraní uPlexa API. Chcete-li tedy uživatelka Jana provést nákup, dojde k odečtení příslušné částky z uživatelova zůstatku prostřednictvím rozhraní API a neprovádí se samostatná transakce přenosu částky z Janiny do Honzovi peněženky.



Úvod do elektronického obchodování (eCommerce)

Odvětví elektronického obchodování vykazuje globální příjmy převyšující 2,3 bilionu dolarů a odhady pro rok 2021 převyšují 4,88 bilionu dolarů. Zdroj: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

Tým uPlexa zpřístupní svou vlastní platformu elektronického obchodování založenou na masivní podpoře různých kryptoměn a státních měn, která bude dále používat síť uPlexa jako soukromou, bezpečnou a anonymní platební bránu pro provozovatele webů a jejich klienty. Po našich klientech, tj. po provozovatelích jednotlivých prodejních webů, nebudou požadovány žádné identifikační údaje, a tito klienti budou přijímat anonymní platby prostřednictvím sítě uPlexa. Na elektronickém tržišti budou provozovatelům webů k dispozici další nabídky, například vývojářské služby, softwarové pluginy a grafické služby. Klienti si budou moci tyto služby pořizovat pro své vlastní elektronické obchody prostřednictvím platidla uPlexa.

Systém elektronického obchodování uPlexa nebude svým uživatelům účtovat žádné poplatky, dokud se těmto klientům nepodaří provozovat ziskový obchod. To znamená, že že obchod je BEZPLATNÝ, dokud nezačne generovat nejméně trojnásobek měsíčního poplatku, který pro základní verzi obchodu bude činit přibližně 29 dolarů. Po překročení částky 29 dolarů budou platby prováděny každodenně. V ostatních případech budou platby prováděny jednou za dva týdny.

Náš tým dříve působil v odvětví elektronického obchodování a věnoval se zde veškerým aspektům technologií BigCommerce, Wordpress (WooCommerce) a Shopify. Budeme se zaměřovat na důslednou realizaci optimalizací a anonymních interakcí elektronického obchodování se záměrem překonání jiných stávajících systémů elektronického obchodování s využitím podnětů a stížností zákazníků, které tyto podniky dlouhodobě ignorovaly. Osobně jsme identifikovali řadu příležitostí ke zvýšení efektivity získávání zákazníků v uvedených systémech, které v těchto systémech nelze realizovat bez zásadních změn. Některé z těchto podnětů jsou v současné době plně využívány v zákaznických obchodech.

S přihlédnutím k výše uvedenému se tým uPlexa bude ve sféře elektronického obchodování zaměřovat na kryptoměny a na optimalizaci získávání platících zákazníků pro naše klienty.

Anonymita hrazení služeb

uPlexa překlene mezeru mezi anonymními platbami a poskytovateli služeb. Tohoto cíle dosáhne navázáním řady partnerství s programátorskými startupy, jež uživatelům umožní hrazení poskytovaných služeb bez ověřování identity při využití sítě uPlexa v roli alternativní platební metody.

Pro by se služby měly platit anonymně?

- Anonymita poskytuje ochranu před sledovacími programy, jejichž jediným cílem je odcizování soukromých informací.
- Pomáhá vás ochraňovat před prodejem údajů o vás pro marketingové a jiné nežádoucí účely
- Při cestování budete platit za služby v zahraničí bez turistických přirážek, protože uPlexa je globální měnou a nikdo nemusí vědět, odkud pocházíte
- Neumožněte dalším podnikům získat informace o tom, komu platíte nebo který podnik si kupujete
- Udržujte informace o svých dodavatelích v bezpečí
- Vyhněte se represi státních orgánů a zákazu určitých služeb
- Nenechte se vydírat od poskytovatelů připojení k internetu ani od zaměstnanců, kteří chtějí krást vaše data
- Plaťte za služby poskytované členům vaší rodiny ze svého vlastního účtu
- Hackeři nebudou moci spojit telefonní číslo s vaším jménem ani se zmocnit přístupu k vašemu telefonu s informacemi o vaší osobě pro získání přístupu k dalším vašim internetovým účtům

Anonymizační funkce systému uPlexa dalece překračují vlastní zdrojový kód do sféry velkých podniků a zásad upravujících identifikaci zákazníků a anonymitu. Nejobtížnější výzvou bude nalezení podniků a partnerů ochotných poskytovat bezpečnou a anonymní alternativu ke svým dosavadním systémům a službám. Proto klademe velký důraz na strategická partnerství a zároveň na motivující odměňování osob, které nám pomáhají s rozvíjením skutečného potenciálu systému uPlexa.

Uplatnitelnost a ziskovost internetu věcí (IoT)

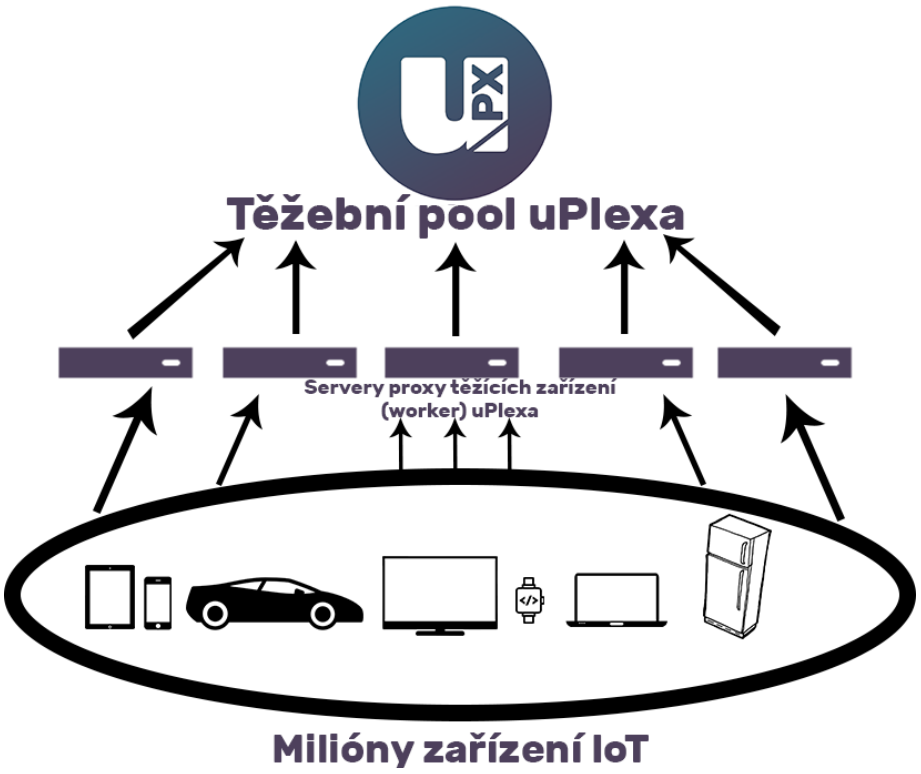
uPlexa zajistí umožní těžení na širokém spektru zařízení IoT: od chytrých telefonů a tabletů přes chytré televizory až po chytré automobily. Toto zajistí náš těžební software. Těžební software uPlexa využívá specifický soubor opatření, která ochraňují používaná zařízení před přehříváním a před narušením jejich funkčnosti omezením těžebného využití na určitou část nevyužité kapacity.
V rámci našich testů těžební software uPlexa obsazuje menší výpočetní kapacitu než běžně používané programy, jako například software k obsluze fotoaparátu či rozhraní portálů Facebook a Netflix.

Počty

Standardní chytrý mobilní telefon: 28 H/s na plný výkon nebo 10 H/s při 35% využití procesoru
Standardní notebook přibližně 45 H/s na plný výkon nebo 16 H/s při 35% využití procesoru

35% využití procesoru poskytuje střední hodnotu hashrate 13 H/s. Má-li Alice 15 zařízení, generuje hashrate a úrovni 13 * 15 = 195 H/s.

Tuto šetrnost k hardwarovým prostředkům umožňuje technologie vzniklá úpravou serveru pro sdružené těžení (tzv. pool) CryptoNight ve spojení s propracovaným protokolem serveru proxy, který snižuje počet spojení navazovaných s poolem. Díky našemu softwaru jsme schopni přijímat více než 2 milióny souběžných připojení na pěti instancích Amazon m5.2xlarge ve funkci serverů proxy a na dvou instancích Amazon m4.16xlarge (jedna je vyhrazena pro pool, druhá pro ověřování zaslaných výsledků a vyvažování pracovní zátěže).



Ziskovost těžení

Ziskovost zaštiťuje naše verze protokolu CryptoNight, kterou jsme vyladili v zájmu maximální profitability při zajištění anonymity těžení na zařízeních IoT. Protokol CryptoNight v současné době poskytuje obstojnou ochranu před použitím specializovaných těžebních zařízení ASIC. Nicméně v budoucnu mohou být pro vyloučení těžby zařízeními ASIC na naší platformě zapotřebí tvrdá rozdělení sítě (tzv. hardfork). Takovéto operace hardfork nebudou rušivá pro uživatele ani nebudou představovat žádné riziko.

Cílem našeho algoritmu je co nejpřesnější vzájemné vyvážení dolarové ziskovosti grafických karet a procesorů našich uživatelů. Základní představa těžení na zařízeních IoT předpokládá vysoký počet zařízení IoT v celém světě, která jsou připojena a pomáhají minimalizovat centralizaci těžení a zároveň poskytují stabilní příjem svým provozovatelům jako odměnu za průběžnou podporu zpracování transakcí blockchainu uPlexa.

Díky systému uPlexa budou lidé moci používat blockchain, který umožňuje ziskové těžení platidla uPlexa po připojení k některému z veřejných poolů uPlexa. Rovněž budou mít možnost připojit se k poolu určitého podniku nebo webových stránek či herního serveru za účelem získání kreditu dotyčné platformy.

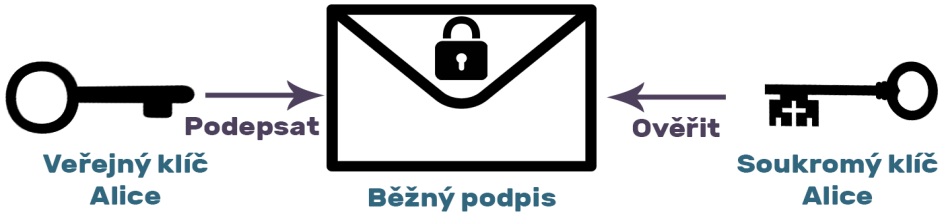
Technický výklad – Přehled algoritmu CryptoNight

Algoritmus CryptoNote

Algoritmus CryptoNote je šířen v souladu s podmínkami licence Open Source. My jsme jej upravili a začlenili do systému uPlexa, neboť jej považujeme za velmi solidní základ odolného a široce testovaného souboru základních kryptoměnových funkcí. Jde o stejnou základní blockchainovou technologii, kterou používají i měny Monero (jež patří mezi 10 největších kryptoměn) a Bytecoin (ta patří mezi 15 největších kryptoměn).

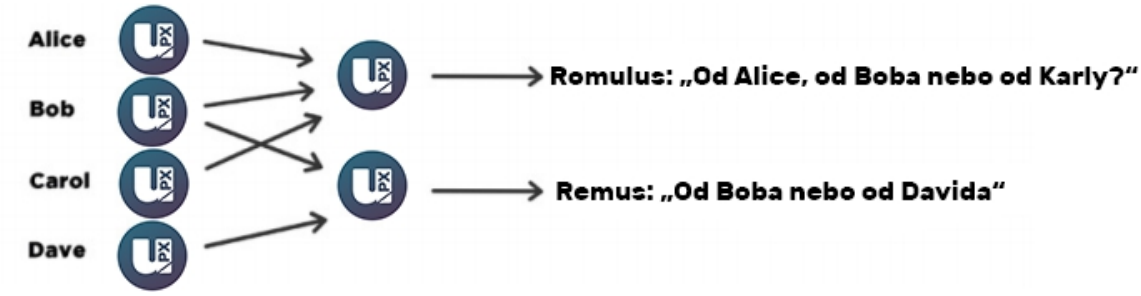
Nevysledovatelné platby

Běžný proces ověření digitálním podpisem (např. (EC)DSA, Schnorr atd.) zahrnuje veřejný klíč podepisující osoby.
Toto je nutná podmínka, protože podpis skutečně dokládá, že původce je držitelem příslušného tajného klíče. Nemusí však vždy jít o postačující podmínku.



Kruhový podpis (ring signature) je propracovanější schéma, jež může pro účely ověření vyžadovat více různých veřejných klíčů. Při použití kruhového podpisu máme skupinu jednotlivců a každý z nich má svůj vlastní veřejný a soukromý klíč. Podstatou tvrzení dokazovaného kruhovým podpisem je skutečnost, že osoba, která podepsala určitou zprávu, je členem dotyčné skupiny osob. Hlavní odlišnost od běžných schémat digitálního podpisu spočívá ve skutečnosti, že podepsaná osoba potřebuje jediný tajný klíč, avšak osoba ověřující platnost podpisu není schopna určit přesnou identitu této podepsané osoby. Pokud tedy dostanete kruhový podpis s veřejnými klíči Alice, Boba a Karly, můžete potvrdit pouze skutečnost, že jedna z těchto osob zprávu podepsala, avšak nebudete schopni určit, která k těchto osob tak učinila.

Tento koncept lze použít k vytváření nevysledovatelných digitálních transakcí odesílaných do sítě použitím veřejných klíčů ostatních členů skupiny kruhového podpisu pro dotyčnou transakci. Tento přístup prokazuje, že původce transakce je oprávněn k utracení částky uvedené ve transakci, ale identita průvodce zůstává neodlišitelná od identit ostatních uživatelů, jejichž veřejné klíče původce použil ve svých kruhových podpisech.



Nevysledovatelné transakce

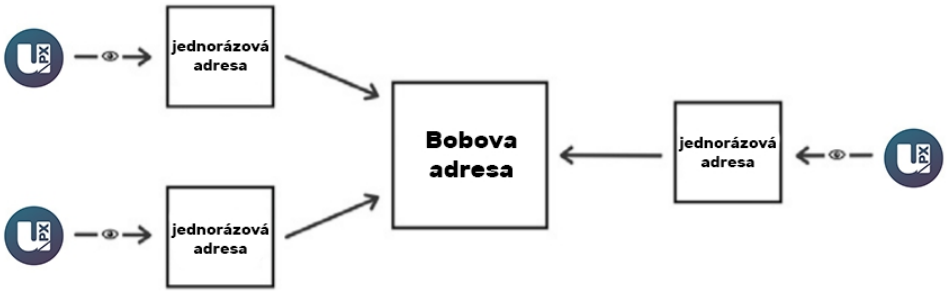
Je třeba uvést, že cizí transakce vás neomezují v utrácení vašich vlastních peněz. Váš veřejný klíč se může vyskytovat ve mnoha kruhových podpisech ostatních osob, avšak pouze jako maskovací prvek (a to samozřejmě i v případě, že jste již příslušný tajný klíč použili k podepsání své vlastní transakce). Dále platí, že i pokud dva uživatelé vytvoří kruhové podpisy s použitím identické množiny veřejných klíčů, podpisy budou vzájemně odlišné (nebudou-li používat shodný soukromý klíč).

Nekorelovatelné transakce

V běžném případě platí, že pokud zveřejníte svou veřejnou adresu, každý si může zobrazit všechny vaše příchozí transakce, a to i v případě, že jsou skryty za kruhový podpis. Chcete-li se této korelaci vyhnout, můžete vytvářet stovky klíčů a zasílat je osobám, od kterých přijímáte platby, nezávislým komunikačním spojením. To vás však zbavuje pohodlí jediné veřejné adresy.

Algoritmus CryptoNote systému uPlexa řeší toto dilema automatickým vytvářením jedinečných jednorázových klíčů pro jednotlivé platby p2p, přičemž tyto klíče jsou odvozovány z jediného veřejného klíče. Řešení spočívá v chytré úpravě protokolu Diffieho–Hellmanovy výměny klíčů. V původní verzi tento protokol dvěma stranám umožňuje vytvoření společného tajného klíče odvozeného z jejich veřejných klíčů. V naší verzi odesilatel použije veřejnou adresu příjemce a svá vlastní náhodná data k vygenerování jednorázového klíče pro platbu.

Odesilatel může vypočítat pouze veřejnou část klíče, zatímco příjemce může vypočítat soukromou část. Příjemce je tak jedinou osobou, která může provést uvolnění částky po potvrzení transakce. Pro ověření,
zda transakce náleží jeho osobě, musí provést pouze jednorázovou kontrolu. Tento proces zahrnuje jeho soukromý klíč a proto tuto kontrolu nemůže provádět nikdo jiný a nikdo jiný tak nemá možnost odhalit korelaci mezi jednorázovým klíčem, který byl vygenerován odesilatelem, a jedinečnou veřejnou adresou příjemce.



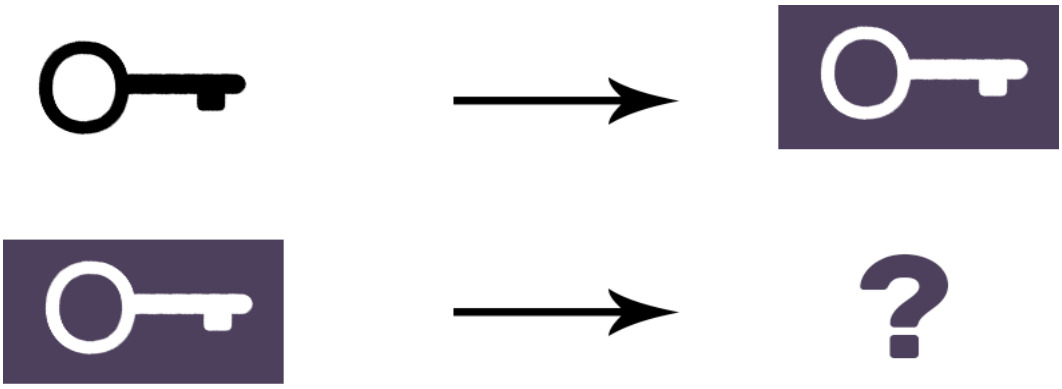
Důležitým prvkem našeho protokolu je použití náhodných dat na straně odesilatele. Výsledkem je vždy odlišný jednorázový klíč, a to i v případě, že odesilatel a příjemce jsou stejné osoby pro všechny transakce (proto jde o klíč „jednorázový“). Dokonce i když je příjemce a odesilatel totožnou osobou, všechny jednorázové klíče budou absolutně jedinečné.

Ochrana před dvojnásobným utrácením

Zcela anonymní podpisy by mohly umožňovat vícenásobné utrácení stejných finančních prostředků, což je samozřejmě v příkrém rozporu s veškerými principy platebního systému. Tento problém lze odstranit níže uvedeným způsobem.

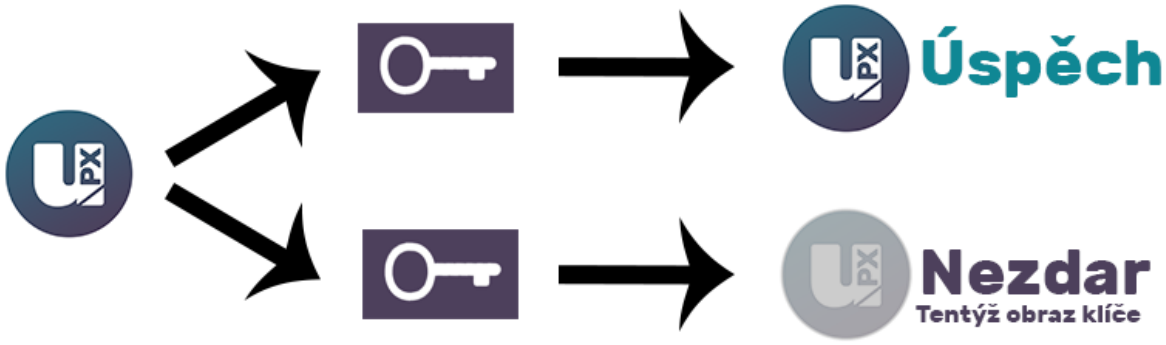
Kruhový podpis je třídou kryptografických algoritmů s různými vlastnostmi. Algoritmus používaný systémem CryptoNote uPlexa používá upravenou verzi "sledovatelného kruhového podpisu". Sledovatelnost jsme převedli na korelovatelnost. Tato vlastnost omezuje anonymitu podepsané osoby tímto způsobem: Pokud podepisující osoba vytvoří více než jeden kruhový podpis s použitím téhož soukromého klíče (množina cizích veřejných klíčů zde není důležitá), budou tyto podpisy vzájemně korelovány, což je příznak pokusu o dvojitou útratu.

K podpoře korelovatelnosti algoritmus CryptoNote systému uPlexa zavádí speciální příznak, který je vytvořen uživatelem při podepisování a který nazýváme termínem „obraz klíče" (key image). Jde o hodnotu jednosměrné kryptografické funkce pro tajný klíč, takže v matematickém smyslu jde skutečně o obraz (zobrazení) tohoto klíče. Jednosměrnost znamená, že z pouhého obrazu klíče nelze odvodit soukromý klíč. Rovněž je z výpočetního hlediska neproveditelná identifikace kolize (nalezení dvou různých soukromých klíčů, pro které funkce generuje stejný obraz). Při použití jiného než určeného vzorce se vygeneruje podpis, pro který ověření nebude úspěšné. S přihlédnutím ke všem činitelům lze říci, že obraz klíče je nevyhnutelný, jednoznačný, a přece zároveň anonymní příznak soukromého klíče.



Obraz klíče vygenerovaný jednosměrnou funkcí

Všichni uživatelé uchovávají seznam použitých obrazů klíčů (v porovnání s historií všech platných transakcí jsou nároky na úložný prostor zanedbatelné) a okamžitě zamítnou každý nový kruhový podpis s duplicitním obrazem klíče. Tato akce sice nezajistí identifikaci dotyčného uživatele, ale zabrání v každém pokusu o dvojité utrácení, který je způsobem nekalou motivací nebo chybami softwaru.

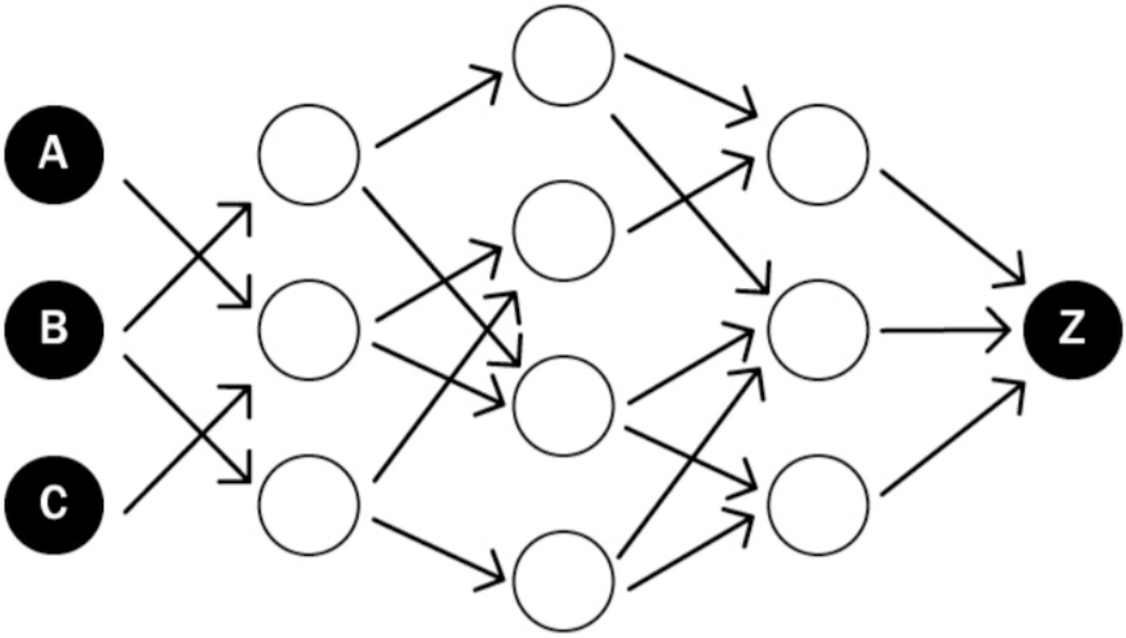


Odolnost vůči analýze blockchainu

Je k dispozici řada výzkumných zpráv, které se věnují analýze obsahu blockchainu měny Bitcoin. Jejich autoři sledují finanční toky, identifikují vlastníky finančních prostředků, zjišťují zůstatky na účtech a tak dále. Schopnost provádět takovéto analýzy je způsobena skutečností, že všechny přenosy mezi adresami jsou viditelné: každý vstup v každé transakci odkazuje na jedinečný výstup. Kromě toho uživatelé často k příjmu a zasílání finančních prostředků používají své adresy opakovaně, což práci analytiků usnadňuje. K tomuto dochází neúmyslně: Máte-li určitou veřejnou adresu (například pro dobročinné dary), používáte tuto adresu pro řadu vstupů a transakcí.

Algoritmus CryptoNote systému uPlexa je navržen s důrazem na zmírnění rizik, jež doprovázejí opakované používání klíčů a korelování vstupů s výstupy. Každá adresa pro platbu je jedinečný jednorázový klíč odvozený z dat odesilatele a příjemce. Pravděpodobnost druhého výskytu shodné adresy se rovná pravděpodobnosti kolize hashe o délce 256 bitů. Při použití kruhového podpisu ve vstupu dochází k nejistotě: který výstup byl právě utracen?

Pokusíme-li se nakreslit graf s adresami ve vrcholech a transakcemi na hranách, uvidíme stromovou strukturu: graf bez cyklů (protože žádný pár klíč/adresa není použit dvakrát). Dále platí, že existují miliardy možných grafů, protože každý kruhový podpis generuje víceznačnost. Z tohoto důvodu si nemůžete být jisti, od kterého odesilatele hrana/transakce směřuje k vrcholu/adrese. V závislosti na velikosti skupiny kruhového podpisu můžete odhadnout, že pochází od „jednoho (odesilatele) ze dvou“ nebo „od jednoho (odesilatele) z tisíce“. Každá další transakce zvyšuje entropii a klade analytikovi další překážky.



Standardní transakce protokolu CryptoNote

Standardní transakce CryptoNote v systému uPlexa se generuje níže uvedeným postupem, který popisujeme v tomto dokumentu White paper.

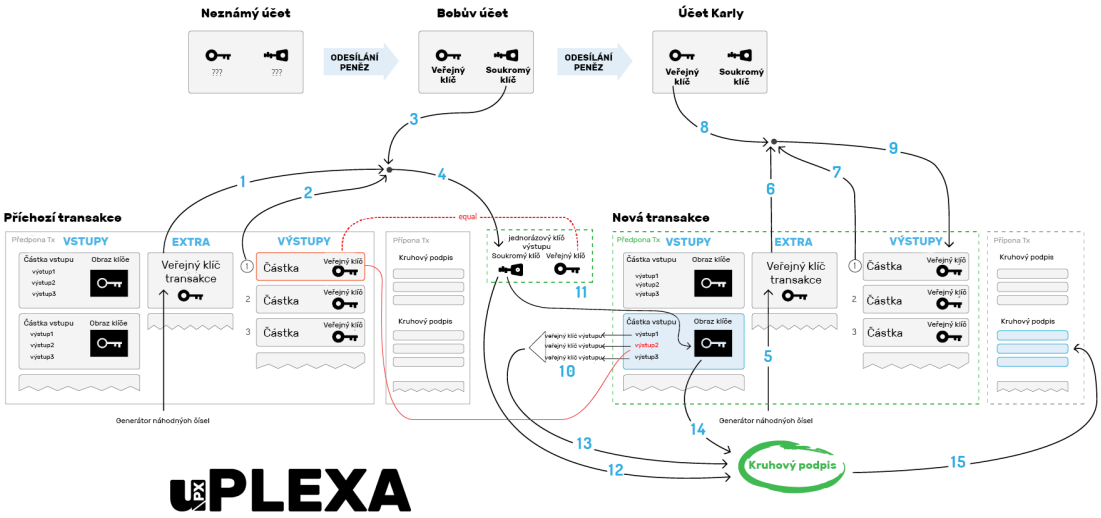
Bob se rozhodne utratit výstup, který byl odeslán do jednorázového veřejného klíče. K získání svého jednorázového soukromého klíče (4) potřebuje tyto údaje: Extra (1), TxOutNumber (2), a soukromý klíč svého účtu (3).

Při odesílání transakce Karle Bob vygeneruje svou hodnotu Extra náhodnou funkcí (5). K získání svého výstupního veřejného klíče (9) použije tyto údaje: Extra (6), TxOutNumber (7) a veřejný klíč účtu Karly (8).

Ve vstupu Bob skryje odkaz na svůj výstup mezi cizí klíče (10).

Jako prevenci dvojitého utracení rovněž přibalí obraz klíče odvozený ze svého jednorázového soukromého klíče (11).

Nakonec Bob podepíše transakci s použitím svého jednorázového soukromého klíče (12), všech veřejných klíčů (13) a obrazu klíče (14). Výsledný kruhový podpis připojí na konec transakce (15).



Přizpůsobivé mezní hodnoty

Decentralizovaný platební systém nesmí záviset na rozhodování jediné osoby, i kdyby tou osobou byl hlavní vývojář. Pevně stanovené konstanty a magická čísla v kódu odrazují od průběžného vývoje systému a proto je zapotřebí
se jim vyhnout (nebo je přinejmenším omezit na naprosté minimum). Každá zásadní mezní hodnota (například maximální velikost bloku nebo minimální výše poplatku) musí umožňovat dynamické stanovení na základě předchozího stavu systému. Proto se neustále interaktivně a nezávisle mění a umožňuje tak síti svůj vlastní nezávislý vývoj.

Algoritmus CryptoNote systému uPlexa je vybaven následujícími parametry, které se pro každý nový blok automaticky upravují:

1. Obtížnost. Obecnou myšlenkou našeho algoritmu je agregace sečtení objemu práce provedené uzly v průběhu posledních 720 bloků a vydělení této hodnoty časem, který byl na toto zpracování vynaložen. Míra práce odpovídá hodnotě obtížnosti pro každý jednotlivý blok. Čas se vypočítává tímto způsobem: seřadí se všech 720
časových razítek a odřízne se 20 % všech krajních hodnot. Interval zbývajících 600 hodnot je doba, která byla vynaložena na zpracování 80 % příslušných bloků.

2. Maximální velikost bloku. Nechť MN je medián velikostí posledních N bloků. Pevným limitem velikosti akceptovaných bloků je pak dvojnásobek hodnoty MN. Tato hodnota zabraňuje v nadměrném bobtnání blockchainu, avšak zároveň umožňuje postupný pomalý růst mezní hodnoty podle potřeby. Velikost transakce výslovně omezena být nemusí. Je vázána na velikost bloku.

Hladká emise

Horní mez celkového počtu všech digitálních platebních jednotek má rovněž v počítačovém světě dobře známou „digitální" hodnotu:

$M_{Supply} = (2^{64} - 1)$ atomických jednotek

Toto je přirozené omezení vycházející pouze z implementačních omezení, nikoli z úvah typu „N mincí by mělo
pro všechny". V zájmu optimalizace procesu generování nových mincí algoritmus CryptoNote systému uPlexa používá následující
vzorec k výpočtu odměn za blok:

$BaseReward = (M_{Supply} - A) >> 18$

kde A je množství dosud vygenerovaných mincí. Tento vzorec poskytuje předem odhadnutelný a plynulý růst počtu platebních jednotek (mincí)
bez prudkých změn.

Závěr

Projekt uPlexa se zaměřuje na zajištění anonymního platebního prostředku s možností využití ve funkci alternativy nezpoplatněných transakcí pro elektronické obchodování a platby poskytovatelům služeb. Tyto prostředky budou vybudovány na základních vrstvách hashovací kapacity masově nasazených zařízení IoT a transakcí mimo blockchain.

Reference

Dokument White paper systému Cryptonote:
https://cryptonote.org/whitepaper.pdf

Cryptonote Inside:
https://cryptonote.org/inside

Dokument White paper systému Bitcoin:
https://bitcoin.org/bitcoin.pdf

Statistica: Zařízení IoT připojovaná v letech 2015 - 2025:
https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

PRISM (sledovací program):
https://en.wikipedia.org/wiki/PRISM_(surveillance_program)

uPLEXA