Wietse Wind rozhovor
+ Marius Kramer, Dario Šuveljak a další

XRP
vládce kryptoměn

aneb ~~bitcoin~~ nemá důvod k existenci

„XRP je kryptoměna a digitální aktivum budoucnosti“

Ing. Petr Kulhánek

Digital Assets Capital

O autorovi

Ing. Petr Kulhánek

Jednatel Digital Assets Capital s.r.o., manažer fondu DAC,
vizionář, evangelista kryptoměn a blockchainu

Ano, vím. Tato kniha nepotěší příznivce bitcoinu. Osobně se zajímám o velké množství kryptoměn a především jejich případy užití v našem reálném světě.

Mnohokrát jsem vedl debatu s tzv. bitcoin maximalisty a zcela objektivně mne zajímaly případy užití bitcoinu pro svět plateb či jako digitálního zlata.

A pokaždé, když jsem porovnal výhody, funkce, technologii a případy užití bitcoinu a XRP, nenalezl jsem v podstatě nic, proč by XRP nemělo nahradit bitcoin a ten mohl přestat existovat.

Tato kniha je věnována XRP jako kryptoměně budoucnosti, kde se snažím vysvětlit důležité funkce, možné případy užití, předpověď budoucí hodnoty a ukázat, jak jsou XRP technologie a funkce potřebné v porovnání se zcela zbytečným BTC.

in petr@digitalassetscapital.eu

Obsah

1

Jak to vše začalo

Jak to vše začalo

Nebude to dlouhý román, jak jsem si oblíbil kryptoměny. Ale rád bych vám představil, jak jsem já sám pronikal na začátku do kryptoměn a jaké kroky a zkušenosti jsem nasbíral.

Píše se rok 2013 a existuje jen malé množství kryptoměn, samozřejmě bitcoin (BTC) a dále i jeho menší kopie litecoin (LTC).

Jelikož se pohybuji celý život v oblasti IT, zajímal jsem se i o digitální měny. Uvažoval jsem, k čemu to může být dobré. Tyto roky se teprve tvořil trh kryptoměn a jejich burzy. BTC byl spojen s darknetem a pochybnými transakcemi. Byl také znám jako velmi nestabilní a volatilní aktivum.

Lákala mne především možnost tzv. miningu. Tedy těžení. Proč? Hrál někdo z vás pamětníků na PC hru zvanou Duna 2?

Jednalo se o strategii, kde se těžilo koření a za něj se dále stavěly budovy a vyráběly stroje.

A teď si představte, že můžete konečně svůj do té doby nečinný počítač používat také k těžbě měny a tu potom prodat a proměnit v reálné dolary. A ono to funguje.

To je motivace. Vlevo vidíte moji grafickou kartu, ano, ta nejzákladnější, co mohla existovat, na které jsem těžil první BTC a později LTC. Jelikož jsem v roce 2013 již nebyl součástí herního světa, měl jsem jen obyčejně sestavené PC z obchodu.

Ale proč to celé zmiňuji? Jelikož toto nevýkonné PC neustále padalo, přerušil jsem těžbu LTC po 3 měsících a již nepokračoval. V té době jsem natěžil 4,2 LTC a 0,03 BTC pomocí Slush Poolu.

Jak to vše začalo

Pamatuji si na svůj vlastní komentář, potom co jsem zaplatil 100 EUR navíc za elektřinu: „Tak a teď mám po 3 měsících těžení a neustálých problémech s PC kryptoměnu litecoin v hodnotě 8 dolarů. “

V té době stál jeden LTC 2 dolary na burze. Opakoval jsem si, že je možné, aby cena vyrostla, ale nebylo vůbec jasné kdy a proč.

V dalších letech 2014 až 2016 jsem se více zajímal o technologii blockchain, která je tou primární ve světě kryptoměn.

Vždy mě zajímalo, jaké případy užití bychom mohli nalézt pro tuto jedinečnou a zcela neprobádanou technologii. Viděl jsem velkou příležitost.

Na druhou stranu, v těchto letech byly zdroje informací velmi omezené. Jednalo se převážně o diskuzní fóra nadšenců a spousta tipů či doporučení nevycházela z nějakého rozumného základu. Případně byly prostě špatně.

Na začátku roku 2017 jsem se aktivně pohyboval také ve světě obchodování komoditních futures kontraktů a stavěl automatické obchodní systémy na platformě Tradestation. A vzpomínám si, že v březnu toho roku jsem uvažoval o koupi ethereum (ETH) kryptoměny.

Chtěl jsem diverzifikovat svoje portfolio a zkusit jinou oblast než komodity. Když jsem se podíval na cenu ETH, byla na 30 dolarech. A pokud jsem šel několik měsíců zpět, tak cena byla jen na 8 dolarech. Říkal jsem si: „Mám to koupit za 6 či 8 tisíc EUR?“, ale cena se může propadnout zase zpět na 8 a níže a potom to bude velká ztráta.

Uvažoval jsem o této investici několik dní a nakonec jsem ETH nekoupil. A zde platí slavné úsloví: „Kdybych to jen býval věděl ☺“. Jelikož tuto knihu píši v roce 2020, z historie již víme, že rok 2017 byl v kryptosvětě naprosto šílený. Vygeneroval zatím největší cenovou bublinu na tomto trhu, a to na základě ničeho. Tedy žádných reálných úspěchů kryptoprojektů anebo skutečných případů užití.

V květnu 2017 došly všem obchodům grafické karty. Těžaři v honbě za zlatou horečkou kryptoměn vykoupili všechny GPU (grafické karty) a samotní skuteční hráči počítačových her je nemohli sehnat. Bitcoin se již nedal těžit pomocí GPU, ale na tzv. ASIC strojích. Ovšem ETH či jiné měny jako decred či ubiq stále poskytovaly zajímavý výdělek, jelikož cena mincí rostla.

Jak to vše začalo

A bylo to zajímavé. Rozhodl jsem se zapojit do těžby také, tentokrát již se silnějším hardwarem.

Svůj první mining rig (těžební stroj) jsem nakoupil přes mineshop.eu od chlapíka z Holandska, který je sám doma sestavoval, v podstatě na koleni. Cena byla také krásná, 1600 EUR za výkon 75 MH (MegaHash) při těžbě ETH. Tedy 6 méně výkonných grafických karet, zdroj, deska, paměť a speciální tlačítko na spouštění stroje. Navíc s předinstalovaným softwarem pro těžbu, simplemining. Tento software byl po čase zpoplatněn.

Po několika e-mailech ohledně nefunkčního stroje se mi podařilo toto speciální tlačítko připojit správně, během transportu se odpojilo, a stroj naběhl. První vystřízlivění přišlo, když jsem uviděl skutečný výkon těžby na ETH. Jelikož obtížnost vzrostla, vycházelo to na 2 ETH mince za rok (!) neustálého těžení a spotřeby elektřiny.

Motivace šla značně dolů, a to se jedna mince ETH prodávala za 400 dolarů. Přešel jsem tedy na tzv. hard fork ETH, a to kryptoměnu ubiq (UBQ).

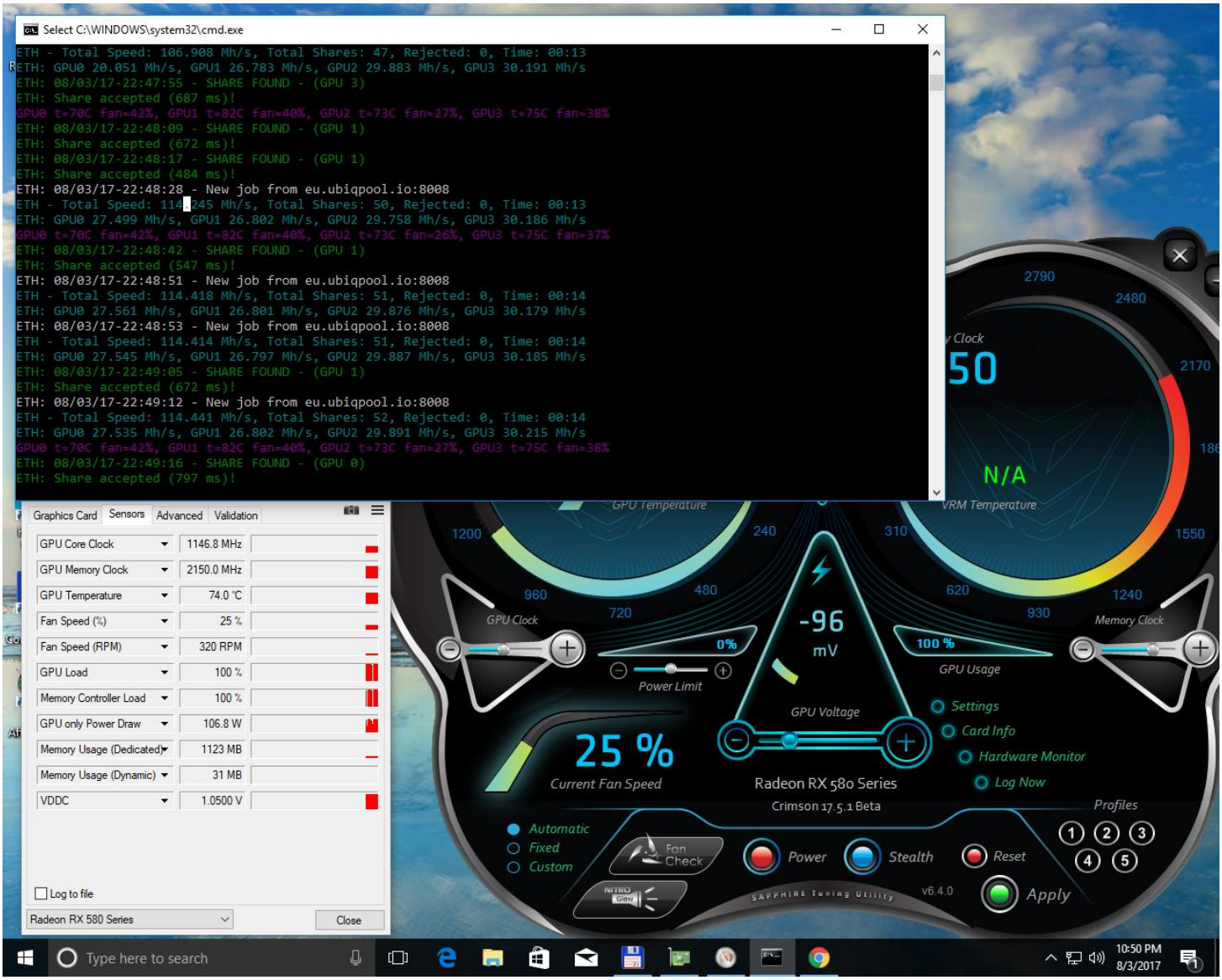
Důvodem, proč tento příběh zmiňuji, je fakt, že bych vám rád ukázal na své vlastní negativní zkušenosti, jak je celá idea těžení v podstatě neefektivní, zbytečná a neskutečně drahá. A navíc naprosto zbytečně zatěžuje naše životní prostředí spotřebou elektřiny.
Tuto nutnost těžby představuje konsenzus sítě nazývaný Proof of Work (PoW). A je to ten, který používá například bitcoin, bitcoin SV, ethereum (ethereum přejde v roce 2020 na PoS, což je Proof of Stake systém, a je daleko šetrnější ke spotřebě elektřiny).

Postupně, jak kryptohorečka narůstala, červen, červenec 2017, jsem vlastnoručně sestavil další dva těžící stroje z grafických karet RX 570 a RX 580 v celkovém počtu 6 karet na jeden stroj. K tomu bylo třeba dokoupit výkonné zdroje, základní desky...

A navíc tyto stroje by měly běžet nepřetržitě, tak aby stále těžily. Když si vzpomenu, jak v létě 2017 bylo i přes 30 stupňů ve stínu a já stále udržoval všechny 3 stroje v chodu a v noci přespával ve stejné místnosti, musím uznat, že to byla opravdu drsná zkouška vůle. Jelikož v této místnosti bez klimatizace a větráku mohlo být i 45 stupňů.

Ale to nejlepší mělo teprve přijít.

Jak to vše začalo



A takhle vypadala skutečná těžba a potvrzení od těžebního poolu o uznané práci a také odměně. Další aplikace sloužily k ladění výkonu a spotřeby elektřiny karet. Na této ukázce běží jen 4 karty ze 6. Největší zábava přicházela, když stroj některou z karet nerozpoznal a bylo třeba zkoušet různá nastavení základní desky, pročítat do úmoru diskuzní fóra a snažit se zbývající nečinné karty rozchodit.

Všimněte si času v dolním rohu. Tento printscreen jsem pořídil téměř v 11 hodin v noci a to byl standardní čas tuningu karet a sledování činnosti strojů.

Jak to vše začalo

Asi dva roky od zastavení těžby UBQ mincí v lednu 2020 jsem zdokumentoval pozůstatky těžebních strojů.

Některé GPU (grafické karty) jsem použil na vlastní PC a případně věnoval dalším, ale stejně mi jich ještě dost zbylo. Všimněte si, že jsem musel použít PSU (power supply unit) EVGA 1200, aby bylo možné napájet celý rig současně s 6 RX 580 kartami. Spotřeba elektřiny byla enormní. Ale o něco slabší zdroj se asi po týdnu chodu kompletně roztavil a shořel.

Když si porovnáte výkon zapnutého vysavače a jeho spotřebu a potom si uvědomíte, že by několik vysavačů bylo zapnutých nepřetržitě 24/7 po dobu celého roku, určitě se dostaví pocit nesmyslnosti PoW konsenzu a tohoto obrovského plýtvání elektřinou, jak to předvádí již více než 10 let bitcoinová síť.
Luxování 1 hodinu týdně stojí zhruba do 1000 Kč za rok. A teď si představte, že luxujete ne 52 hodin za rok, ale 8760 (24 hodin x 365 dnů) hodin ročně, krát tři za tři těžící stroje.

Co byla vlastně ta ubiq kryptoměna? Tedy ještě je, jelikož existuje i v roce 2020.

Ubiq poskytuje dvakrát rychlejší transakce a o 90 % stabilnější a zabezpečenější síť než ETH. Dále má síť sloužit k vývoji Dapps a smart kontraktů. Má také zajímavý on-chain governance systém založený na escher tokenech. Primární zaměření je na enterprise aplikace. Stránky Ubiq teamu i celková prezentace byly na úrovni. Team si žádné mince nenatěžil předem a jednalo se o zkušené vývojáře.

V roce 2017 bylo těžení UBQ zajímavé, jelikož obtížnost byla o hodně nižší než u ETH. Dokonce si pamatuji naši dovolenou na Krétě po dobu 10 dní, to se psalo září 2017, a já denně sledoval obtížnost sítě ubiqu, jelikož jsem musel vypnout všechny tři stroje. V této době ještě kryptobublina rostla a s ní i obtížnost těžby. A kdykoliv se obtížnost zvýšila, přemýšlel jsem, o kolik méně mincí natěžím po návratu.

Cena 1 UBQ mince byla touto dobou kolem 5 dolarů a její maximum na 7 dolarech. Vypadalo to jako dobrý nápad dále těžit. Ale to už se blížil konec roku 2017 a jeden z dlouhých medvědích trhů.

V srpnu 2018 jsem zastavil kompletně těžbu, ptáte se proč? Od ledna 2018 začala kryptobublina praskat a všechny měny ztrácely, a ubiq výrazně. Ale to nebylo hlavní příčinou. V červenci 2018 jsem opsal počet kilowatt hodin z našeho měřicího zařízení v domě a poslal na našeho poskytovatele elektřiny. A ještě k tomu to bylo v Německu, kde je elektřina jedna z nejdražších v celé Evropě.

Milé překvapení netrvalo dlouho. Nejdříve nás kontaktoval technik, že přijde sám zkontrolovat naše měřidlo, jelikož se mu zdá naše spotřeba elektřiny příliš vysoká. Neshledal závadu, ano, víme, nebyla tam. A následně mi přišel doplatek za elektřinu na 3000 EUR navíc k běžné spotřebě. Ještě v ten den jsem rozmontoval všechny stroje. A jako bonus se cena ubiq mince stále propadala, až na dnešních (k lednu 2020) 0,07 dolaru.

A to je už značný rozdíl oproti maximálním hodnotám. U ubiq platformy se začaly projevovat důsledky velmi malého teamu (5 lidí) a neschopnosti spolupráce platformy se skutečnými firmami a společnostmi, tedy vytvoření reálných případů užití.

Ubiq bohužel v ničem výrazně nepřekonává ethereum a oba projekty jsou ze staré PoW školy. Dnes máme spoustu blockchain projektů, které jsou mnohem rychlejší a škálovatelnější a nepoužívají PoW. Například tezos, EOS, cardano a samozřejmě XRP.

Proto i když mise od Ubiq teamu byla zajímavá, projekt nedokázal ničím zaujmout a předstihnout konkurenci. Tedy nemá důvod k existenci a cena UBQ kryptoměny může jít až na 0.

Ještě se podívejme na průběh ceny UBQ v čase. Vidíme, jak se cena v podstatě z ničeho dostala do spekulativních hodnot až 7 dolarů, a potom následně již jen klesala.

Možná si teď říkáte, kolik že jsem těch UBQ mincí nakonec natěžil? Je jich 1600. Stále je ještě mám a v dnešních cenách v lednu 2020 mají cenu kolem 120 dolarů. Proto tato lekce byla dostatečná k tomu, abychom mohli říci, že kryptoměny používající PoW v roce 2020 a dalších letech zde již nemají své místo z pohledu životního prostředí, efektivity a spotřeby zdrojů.

A proto zde máme XRP, které nepoužívá ani PoW a dokonce ani PoS k transakcím v síti.

Ještě se vraťme ke dvěma věcem.

Jistě si pamatujete, že jsem zmínil 4,2 LTC, které jsem natěžil v roce 2013. A tehdy měly tyto mince hodnotu 8 dolarů. V rámci kryptohorečky v listopadu 2017 jsem tyto mince prodal, nebylo to na úplném cenovém vrcholu, ale přesto se mi podařilo dostat za 1 LTC kolem 250 dolarů.

A to jsem ještě celé ty 4 roky měl těchto pár mincí v nezaheslované peněžence jen jako soubor na disku počítače. Ale i po těch letech byla peněženka funkční a lehce jsem LTC převedl na burzu Bitstamp a prodal.

Jedinou věcí, které jsem litoval, bylo, že jsem těch LTC za 2 dolary nenakoupil několik tisíc.

A ještě poznámka k ETH na ceně 30 dolarů. Tehdy jsem uvažoval, jestli to není již vysoká cena a nepůjde zase dolů. Jak již víme, čekalo nás zatím nejšílenější období kryptoměn v následujících 8 měsících a cena jednoho ETH se vyšplhala až na 1400 dolarů.

K dnešnímu dni v lednu 2020 je cena ETH kolem 160 dolarů.

Tyto cenové hladiny byly dosaženy při celkové tržní kapitalizaci všech kryptoměn na konci roku 2017 okolo 800 miliard dolarů. A to na základě čisté spekulace bez jakýchkoliv reálných příkladů používání kryptoměn.

A nyní si představme, že zde máme XRP, které si klade jako jeden z cílů vstoupit do světa cross-border plateb, odstranit nostro/vostro účty a stát se tzv. bridge měnou pro všechny ostatní kryptoměny včetně všech fiat měn a dalších tokenizovaných aktiv jako akcie či nemovitosti.

Zde už se nejedná o miliardy, ale biliony dolarů, které mohou být denně převáděny přes XRP Ledger. **K tomu bude zapotřebí, aby cena XRP výrazně vzrostla, aby XRP mince mohly pokrýt takovéto množství likvidity.**

2

Představme si XRP

Představme si XRP

Co je XRP Ledger?

Je to decentralizovaná kryptografická kniha (databáze), která běží na serverech sítě peer-to-peer.
XRP Ledger obsahuje jako nativní kryptoměnu XRP.

Co je XRP?

XRP je digitální aktivum (kryptoměna) vytvořené jako most k množství dalších měn k celosvětovému použití. XRP má sloužit k tzv. Internet of Value, tedy tak, aby bylo možné posílat peníze stejně rychle a snadno jako dnes posíláme informace.
X = ISO 4217 standard pro označení nestátních měn
RP = ze slov „ripple credits“ nebo zkráceně „ripples“

Kdokoliv má kryptografický klíč a připojení k internetu, může přijímat, držet a posílat XRP komukoliv dalšímu.

XRP jako kryptoměna má více velmi zajímavých charakteristik a vlastností:

- rezistentní zpracování transakcí vůči cenzuře,
- velmi rychlý a efektivní algoritmus konsenzu,
- konečné množství XRP mincí,
- odpovědné řízení vývoje XRP Ledger (open source),
- bezpečnou a adaptabilní kryptografii,
- moderní funkce pro smart kontrakty,
- přímo na XRP Ledger možnost vytvoření decentralizované burzy.

Toto je příklad spíše technických vlastností XRP a neméně zajímavé jsou také obchodní případy užití a další potenciální využití.
Například ve hraní počítačových her (gaming) a především jejich ekosystému nákupu virtuálních předmětů a plateb mezi hráči.

Skutečných případů užití si v této knize projdeme ještě velké množství. A bude to jízda.

Rezistentní zpracování transakcí vůči cenzuře

XRP je součástí nové třídy peněz. Ano, jsou to kryptoměny tak jako bitcoin.

XRP je decentralizované digitální aktivum, které existuje v počítačových systémech a není zde žádný centrální administrátor, tedy například nám dobře známá banka.
A jak víme, banka má skutečnou kontrolu nad našimi penězi uloženými na kontě u této banky.

Na druhou stranu, pokud se bavíme o skutečné a dostatečné decentralizaci, znamená to, že nikdo nemůže svévolně provést například vrácení transakcí, zmražení vkladů a účtů a případně zablokovat používání decentralizovaného digitálního aktiva.

Pokud se bavíme o digitálních aktivech, tak ty jsou přirozeně digitální, a proto mohou být použity v online prostředí bez jakýchkoliv omezení vzhledem ke vzdálenosti či zemi.

Fyzické peníze a mince, jako česká koruna, mohou být použity k platbám a obchodním transakcím bez centrální autority. Je to pěkné, ale neefektivní, jelikož nemohou být použity v online světě. A upřímně, pokud chcete provést peněžní transakci na delší vzdálenost či do jiné země, asi se vám nebude chtít vozit kufřík s několika miliony v papírových bankovkách.

Centralizované digitální měny potřebují administrátora, který schvaluje transakce. Tento administrátor, tedy například banka, může zastavit transakce, vrátit je nebo zakázat některým účastníkům provádění převodů peněz. A dokonce může peníze i zabavit. Na druhou stranu je tento systém digitální a lze provádět online transakce na dlouhé vzdálenosti.

A teď se vraťme k XRP, tedy decentralizovanému digitálnímu aktivu.

Spojuje výhody jak online možnosti transakcí peněz, tak i toho, že zde není žádná banka či administrátor.
XRP Ledger používá systém důvěryhodných potvrzovačů (validators) s malým zapojením lidské interakce, tak aby se autorita rozložila lépe než v jiných decentralizovaných systémech.

Hlavní rozdíl je v tom, že například v bitcoin síti se jedná o plně automatický systém dosahování konsenzu od neznámého počtu účastníků sítě, kteří mají výpočetní sílu podle koncentrace levné elektřiny. K tomu se ještě dostaneme, ale již dnes (leden 2020) mají těžební skupiny (pools) v Číně 65 a více procent výkonu celé těžební sítě, a tudíž se centralizuje rozhodovací právo k potvrzování transakcí. A jak víme, režim v Číně může relativně snadno rozhodnout o dalších krocích těchto skupin a případně je plně zakázat.

Ohledně XRP Ledger, společnost Ripple spravuje list prověřených validátorů, kteří pocházejí z různých firem a zemí. Proto se XRP Ledger může stát odolnější vůči cenzuře a případně vnějším tlakům než sítě založené na PoW těžbě.

Postupně Ripple jako společnost podle svojí decentralizační strategie spravuje méně validátorů, tak aby celá síť byla maximálně decentralizovaná. Mají pravidlo, že jeden potvrzovací uzel od Ripple bude nahrazen vždy dvěma novými od jiných prověřených společností. A to se jim velmi daří. V podstatě lze říci, že XRP Ledger je mnohem decentralizovanější než bitcoin a dále se tento rozdíl bude zvětšovat.

Velmi rychlý a efektivní algoritmus konsenzu

Asi jedním z největších rozdílů mezi XRP Ledger, to znamená i XRP kryptoměnou, a ostatními kryptoměnami jako bitcoin či ethereum, je, že používá unikátní konsenzus algoritmus, který nevyžaduje čas a především elektrickou energii k těžbě.

XRP Ledger konsenzus algoritmus není ani Proof-of-Work, ani Proof-of-Stake. Ale používá list důvěryhodných validátorů, kteří efektivně rozhodují, jaké se stanou transakce a v jakém pořadí.

Rozdíly mezi bitcoinem a XRP si ještě více rozebereme, ale již nyní můžeme říci, že potvrzení transakce na XRP Ledger trvá zhruba 4 sekundy v porovnání s někdy i hodinami na bitcoinové síti. A navíc k potvrzení transakce potřebuje XRP zanedbatelné množství energie.

Dále každá nová verze knihy (ledger) v XRP Ledger (něco jako ekvivalent k blokům) obsahuje aktuální a kompletní stav všech účtů, takže se server může synchronizovat se sítí v řádu minut. Namísto toho v bitcoinové síti je potřeba stahovat celou transakční historii, což trvá hodiny.

Konečné množství XRP mincí (tokenů)

Pokud se zamyslíme na tím, co způsobuje pád či zánik některé měny, může to být válečný konflikt nebo změna politického režimu. Ale asi nejčastějším důvodem je hyperinflace.

Co přesně znamená hyperinflace?
Je to inflace vyjádřená tří a víceciferným číslem (více než 100 %). Pro ekonomiku to znamená rozpad peněžního systému a zhroucení hospodářských vazeb. Peníze jsou znehodnocené, přestávají plnit svoji funkci – nejsou uchovatelem hodnoty, z výměnných procesů jsou vytlačovány výměnou zboží.

Jako příklad se můžeme podívat na bankovku Zimbabwe, která měla hodnotu
100 000 000 000 000 dolarů. A jejich hyperinflace dosáhla na konci roku 2008 231 milionů procent.

Zatímco decentralizovaný systém validátorů pomáhá XRP odolávat politickým tlakům, tak pravidla XRP Ledger poskytují jednodušší řešení hyperinflace.

A to tak, že množství XRP mincí je konečné, nelze vytvořit žádné další XRP mince do budoucna. A proto je XRP mnohem odolnější vůči hyperinflaci než jiné fiat měny a kryptoměny.

XRP má dokonce deflační chování. Tedy XRP mince v oběhu ubývají a žádné nové nemohou vzniknout. To znamená, že se bude XRP stávat v průběhu času více a více vzácné, a tudíž v závislosti na případech užití bude jeho hodnota růst.

Celkové množství vytvořených XRP mincí bylo 100 miliard. Ale ani toto číslo už neplatí, jelikož se již několik milionů mincí tzv. zničilo.

Podívejme se, jak se z XRP digitálního aktiva stává v průběhu času vzácná kryptoměna:

1. Posílání transakcí v XRP Ledger ničí malé množství XRP. Ten, kdo posílá transakci, vybírá, kolik se zničí. Jsou zde stanoveny minimální hodnoty v závislosti na vytíženosti sítě a odhadu náročnosti zprocesování transakce. Pokud je síť vytížena, tak ty transakce, které slibují vyšší množství zničených XRP, se mohou posunout k dřívějšímu zpracování. Toto je především anti-spam opatření, které by případný DDoS útok velmi prodražilo. Aktuálně nejnižší transakční poplatek je 0,00001 XRP (tzv. 10 kapek – drops).
2. Každý účet v XRP Ledger musí mít malé množství XRP mincí jako rezervu. Je to opět anti-spam opatření, tak aby se nevyplatilo držet příliš mnoho dat na XRP Ledger. XRP Ledger validátoři mohou hlasovat o množství XRP, které slouží jako rezerva. A to především s přihlédnutím ke skutečné hodnotě XRP mincí v reálném světě. V roce 2013 již jedno snížení proběhlo, a to z 50 na 20 XRP.
3. Společnost Ripple drží velké množství XRP v tzv. escrow účtech. Na začátku každého měsíce se uvolní 1 miliarda XRP z escrow účtu pro použití společností Ripple. Ripple používá XRP k růstu XRP Ledger ekosystému a prodává XRP institucionálním investorům. Dále Ripple prodává malé množství XRP na kryptoburzách, v porovnání s objemem transakcí na dané burze. Na konci každého měsíce se XRP, které nebylo prodáno, vrací na nový escrow účet na dobu 54 měsíců. K lednu 2020 má Ripple cca 50 miliard XRP na escrow účtech. XRP mince jsou uloženy na escrow účtech především z důvodu lepšího odhadu nabídky mincí v oběhu.

Odpovědné řízení vývoje XRP Ledger (open source)

XRP Ledger je software. Je to program a je pravdou, že na kvalitě programu velmi záleží, a tím pádem i na vysoké kvalitě programátorských týmů.
Ripple zaměstnává nejkvalitnější inženýry, kteří pracují na XRP Ledger softwaru a speciálně na hlavním serveru „rippled“ na plný úvazek. Důvod, proč toto zmiňuji, je, že v celém kryptosvětě k dnešku nenajdete dedikovanější, početnější a kvalitnější tým pracující full-time pro danou kryptoměnu, než je XRP. Zdrojový kód pro „rippled“ je k dispozici jako open source licence.

Ripple jako vlastník velkého počtu XRP mincí zajišťuje, aby XRP bylo používáno na mnoho způsobů a zároveň byly splněny zákonné podmínky a také podmínky udržitelnosti.

Ripple poskytuje technickou podporu společnostem a projektům, pokud chtějí pracovat s XRP Ledger a rozvíjet dále myšlenku Internet of Value.

A navíc Ripple spolupracuje se zákonnými zástupci a regulátory celosvětově, aby pomáhal vést a implementovat důležité zákony a pravidla ve světě digitálních aktiv a společných obchodních modelů.

Zastavme se na chvíli. Zamyslete se nad těmito větami. Ve světě kryptoměn je toto ojedinělý přístup. Ripple jako obchodní společnost spolupracuje s regulátory, centrálními bankami a komisemi, tak aby podporoval růst kvalitních kryptoměnových projektů, a navíc je jeho hlavním zaměřením XRP.

Má takovéto férové a otevřené zastoupení, jednání a správu nějaká jiná kryptoměna? NE.

Bezpečnou a adaptabilní kryptografii

Kryptografie je velmi důležitá část všech digitálních aktiv, proto se také tyto měny nazývají kryptoměny.

Je pravdou, že pro většinu běžných uživatelů PC nebo přímo i uživatelů kryptoměn je tato oblast složitá na pochopení. Na druhou stranu není nutné znát všechny detaily, jak je kryptografie použita pro danou kryptoměnu.

Důležité ale je vědět, jak bezpečně zacházet se svými veřejnými (public keys) a privátními (private keys) klíči.

XRP Ledger používá standardní kryptografická schémata pro podepisování a ověřování transakcí a také podporuje tzv. multi-signing funkce.

Digitální podpis (signature) potvrzuje, že transakce je autorizovaná a může provést požadované akce. Pouze podepsané transakce mohou být zpřístupněny síti a vloženy do schválené knihy (ledger).

Každý digitální podpis je provázán s odesílajícím účtem a jeho kryptografickým párem klíčů. Pár klíčů může být vytvořen jakýmkoliv kryptografickým podpisovým algoritmem, který je podporován XRP Ledger.

Aktuálně jsou to dva:

Secp256k1 (ECDSA) – stejný algoritmus je použit i bitcoinem a je přednastaven i pro XRP Ledger

ed25519 (EdDSA) – novější typ algoritmu, který je rychlejší

Budoucnost, asi jste již slyšeli o kvantových počítačích, zatím ještě nejsou plně funkční, ale očekává se, že by mohly znamenat jistou hrozbu pro kryptografii. Proto XRP Ledger zůstává plně adaptabilní a může implementovat nový algoritmus podpisů, pokud se prokáže ohrožení současné kryptografie eliptických křivek a jejich prolomení. Takovýto algoritmus se nazývá kvantově odolný (quantum-resistant).

Řekněme si trochu více o tom, jak fungují privátní a veřejné klíče a k čemu že je ta kryptoměnová peněženka.

Kryptopeněženka uchovává vaše dva klíče – veřejný i privátní. Ve skutečnosti na ní nejsou uloženy vaše kryptoměny. Ty jsou stále uloženy v blockchainu sítě.

Standardně si můžeme představit veřejný klíč jako váš bankovní účet.
A privátní klíč jako heslo k tomuto účtu.

Podobně jako dnes, pokud vám někdo posílá peníze na bankovní účet, musí ho tato osoba znát. Samozřejmě nezná vaše heslo či PIN zajišťující přístup k tomuto účtu.
Obdobně funguje veřejný klíč, též ho lze nazvat veřejná adresa. Pozor, pro každou kryptoměnu potřebujeme vlastní, tzn. jiný veřejný a privátní klíč, protože se jedná o jinou síť a blockchain. Toto pravidlo nemusí platit u tzv. ERC tokenů, které jsou vytvářeny například na ethereum síti.

Příklad veřejného klíče pro XRP účet:
rU983VW3mzMaC5WFaYE4M474AVWbNEa2Nv

Privátní klíč může mít například tuto podobu, ale samozřejmě se nejedná o platný klíč k naší veřejné adrese:
0B28FFA386C7A227601B2AISODOS2211EC86D3BF1FFE471BE795

Kryptoměnami uloženými v peněžence může disponovat každý, kdo zná privátní klíč. Proto existuje celá řada způsobů, jak bezpečně ukládat kryptoměny. Jako hardwarové peněženky typu Ledger Nano X či Trezor.

Pro kryptoměny se používá tzv. asymetrická kryptografie. Veřejným klíčem zašifrujeme transakci a privátním ji dešifrujeme. Logicky to znamená, že váš veřejný klíč můžete dát vědět komukoliv, ale naopak privátní klíč nesmí znát nikdo další.

Ano, kryptoměny v sobě přinášejí hodně svobody a možnost vlastního rozhodování, komu jaké prostředky pošleme, ale také s nimi přichází 100% vlastní odpovědnost za bezpečnost našich kryptoměn a nakládání s nimi. Není tu žádná třetí strana, kterou si platíte za zprostředkování transakcí a zajištění bezpečnosti.

Moderní funkce pro smart kontrakty

XRP Ledger umožňuje přenos hodnoty pomocí XRP plateb, ale má také další speciální funkce, které podporují vizi Internet of Value.

Tyto funkce umožňují dalším aplikacím stavět na XRP a poskytovat služby, které by byly dříve nepraktické a těžko realizovatelné. U XRP Ledger není nutné spouštět aplikace jako smart kontrakty přímo v síti, ale XRP Ledger poskytuje možnost tyto kontrakty zpracovat, ačkoliv aplikace samotné běží v jiném prostředí.

Můžeme tento koncept nazvat „Keep it simple“ a umožňuje flexibilní, škálovatelný a účinný přístup.

Několik příkladů těchto funkcí:

- **Platební kanály** umožňují asynchronní změny stavu účtů, tak rychle, jak je zpracován digitální podpis (vytvořen a schválen).
- **Escrow** uzamkne XRP do doby vypršení definovaného času nebo je splněna kryptografická podmínka.
- **DepositAuth,** uživatelé mohou rozhodnout, kdo jim smí poslat peníze a kdo nikoliv.
- **Decentralizovaná burza**, XRP Ledger umožňuje jako jeden z mála plně funkční burzu, kde uživatelé mohou obchodovat vydané měny versus XRP nebo přímo navzájem. XRP Ledger podporuje tzv. atomické cross-currency transakce.