Blockchain pro začátečníky

Jan Seidl

V současnosti je Blockchain často zmiňovaným pojmem. V řadě případů však dochází k záměně pojmů Blockchain a Bitcoin, ne zcela správnému pochopení významu technologie Blockchain a nejasnému výkladu s ním souvisejících termínů. Aby společnosti a jejich zástupci mohli vůbec uvažovat o možném využití Blockchainu pro své obchodní aktivity, je třeba nejprve pochopit základní principy jeho fungování a podstatu jeho výhod a omezení. Tento článek by měl popsat vlastností Blockchainu, přičemž jednotlivé principy vysvětluje v logickém sledu vývoje této technologie.

Co je Blockchain

Označení Blockchain má z technologického pohledu dva základní významy. Prvním z nich je označení množiny softwarových protokolů, které umožňují realizaci fungování Blockchainu, jako technologické platformy. Druhým významem je pak označení Blockchainové databáze, nad kterou jednotlivé Blockchain protokoly operují.

Do povědomí lidí začal pojem Blockchain pronikat s příchodem dnes nejznámější kryptoměny Bitcoin, jejíž implementace byla zprovozněna v roce 2009. V té době bylo vnímání Bitcoinu spojováno především s anonymitou jejích uživatelů a z toho důvodu začal být vnímán jako prostředek pro provádění nelegální činnosti. Nevalná pověst Bitcoinu tak částečně zastřela původní myšlenku, umožnit důvěryhodnou výměnu aktiv napříč Internetem, bez potřeby vzájemné či zprostředkované důvěry.

Mezi klíčové vlastnosti Blockchainu patří:

- Systém funguje bez centralizované důvěry.
- Všichni znají stav všech ostatních účtů.
- Transakce jsou schvalovány konsensuálním způsobem, který je reprezentován procesem těžení.
- Autenticita transakcí je chráněna asymetrickou kryptografií.
- Za jednotlivé transakce jsou odváděny transakční poplatky.
- Databáze je distribuována mezi jednotlivé účastníky.
- Integrita databáze je silně chráněna procesem těžení a řetězením bloků.

Základní principy Blockchainu

Jednotlivé principy fungování Blockchainu popíšeme postupně na příkladě čtyř lidí, které pro tyto účely pojmenujeme Adrian, Bára, Cyril a Dáša.

Uvažme situaci, kdy Bára se ocitla ve finanční tísni. Poprosí přítele Adriana, aby jí na účet poslal 1000 Kč. Adrian se přihlásí do svého internetového bankovnictví a zadá příkaz k převodu peněz na účet Báry. Banka, ve které má Adrian účet, zkontroluje stav účtu a ověří, že Adrian disponuje částkou alespoň 1000 Kč a provede převod. Druhý den Bára zadá bankomatu požadavek na výběr 1000 Kč. Bankomat se spojí s její bankou, ověří, že má na účtu alespoň 1000 Kč a vydá jí je.

Tento příklad demonstruje převod finanční částky s využitím bankovního systému. Nezbytným faktorem v tomto procesu je důvěra v banku. Samotná hodnota měny je pouhou metrikou, kterou lze měřit hodnotu jednotlivých aktiv, přičemž měna je reprezentantem této metriky. Je tedy zcela logické, že aby mohla být daná měna akceptována, musí být vydávána někým důvěryhodným a její hodnota musí být náležitě chráněna. Otázkou však je, jestli je to jediný možný způsob.

Představme si, že se Adrian, Bára, Cyril a Dáša rozhodli, že si mezi sebou vytvoří vlastní měnu, kterou si mezi sebou budou posílat. Aby se vzájemně nemohli podvádět, potřebují se dohodnout na tom, jakým způsobem zajistí důvěru. Jednou variantou je, že vyberou jednoho zástupce, např. Adriana, který bude spravovat stav účtů všech a bude schvalovat jednotlivé finanční transakce. Adrian by tak fungoval jako centrální autorita, která by plně rozhodovala o tom, kdo má kolik peněz komu posílat. Cyril s Dášou si ale vzájemně nevěří a nevěří ani ostatním, proto s daným rozhodnutím nesouhlasí. Po této vzájemné neshodě se přátelé rozhodnou, že budou každou transakci ověřovat

společně. Zároveň si však uvědomí, že může nastat situace, kdy nebudou všichni současně k dispozici. Potom by docházelo ke zpoždění transakcí. Proto zavedou pravidlo, že pro potvrzení transakce stačí k ověření nadpoloviční většina, tedy tři lidé.

> Dáša chce poslat 1000 jednotek dohodnuté měny Báře. Vytvoří příkaz k odeslání 1000 jednotek na Báry účet a pošle prosbu o schválení na všechny. Každý, kdo upozornění obdrží, zkontroluje, zda je daná transakce v pořádku a pokud je, pošle potvrzení ostatním, aby věděli, že transakci schválil. Jakmile alespoň tři transakci potvrdí, je akceptováno, že Dáša má o 1000 jednotek méně a Bára o 1000 jednotek více.

Touto cestou, ve které nefiguruje centralizovaná důvěra, se vydal Blockchain. Jak je ale z příkladu patrné, vyvstává zde několik otázek. Jak víme, že transakci poslala opravdu Dáša a ne například Adrian, který by se za Dášu vydával? Jak víme, kolik má Dáša na svém účtu? Co když má Dáša na svém účtu přesně 1000 jednotek a vytvoří současně dvě transakce, přičemž v jedné tvrdí, že posílá 1000 jednotek Báře a ve druhé 1000 jednotek Cyrilovi? Co když se někdo rozhodne, že nebude potvrzovat správné transakce a tím omezí provádění transakcí? Co když Bára jednoho dne prohlásí, že daných 1000 jednotek od Dáši nikdy nedostala?

Jak ostatní vědí, že transakci poslala opravdu Dáša a ne například Adrian?
Pravdou je, že ostatní to nevědí. Nemohou. V jednotlivých transakcích jsou totiž uvedeny čísla účtů odesílatele, příjemce a samotná převáděná částka, ale nikoliv jména vlastníků účtů. Pokud bychom se podívali na samotné transakce, pak bychom nezjistili, že Dáša poslala 1000 jednotek Báře, ale jen to, že z účtu X odešlo 1000 jednotek na účet Y. A vzhledem k tomu, že v tomto systému není centralizovaná autorita, nikdo nemusí vědět, komu dané účty skutečně patří. Právě tato forma anonymity stála za již zmíněnou nevalnou pověstí kryptoměny Bitcoin.

Jak tedy ostatní vědí, že účet odesílatele uvedený v transakci je skutečně účtem, ze kterého byla transakce odeslána?
Blockchain k tomu využívá asymetrickou kryptografii. Ke každému účtu je vygenerována dvojice kryptografických klíčů, přičemž jeden se označuje jako privátní klíč a druhý jako veřejný klíč. Privátní klíč je znám pouze majiteli účtu, veřejný klíč je uveřejněn všem ostatním. Pokud má být z daného účtu odeslána transakce, je nejprve tato transakce digitálně podepsána privátním klíčem. Ostatní, kteří transakci mají kontrolovat, nejprve ověří, že byla skutečně odeslána z účtu, který je uveden jako odesílající. A to právě kontrolou digitálního podpisu veřejným klíčem. Podobný princip používá obecně známé PKI, ovšem s tím rozdílem, že v Blockchainu postrádáme certifikáty, které by svazovaly konkrétní entity s danými veřejnými klíči.

Proč Blockchain nevyužívá certifikáty?
Aby mohl Blockchain pracovat s certifikáty, musela by existovat centrální důvěryhodná autorita, která by je vydávala, ta ale neexistuje.

Jak ostatní poznají, který veřejný klíč mají pro ověření podpisu k danému účtu použít?
Samotná čísla účtů nejsou generována náhodně, ale jsou odvozena z k nim příslušného veřejného klíče. Pokud někdo obdrží transakci, u které chce digitální podpis pro účet odesílatele ověřit, pak na základě samotného čísla účtu ví přesně, který veřejný klíč má použít. Je tedy zřejmé, že jakmile někdo vlastní privátní klíč, je schopen vytvářet validní transakce a tím pádem plně kontrolovat daný účet. Celá ochrana účtu tak spočívá v zabezpečení privátního klíče, běžně uchovávaného v tzv. kryptopeněženkách, které mohou mít softwarovou, ale i hardwarovou podobu.

Co když se někdo nebude potvrzovat správné transakce a omezí tak provádění transakcí?
Nepotvrzení správné transakce nemusí být vždy záměrné. Může k tomu dojít i v případě, že si někdo uchovává jinou databázi než ostatní, například důsledkem chyby. Abychom byli schopni odpovědět, musíme se podívat na to, jakým způsobem Blockchain řeší ukládání informací a jak zajišťuje integritu ukládaných dat.

Nejprve si představme transakční systém, který není tvořen jen čtyřmi přáteli, ale miliony lidí. Kdybychom vždy čekali na potvrzení nadpoloviční většinou, systém by byl značně neefektivní. Při návrhu Blockchainu se již s možným rozšířením počítalo a byl vymyšlen jiný způsob. Původní metrika počtu účastníků byla převedena na výpočetní výkon celého systému. To znamená, že aby byla transakce ověřena, musí k tomu být použit výpočetní výkon reprezentující účast alespoň 51 % členů (tzv. hashrate). Míra výpočetního výkonu je dána složitostí matematického problému, jehož řešení je právě výpočetně náročné. A vzhledem k tomu, že stav účastníků se v celém systému dynamicky mění, mění se tím i úroveň složitosti řešení tohoto matematického problému. Proces potvrzování transakcí se nazývá těžení (mining) a lidé, kteří verifikaci provedli, se pak nazývají těžaři (mineři).

- Ověřování transakce probíhá v několika krocích:
- Ověření digitálního podpisu dané transakce.
- Ověření stavu účtu vůči převáděné hodnotě.
- Provedení výpočtu pro nalezení patřičného vzoru.
- Vystavení informace o ověření transakce (blok).

Víme tedy, že blok v sobě obsahuje vstupní hodnotu do hashovací funkce sloužící jako důkaz potvrzení transakce neboť víme, že dotyčný těžař musel vynaložit dostatečné úsilí (výpočetní výkon) pro získání požadované hodnoty. Blok je následně odeslán na všechny účastníky. Každý účastník daný blok vezme, vezme uvedenou hodnotu, spočítá její hash a ověří důkaz. Následně se podívá, pro kterou transakci je daný blok důkazem a tuto transakci považuje za potvrzenou. Pokud je tedy i samotný blok validní, uloží si ho příjemce do své lokální databáze. Uložení není nicméně pouhým vložením přijatého bloku vedle jiného bloku, ale jednotlivé bloky jsou dohromady zřetězeny. Řetězení (chaining) funguje tak, že aktuálně přijatý blok v sobě navíc obsahuje hodnotu, jejíž součástí je hash předchozího vydaného bloku. Při vytváření nového bloku se tak vezme i hodnota posledního vydaného validního bloku a ta je započítána do bloku nového. Tím vzniká vazba na předchozí blok. Proces řetězení vytváří spojenou databázi bloků, tzv. blockchain.

K čemu řetězení vlastně je?
Řekli jsme si, že každý z účastníků našeho transakčního systému si udržuje vlastní

databázi potvrzených transakcí (bloků). Pokud má Dáša jinou databázi než Cyril, je některá z nich neplatná a bude to právě ta, jejíž bloky na sebe nenavazují, neřetězí se. Proto hraje řetězení důležitou roli.

V případě, že by někdo chtěl záměrně falšovat databázi - nahradit posledních 5 bloků vlastními navazujícími bloky, musel by vynaložit obrovský výpočetní výkon, který by představoval více než 50 % výpočetního výkonu celého Blockchain systému (tzv. 51 % útok). To je velice málo pravděpodobné. Celá integrita Blockchain databáze je tak silně chráněna a značně rigidní.

Jaká je tedy motivace těžařů?
Čím větší je sytém, tím větší výpočetní výkon vyžaduje proces těžení. K tomu se pochopitelně vážou vysoké finanční náklady za spotřebu elektrické energie. Jaká je tedy motivace těžařů? Blockchain je nastaven tak, že každý, kdo vytváří transakci, za ni musí zaplatit poplatek, ten náleží právě těžaři, který danou transakci validuje. Každý těžař zároveň dostává fixně stanovenou odměnu za vytvoření validního bloku. Hlavní motivací těžařů je tak obdržení odměny.

Jak ostatní vědí, kolik má Dáša na svém účtu?
Vzhledem k tomu, že si všichni udržují veškeré bloky ve své vlastní databázi, vědí, kolik jednotek je na každém z účtů v systému.

Co když má Dáša na svém účtu přesně 1000 jednotek a vytvoří současně dvě transakce, přičemž v jedné posílá 1000 jednotek Báře a ve druhé 1000 jednotek Cyrilovi?
Pokud jsou z jednoho účtu odeslány dvě různé transakce, jsou vytvořeny ve stejném čase dva různé, nicméně validní bloky. V momentě, kdy jsou oba bloky přijaty, dojde v místě posledního bloku v Blockchain databázi k rozdělení na dvě paralelní větve. Růst databáze pokračuje vydáváním dalších nových bloků a jejich postupným řetězením do jednotlivých větví podle toho, na jaký blok navazují. V momentě, kdy jedna větev začne být delší než druhá větev, je kratší větev zahozena a pokračuje se pouze s delší větví. Co to znamená v praxi? Aby si příjemce některé transakce mohl být jistý, že mu skutečně daná částka náleží, počká ještě na vydání několika dalších bloků, které potvrdí, že jsou větví, která nebude zahozena.

Co když Bára jednoho dne prohlásí, že žádných 1000 jednotek nikdy od Dáši nedostala?

Stačí se podívat do databáze a najít blok potvrzující danou transakci, ve které je uveden převod 1000 jednotek z příslušného účtu na daný účet. Vzhledem k silné ochraně integrity databáze víme, že je velice nepravděpodobné, aby transakce neproběhla.

Smart Contracts

Doposud jsme fungování Blockchainu chápali jen jako systém transakční, reprezentující přesun jednotek vyjadřující finanční hodnotu, tzv. kryptoměnu. Vraťme se ale k prvotní myšlence, tedy že by Blockchain měl umožnit důvěryhodnou výměnu aktiv napříč Internetem, bez potřeby vzájemné či zprostředkované důvěry. V této větě se nic neříká o tom, že by měl sloužit jen k přesunu transakcí v podobě měn, tedy kryptoměn. Transakce je pouhým kusem dat, proto může nést libovolnou jinou hodnotu. Uveďme si příklad.

Řekněme, že Adrian, Bára, Cyril a Dáša pracují společně na dokumentu, jehož verze si navzájem vyměňují a každý z nich doplňuje svou část textu. Až bude finální podoba dokumentu dokončena, každý z autorů bude ohodnocen na základě jeho příspěvku. Pro všechny je tak důležité, aby mohli prokázat, jakou část vypracovali. Vzhledem k jejich vzájemné nedůvěře se rozhodnou využít Blockchain. Poté, co každý z nich napíše svou část příspěvku, vezme daný dokument, spočítá pro něj hash pomocí hashovací funkce a tento hash pošle formou transakce na Blockchain. Transakce je validována a je k ní zařazen příslušný blok do Blockchain databáze. Když dojde na konsolidaci příspěvků v rámci finalizace dokumentu, je už úplně jedno, kdo tuto finalizaci provede. Pokud by se např. Adrian rozhodl zpochybnit příspěvek Dáši, stačí vzít příslušný příspěvek, spočítat k němu hash a najít ho v Blockchain databázi. Pokud tam takový hash od Dáši je, je vzhledem k silné integritě databáze prokazatelné, že autorství daného příspěvku skutečně náleží jí.

Blockchain není pouhým transakčním systémem pro převod kryptoměn. Namísto jednoduchých dat uvnitř transakcí si můžeme představit i složitější data, která v sobě mají zakódované podmínky, dle kterých jsou různě interpretována, jak je tomu v následujícím příkladu.

Bára s Dášou se vsadí, že Adrian utratí za týden všechny jednotky na svém účtu. Bára vytvoří transakci, ve které uvede dané podmínky sázky, vytvoří tzv. smart contract (SC), a ten pošle na Blockchain. SC má svou vlastní adresu, podobně, jako ji mají jednotlivé účty v Blockchain systému. Jakmile je SC na Blockchainu vypublikován, Dáša a Bára tyto podmínky potvrdí vygenerováním transakce směrem na účet SC a SC obdrží vsazené částky od Báry i Dáši. V tento moment je SC uzavřen a čeká na své plnění. Podle toho, jestli Adrian své jednotky do týdne utratí, nebo ne, exekuuje SC stanovené příkazy. Velkou výhodou SC je, že není potřeba důvěry mezi Bárou a Dášou, neboť SC je platný až ve chvíli, kdy obě vložily sázky. Zároveň SC nelze rozvázat, jakmile byl aktivován. SC tak funguje zcela autonomně. Tento koncept byl poprvé představen autorem Vitalikem Buterinem, v rámci nové kryptoměny Ethereum v roce 2015 a je často označován jako koncept Blockchain 2.0.

Omezení technologie Blockchain

Ne vždy je žádoucí, aby všichni věděli všechno

V celém systému figurují sice jen čísla účtů, ne jména vlastníků, nicméně informace obsažené v transakcích mezi jednotlivými účty jsou všem známy. Pokud se tedy Bára dozví, který účet Dáše patří, bude schopna dohledat i její celou transakční historii. Vzhledem k tomu, že každý může vlastnit více účtů, nabízí se jednoduché řešení, založit si pro každou transakci nový účet.

Dalším řešením je úprava Blockchain protokolů, které umožňují dosažení plné

anonymity, jakou např. využívá kryptoměna ZCash. Úplně jiným přístupem je vybudování privátního Blockchain systému, v němž bude zavedeno plné řízení přístupu spolu s rolemi a jejich právy. Často jsou tyto typy Blockchain systémů označované jako permissionfull, zatímco původní, veřejné Blockchain systémy jako permissionless systémy. S různými variantami privátních Blockchain systémů se dnes můžeme setkat velice často, když se ale vrátíme k základnímu principu Blockchainu jakožto decentralizovaně řízenému systému, pak jakékoliv zavedení regulace na úrovni řízení jednou konkrétní entitou zcela postrádá smysl. Lze pak jen těžko mluvit o Blockchain systému.

Objemná databáze

Dalším problémem je potřeba mít kopii Blockchain databáze, která může zabírat i desítky GB dat. Jako řešení vznikl koncept částečných a plných uzlů. Částečné uzly mají ty účty, které neuchovávají celou databázi, ale jen takovou část, která jim umožňuje uznávání transakcí nových. Plné uzly mají ty účty, které uchovávají celou databázi, patří mezi ně typicky těžaři, kteří pro verifikaci transakcí potřebují znát skutečně celou historii jednotlivých účtů.

Další možností, jak zmenšit objem databáze, je snižování počtu transakcí nebo snižování počtu bloků. K tomu byl navržen koncept lightningu. Aby došlo ke snížení počtu zasílaných transakcí na Blockchain, ale zároveň k neomezování počtu výměn mezi jednotlivými účty, využil se koncept clearingu. V podstatě se mezi účty, které si chtějí posílat transakce, vytvoří separátní kanál mimo Blockchain síť, ve kterém dochází ke vzájemné výměně transakcí. Až poté, co dojde k výměnám transakcí, dojde k uzavření kanálu, vzájemnému vyúčtování výsledného stavu pro dané účty (clearingu) a pouze rozdíl stavu daných účtů oproti jejich původnímu je zapsán do transakce, která je poslána na Blockchain.

Další variantou je snížení počtu bloků. Vzhledem k tomu, že bloky slouží jako důkazy pro verifikaci validních transakcí a žádná transakce není akceptována, dokud není potvrzena blokem, musí být počet transakcí alespoň takový, jaký je počet bloků. Lze ale začít zvětšovat velikost bloku a vystavit jeden blok jako důkaz pro více. Nebo snížit velikost dat, které je třeba v rámci bloku ověřit.

Jednotlivé přístupy jsou intenzivně probírány v rámci Blockchain komunity a neshody vedly např. k rozdělení kryptoměny Bitocin na původní Bitcoin a nový Bitcoin Cash.

Beze změny

Silná ochrana integrity databáze je velkou výhodou, v některých případech může být ale nežádoucí. Problém nastává ve chvíli, kdy dojde k neúmyslné chybě, kterou je třeba opravit. V Blockchain databázi to ale není možné, jednou vložená informace bude uložena již po celou historii Blockchain systému.

Spotřeba elektrické energie

Proces těžení slouží k verifikaci transakcí a je postaven na principu prokázané práce (proof-of-work). Přestože tento mechanismus má své opodstatnění, s rostoucím systémem roste i potřeba výpočetního výkonu a dochází k enormní spotřebě elektrické energie.

Alternativní přístupy, které by nebyly založeny na výpočetním výkonu, již existují. Proof-of-stake využívá k výběru dalšího těžaře pravděpodobnostní kombinace. Proof-of-space využívá namísto výpočetního výkonu paměť. Vzhledem k řadě problémů, které alternativní přístupy přináší, je ale stále koncept proof-of-work nejrozšířenější variantou.

Pravidla hry

Zcela jiným omezením, které nesouvisí s technickou stránkou Blockchainu, je chybějící standardizace, která by jasně popisovala, jakým způsobem má být Blockchain implementován, kontrolován a vyhodnocován.

Využití Blockchainu

Blockchain vstoupil do povědomí lidí s příchodem prvních kryptoměn, které světu ukázaly, že díky globálnímu propojení pomocí Internetu lze dnes realizovat systémy, které jsme si dříve neuměli ani představit. Důležitým milníkem bylo zavedení smart kontraktů, které pozvedly transakční systém na systém, který je schopen realizovat navíc řadu funkcí a může sloužit nejen k přesunu kryptoměn. Právě smart kontrakty spustily obrovský zájem společností o technologii

Blockchain. Firmy začaly do analýzy této technologie a implementace prototypů investovat nemalé peníze. Jiným fenoménem se staly ICO (Initial Coin Offering), které umožňují zejména startupovým společnostem získat velké investice od běžných lidí.

Blockchain má řadu velmi zajímavých vlastností, aby však mohly být náležitě využity, je třeba klást velký důraz na správné pochopení principů fungování Blockchain technologie a její adekvátní zasazení do obchodních činností společností.

Blockchain trpí některými nedostatky. Jedná se ale o zcela inovativní technologii, která se stále vyvíjí. Očekává se, že řada jejích omezení bude vyřešena v průběhu roku 2018 a zájem o tuto technologii v nejbližších letech ještě vzroste. ■

Jan Seidl

Autor článku je odborníkem na kryptoměny ve společnosti Deloitte.