
# **Blockchain** představuje netušené příležitosti v oblasti ochrany dat

Vojtěch Bínek

Vzestup technologie blockchain je jedním z nejsledovanějších IT trendů současnosti. Jedním z důvodů je jistě zajímavá skutečnost, že nejznámější aplikace blockchainu má dnes hodnotu 14,5 miliardy dolarů. Důležitější jsou ale jeho unikátní technické vlastnosti, které nesou potenciál ještě větší. Tyto vlastnosti vedou mnohé firmy a organizace k tomu, že začínají uvádět na trh komerční řešení postavená na technologii blockchain.

## O prvním blockchainu

Poprvé byl blockchain představen v roce 2008 v krátkém textu anonymního autora, pracujícího pod pseudonymem Satoshi Nakamoto. V jeho textu byl popsán a matematicky vysvětlen koncept elektronické měny, která by se obešla bez centrální autority – všechny procesy nutné k fungování měny by byly podle důmyslného protokolu vykonávány na počítačích samotných uživatelů. Tento protokol dnes nazýváme blockchainem.

Nakamoto nezůstal u teorie a koncept převedl v realitu. Zrodila se tak první kryptoměna na světě a dnes nejznámější, největší a nejhodnotnější aplikace blockchainu – Bitcoin. Do roka se začalo mluvit o revoluci ve světě finančnictví.

## Digitalizace měn a bezhotovostní ekonomika

Kryptoměny dnes umožňují snadnější, rychlejší a levnější provádění zahraničních finančních transakcí než klasické banky. Stinnou stránkou je jejich větší volatilita – i když se například kurz Bitcoinu v posledním roce relativně uklidnil, až pětiprocentní skoky kurzu nejsou stále žádnou výjimkou.

Rok 2017 se pravděpodobně stane rokem, kdy budou spuštěny také první státní kryptoměny. Současně se tak pravděpodobně začnou zavírat dveře dnešním, nestátním, decentralizovaným kryptoměnám. Prvními, prozatím experimentujícími pionýry mezi státy se zdají být Ukrajina, Tunisko, Indie, Rusko a samozřejmě také všechny tradičně progresivní skandinávské země.

V prvním kroku se počítá s propojením kurzu nové kryptoměny s kurzem staré, klasické, fiat měny.

Další vývoj ale bude zajímavější. Pokud se totiž fungování těchto státních kryptoměn ukáže být bezproblémovým, zbude k zachování hotovostních měn jen velmi málo důvodů. Kryptoměna je méně náročná na provoz (tisk,

ochrana proti falzifikaci, transport), zamezuje anonymnímu nakládání s finančními prostředky a poskytuje tak silnější ochranu proti jejímu zneužívání ke kriminálním a nelegálním aktivitám (nebo k jejich financování). Přirozeným konečným stavem digitalizace měny se tak zdá být úplný přechod na cashless (bezhotovostní) ekonomiku.

## Princip blockchainu nabízí průlomové zabezpečení dat

Digitální měny na bázi blockchainu se nazývají kryptoměnami, protože je jejich integrita zajišťována důmyslným kryptografickým protokolem. Ten v podstatě zajišťuje, že se s jednotlivými mincemi dá manipulovat pouze z peněženky, ve které jsou uloženy. Jinými slovy chrání autenticitu uložených dat. Představte si, že bude protokol stejným způsobem chránit data ve vašem systému – blockchain garantuje, že v zapsaných datech nikdo nezmění ani čárku, pokud k tomu nebude mít oprávnění.

Kryptoměny jsou tedy jenom jednou z možných aplikací blockchainu, intenzivně se zkoumá jeho využití pro zabezpečení cloudů a různorodých interních systémů. Teoreticky jím lze před neoprávněnou manipulací zabezpečit téměř jakákoli data. Mluví se tak o zabezpečení podnikových i státních řídících systémů klíčové infrastruktury, které musí být na síti, včetně odpalovacích mechanismů amerických jaderných zbraní. Zdá se, že platí jednoduché pravidlo: Čím citlivější vaše data jsou, tím cennější pro vás implementace blockchainu může být.

Sekundární vlastností kryptografického protokolu je zaznamenávání všech zapsaných změn, čímž vznikají možnosti využití pro rozsáhlé databáze s velkým množstvím zapisovatelů. Neustále se rodící a zase rozpadající světová konsorcia bankovních institucí se například snaží vymyslet, jak blockchain využít ke zjednodušení systémů mezibankovního vyrovnávání a k efektivnímu propojení registrů napěchovaných informacemi o klientech – zatím se spolu ale domluvit nedokázala.

## Proč tedy blockchain ještě není všude?

Technologie blockchainu je velmi mladá. Pro rozhodnutí o využití blockchainu musí jeho účinnější zabezpečení, vyšší efektivita a nižší náklady na provoz převážit nemalé jednorázové finanční výdaje, časovou a pracovní náročnost a riziko selhání implementace. V současnosti je tak ostré nasazení blockchainu často vnímáno jako až příliš náročné a rizikové dobrodružství. Nepomáhá slabá technická standardizace ani ve většině zemí neexistující právní regulace.

A nakonec, i když unikátní, blockchain je pořád jenom technologie v rukou svých uživatelů. Statistiky jasně ukazují, že slabým místem v zabezpečení jakýchkoli systémů bývají častěji lidé než technologie – ani blockchain nedokáže zastavit někoho, kdo si přístupové údaje jednoduše opsal z nálepky na vašem monitoru.

Přesto je pravděpodobné, že blockchainu patří budoucnost. Už dnes se technologie blockchainu na fungování světa nepochybně podepisuje. Také se zdá být jasné, že rychle nachází rozsáhlé uplatnění i mimo svět kryptoměn, především v oblasti zabezpečení různorodých interních systémů, databází a jiných datových úložišť. Pokud nebude další vývoj blockchainu neočekávaně zastaven, pravděpodobně se můžeme těšit na rychlé a zásadní změny, od makroúrovně států po mikroúroveň jednotlivých uživatelů a každého z nás. ■

Vojtěch Bínek

Autor článku je studentem Fakulty sociálních studií na Masarykově univerzitě, který se intenzivně zabývá technologiemi z oblasti informační bezpečnosti.

## Praktické aplikace blockchainu v oblasti ochrany dat

Dnešní digitální svět obsahuje nesmírné množství materiálu, jehož původnost a vlastnictví je těžké a hlavně nákladné sledovat a dohledávat. Blockchain tento problém dokáže vyřešit poskytnutím globální pravosti a bezpečnosti pro data a transakce jakéhokoliv druhu, čímž redukuje náklady a složitost centralizovaných systémů a přitom poskytuje odolnost proti neoprávněné manipulaci. S technologií blockchain mohou být data a transakce aktualizovány pouze na základě pravidel dohodnutých mezi účastníky v systému a nově přidaná data nemohou být nikdy smazána.

Netradiční přístup k využití technologie blockchain pro řešení specifických problémů v oblasti ochrany dat zvolila společnost Acronis, známá především svými zálohovacími řešeními: rozhodla se, že bude vyhledávat a rozvíjet existující specifické uživatelské případy a zkušenosti. Na základě tohoto přístupu představila řešení Acronis Storage. Jde o řešení softwarově definovaného úložiště s autentizací dat postavené na technologii blockchain a s univerzální podporou souborů, bloků a objektů. Jedná se o univerzální řešení softwarově definovaného úložiště, které integruje bloky, soubory a objekty s využitím běžného hardwaru.

Dalším příkladem aplikace blockchainu je aplikace Acronis Notary pro autentizaci dat na bázi blockchain. Aplikace Notary nabízí certifikaci obsahu jakéhokoliv souboru a verifikaci obsahových modifikací v porovnání s původní verzí. Jedinečný „otisk digitálního souboru“ je uložen v distribuované, nezměnitelné databázi postavené na technologii blockchain, která umožňuje uživatelům kdykoliv verifikovat autentičnost informací. To je důležité zejména v případě cenných dokumentů, jako jsou smlouvy, zdravotnické záznamy a finanční dokumenty.

A do třetice můžeme uvést Acronis ASign, což je řešení pro certifikaci dokumentů chráněných technologií blockchain. ASign dovoluje více stranám vytvářet a certifikovat dokumenty se zabezpečeným a veřejně auditovatelným podpisem. Uživatelé mohou chránit své zálohované dokumenty, které jsou verifikovány s pomocí Acronis Notary a elektronicky podepsány – vše v rámci jednoho zálohovacího řešení.