FAKULTA APLIKOVANÝCH VĚD
ZÁPADOČESKÉ UNIVERZITY
V PLZNI

KATEDRA
KYBERNETIKY

Bitcoin a jeho kryptografické fungování

Obrázek 1: Bitcoinové logo

"Fix the money, fix the world" - Satoshi Nakamoto

Západočeská Univerzita V Plzni
Katedra Kybernetiky
Semestrální práce - HKUI

Jan Šemora
ZS 2021/22
20. listopadu 2021

Obsah

Seznam obrázků

1 Proč je Bitcoin tak revoluční záležitost?

Bitcoin je peer-to-peer elektronická měna, nová forma elektronických peněz, které si mezi sebou můžou lidé či počítače posílat bez jakéhokoliv prostředníka, kterému musí důvěřovat (jakým je například banka), a jejichž vydávání není pod kontrolou nějaké jedné instituce nebo skupiny.

Přechod k digitálním platbám s sebou přinesl závislost na centrální autoritě, která musí každou platbu schválit a potvrdit. Je tomu tak proto, že povaha peněz se změnila z něčeho materiálního, co můžete nosit u sebe a sami si kontrolovat, na digitální informaci, která musí být uložena a ověřena třetí stranou, zodpovědnou za převod.

Když se zbavujeme hotovosti ve prospěch pohodlných digitálních plateb, vytváříme tak zároveň systém, v němž dáváme mimořádnou moc těm, kteří se nás můžou pokusit ovládat. Digitální platební platformy se stávají základem dystopických autoritářských systémů kontroly, které využívá např. čínská vláda ke sledování disidentů a k tomu, aby zabránila nákupu zboží a služeb lidí, jejichž chování se jí nelíbí.

Bitcoin nabízí alternativu k centrálně kontrolovaným digitálním penězům.

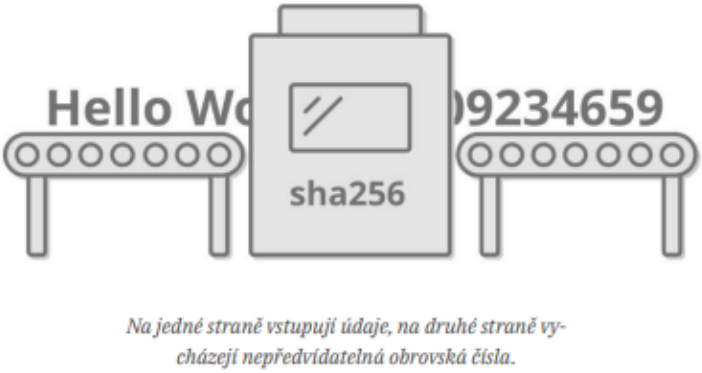
Bitcoin je síť počítačů, na kterých je spuštěn bitcoinový klient.

Obrázek 2: Propojení počítačů v Bitcoinové síť

2 Hashování - způsob, jak zajistit bezpečnost

Asymetrický rébus důkazu o vykonané práci v síti Bitcoin zahrnuje použití hashovací funkce. Ze základní algebry víme, že funkce je jakási krabička, kam vložíte jako vstup nějakou hodnotu x a jako výstup dostanete hodnotu f(x). Například funkce f(x)=2x bere nějakou hodnotu a násobí ji dvěma. Pro vstup x=2 dá výstup f(x)=4. Hashovací funkce je speciální funkce, do které vložíte jakýkoliv řetězec písmen, čísel a jiných údajů, například „Hello world", a dostanete obrovské náhodné číslo.

Hashovací funkce, kterou je použita k zahashování řetězce „Hello world", se nazývá **SHA-256** a je to náhodou zrovna ta funkce, kterou používá Bitcoin.



Obrázek 3: Popis funkce SHA-256

Hashovací funkce SHA-256 má následující vlastnosti, které jsou pro nás užitečné:

- 1. Výstup je pevně daný: stejný vstup vždy vyprodukuje stejný výstup.
- 2. Výstup je nepředvídatelný: změna třeba jen jednoho písmena nebo přidání mezery do řetězce na vstupu radikálně změní výstup, a to tak, že nelze vypozorovat žádnou korelaci se změnou vstupu.
- 3. Výstup (hash) lze spočítat rychle pro jakoukoliv velikost vstupních údajů.

- 4. Je nemožné najít dva řetězce, které vyprodukují tentýž výstup.
- 5. Známe-li výstupní hash funkce SHA-256, je nemožné získat z něj vstupní řetězec. Říkáme, že funkce je jednosměrná (nebo též jednocestná).
- 6. Výstup má vždy specifickou velikost (u funkce SHA-256 je to vždy 256 bitů).

2.1 Jak velká je pravděpodobnost uhodnutí hashovací funkce?

Počet unikátních hodnot, které lze reprezentovat pomocí 256 bitů, což je velikost hashovací funkce SHA-256. To je obrovské, skoro nepředstavitelné číslo. Pokud bychom ho zapsali v desítkové soustavě, bylo by to 78místné číslo. Jen pro ilustraci, tohle číslo se přibližně rovná odhadovanému počtu atomů v celém známém vesmíru.

$2^{256} = 115\,792\,089\,237\,316\,195\,423\,570\,985\,008\,687\,907\,853\,269\,984$
$665\,640\,564\,039\,457\,584\,007\,913\,129\,639\,936$

Obrázek 4: Číselné vyjádření velikosti funkce SHA-256

Toto je počet možných výstupů při zahashování jakéhokoliv řetězce pomocí funkce SHA-256. V podstatě se nedá odhadnout, jaká bude výsledná hodnota. Bylo by to jako správně předpovědět všechny výsledky 256 hodů mincí nebo uhodnout umístění nějakého konkrétního atomu, který jsem vybral kdekoliv ve vesmíru. Zápis tohoto čísla zabere opravdu příliš mnoho místa.

3 Bitcoinové adresy (Bitcoinový účet)

Stejně jako funguje generování velkých náhodných čísel pomocí funkce sha-256, můžeme stejný trik použít na vytváření účtů. K vytvoření „bitcoinového účtu", který je taky známý jako adresa, nejprve vygenerujeme dvě 256bitová čísla, která jsou matematicky propojena a jsou známa pod názvy veřejný klíč a soukromý klíč. Vzpomeňte si, že 256bitové číslo je zhruba tak velké jako počet atomů ve vesmíru, takže je téměř nemožné, aby dva lidé vygenerovali stejný soukromý klíč. Naši adresu poskytneme komukoliv, kdo nám chce poslat peníze. K poslání mincí námi použijeme soukromý klíč. Funguje to takhle.

Šifrování je metoda skrývání údajů tak, aby je mohl přečíst jen ten, kdo má klíč, jímž může vzkaz dešifrovat. Jako děti si někteří z nás hráli s jednoduchými šifrovacími hračkami, které používaly určitý klíč k převedení nějakého vzkazu do nesrozumitelné řeči a zase zpátky. Tenhle druh šifrování se nazývá symetrický a používá jen jeden klíč. Systém dvojic veřejných a soukromých klíčů je asymetrický, protože jedním klíčem šifrujete, zatímco druhým klíčem dešifrujete.

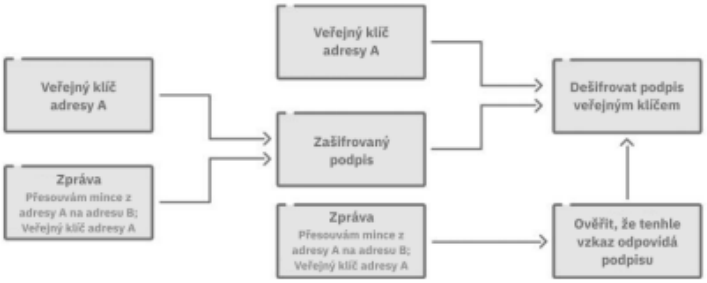
Svůj veřejný klíč můžete klidně sdílet s celým světem. Lidé, kteří vám chtějí posílat vzkazy, je můžou zašifrovat pomocí vašeho veřejného klíče. Protože soukromé klíče máte jen vy, jste taky jediný, kdo je může dešifrovat.

3.1 Jak probíhá transakce s digitálními (Schnorrovy) podpisy?

Podívejme se teď, jak Alena pošle mince Bedřichovi. Aby mohl Bedřich transakci přijmout, vygeneruje si dvojici klíčů a svůj soukromý klíč si nechá pro sebe. Vytvoří adresu, která je velkým číslem vycházejícím z hashe Bedřichova veřejného klíče. Bedřich tuto adresu sdělí Aleně. Tuto adresu si můžete představit jako poštovní schránku. Namísto dopisů do ní Alena může hodit mince. Jen Bedřich však má soukromý klíč, kterým lze schránku otevřít a získat k mincím přístup. Když přesouváte peníze v bance, zadáváte své uživatelské jméno a heslo. Když vypisujete šek, podepisujete ho, abyste potvrdili, že jste ho vypsali vy. Když přesouváte bitcoiny, předkládáte důkaz, že vlastníte klíč k adrese, kde jsou bitcoiny uloženy. Alena potřebuje dokázat, že má soukromý klíč ke své schránce založené na veřejném klíči, ale nechce svůj soukromý klíč odhalit hackerům, kteří by pak mohli její schránku vykrást a mince utratit. Alenin důkaz vlastnictví se nazývá digitální podpis,

tzv. **Schnorrův podpis**. Alena vytvoří transakci, což je v podstatě kousek dat, který vypadá přibližně takhle: Adresa 12345, kde je uloženo 2,5 bitcoinu, posílá 2 bitcoiny na adresu 56789 a 0,5 bitcoinu zpět na adresu 12345. Čísla adres jsou ve skutečnosti velká čísla o 160 bitech. Alena pak transakci zašifruje pomocí svého soukromého klíče a vytvoří tak digitální podpis. Když svou transakci odešle ostatním uzlům sítě, odhalí veřejný klíč schránky, z níž transakci posílá, a podpis zašifrovaný soukromým klíčem. Alena oznámí následující:

- Posílám mince z adresy 12345.
- Tady je veřejný klíč pro adresu 12345 a můžete si ověřit, že to je opravdu veřejný klíč, když si ho zahashujete a získáte číslo adresy.
- Tady je podpis, který jsem zašifrovala soukromým klíčem odpovídajícím této adrese. Můžete ho dešifrovat veřejným klíčem a ověřit si, že je shodný s údaji posílané transakce.



Transakce, kterou se přesouvají mince, je zašifrovaná soukromým klíčem, čímž vzniká digitální podpis. Je dešifrována veřejným klíčem, který všichni znají.

Obrázek 5: Průběh transakce v Bitcoinové síti

Protože teď všichni mají Alenin veřejný klíč k adrese její schránky, můžou snadno dešifrovat digitální podpis. Díky tomu, že můžou správně dešifrovat podpis veřejným klíčem k adrese, všichni vědí, že Alena musela použít soukromý klíč k této adrese, aby podpis vytvořila. Jinak by jejich dešifrování neuspělo, protože veřejný klíč může dešifrovat jen vzkazy zašifrované soukromým klíčem. Důležité však je, že nikdo neviděl Alenin soukromý klíč, ale

jen důkaz, že ho použila k zašifrování svého podpisu. Na rozdíl od podpisu na šeku nebo hesla k bankovnímu účtu je digitální podpis vždy specifický pro jedinečná transakční data, která podepisujete. Proto ho nejde ukrást a znovu použít na jinou transakci. Každá transakce má jiný podpis, i když je uskutečňována ze stejné veřejné adresy a se stejným soukromým klíčem, protože jakákoliv jiná data změní hash podpisu.

3.2 Lze soukromý klíč uhodnout?

Pojďme se podívat, jak moc je pravděpodobné, že by se někomu podařilo uhodnout soukromý klíč, který by mu umožnil přesouvat mince z příslušné veřejné adresy. Připomeňme si, že klíč má velikost 256 bitů. Každý bit může nabývat jen dvou hodnot (jedna nebo nula). Každý bit si proto můžete představit jako hod mincí. Kdybychom měli soukromý klíč o velikosti 1 bit, bylo by to jako hod jedinou mincí. Padne panna, nebo orel, jedna, nebo nula? Máte šanci jedna ku dvěma, že klíč uhodnete.

Zopakujme si rychle základy statistiky: Pravděpodobnost víc událostí zároveň se počítá tak, že vynásobíme pravděpodobnosti všech jednotlivých událostí. Pokud je u hodu mincí pravděpodobnost 1/2 že padne panna, potom pravděpodobnost, že padne panna dvakrát po sobě, je 1/2 * 1/2 = 1/4 neboli 1 ku 4.

Kreditní karta má číslo o šestnácti číslicích. Každá číslice může nabývat 10 hodnot a je jich celkem 16, takže pravděpodobnost, že uhodnete číslo mé kreditní karty, je 1 ku 10 na 16, což je 1 ku 10 000 000 000 000 000 neboli zhruba 1 ku deseti kvadrilionům. Na zemi je okolo 10 na 50 atomů. Když si náhodně vyberu jeden z nich, pravděpodobnost, že uhádnete, který to je, je okolo 1 ku 1 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000.

Soukromý klíč má 256 bitů, což je 2 na 256 nebo přibližně 10 na 77. Uhodnout celý klíč by bylo podobné jako uhodnout jeden konkrétní atom v celém vesmíru nebo vyhrát v loterii Powerball devětkrát po sobě: 1 ku 115 792 089 237 316 195 423 570 985 008 687 907 853 269 984 665 640 564 039 457 584 007 913 129 639 936.

Co kdybyste však měli supersilný počítač, který by hádal za vás? Zde je příklad, jak by to mohlo vypadat:

Kdybyste mohli použít celou planetu jako harddisk a uložit 1 byte do jednoho atomu, jako palivo používat hvězdy a zapisovat 1 trilion klíčů za vteřinu, potřebovali byste k uložení všech klíčů 37 oktilionů zeměkoulí a 237

miliard Sluncí, abyste dokázali napájet takovýto přístroj, a trvalo by vám to 3,6717 oktodecilionů let.

4 Závěr

Bitcoin přináší celou řadu lepších způsobů, jak zlepšit finanční ekosystém. V práci nebyly zmíněné všechny způsoby nebo průběhy, jak celý proces funguje, jelikož by byla příliš obsáhlá. Představil jsem vám, proč používat zrovna Bitcoin a jakým způsobem zajistit jeho bezpečnost přeš kryptografické funkce. Pořád se obáváte? Je tedy v podstatě nemožné, aby někdo uhodl váš soukromý klíč. Navíc počet všech možných bitcoinových adres je tak velký, že je na bitcoinové síti zvykem pro každou transakci vytvořit novou adresu s novým soukromým klíčem. Místo toho, abyste měli jeden účet, tak můžete mít tisíce nebo dokonce miliony bitcoinových účtů, jeden pro každou transakci, kterou jste kdy uskutečnili. Možná vás zneklidňuje, že je váš bitcoinový účet zajištěn jen statisticky, ale na základě výše zmíněné ilustrace je snad už jasné, že je nesrovnatelně bezpečnější než heslo k vašemu bankovnímu účtu, které je uložené na centralizovaném serveru a přístupné případným hackerům.

5 Citace písemných zdrojů

Veškeré zdroje byly čerpány ze stránky od společnosti Braiins, konkrétně z digitální verze knihy s názvem Vynález jménem Bitcoin. Autorem: YAN PRITZKER, Vydavatel: Braiins

1. Braiins — Bitcoin mining company. Braiins — Bitcoin mining company [online]. Dostupné z: https://cs.braiins.com/

6 Citace obrázků

Veškeré obrázky byly čerpány ze stránky od společnosti Braiins, konkrétně z digitální verze knihy s názvem Vynález jménem Bitcoin. Autorem: YAN PRITZKER, Vydavatel: Braiins

1. Braiins — Bitcoin mining company. Braiins — Bitcoin mining company [online]. Dostupné z: https://cs.braiins.com/