Modul 5

Důvěryhodné zdroje blockchainu – komu věřit

Co-funded by the European Union

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost.

Popis modulu

- Téma: ‚**Důvěryhodné zdroje blockchainu – komu věřit**‘
- Význam: Potenciál ilustrovat, do jaké míry lze na blockchain nahlížet jako na důvěryhodnou technologii.
- Prominentní v akademické literatuře
- Odpovědi na otázky, do jaké míry je používání blockchainu v zemědělsko-potravinářském sektoru důvěryhodné.

Výsledky studia

- **Prokázání** jasného pochopení klíčových vlastností technologie blockchain a její důvěryhodnosti jako potenciálního řešení mnoha z těchto problémů
- **Analyzování** roli blockchainové technologie jako důvěryhodné technologie
- **Posouzení** důvěryhodnosti blockchainových technologií v zemědělsko-potravinářském dodavatelském řetězci

contents

BLOCK CHAIN FOR AGRI FOOD EDU

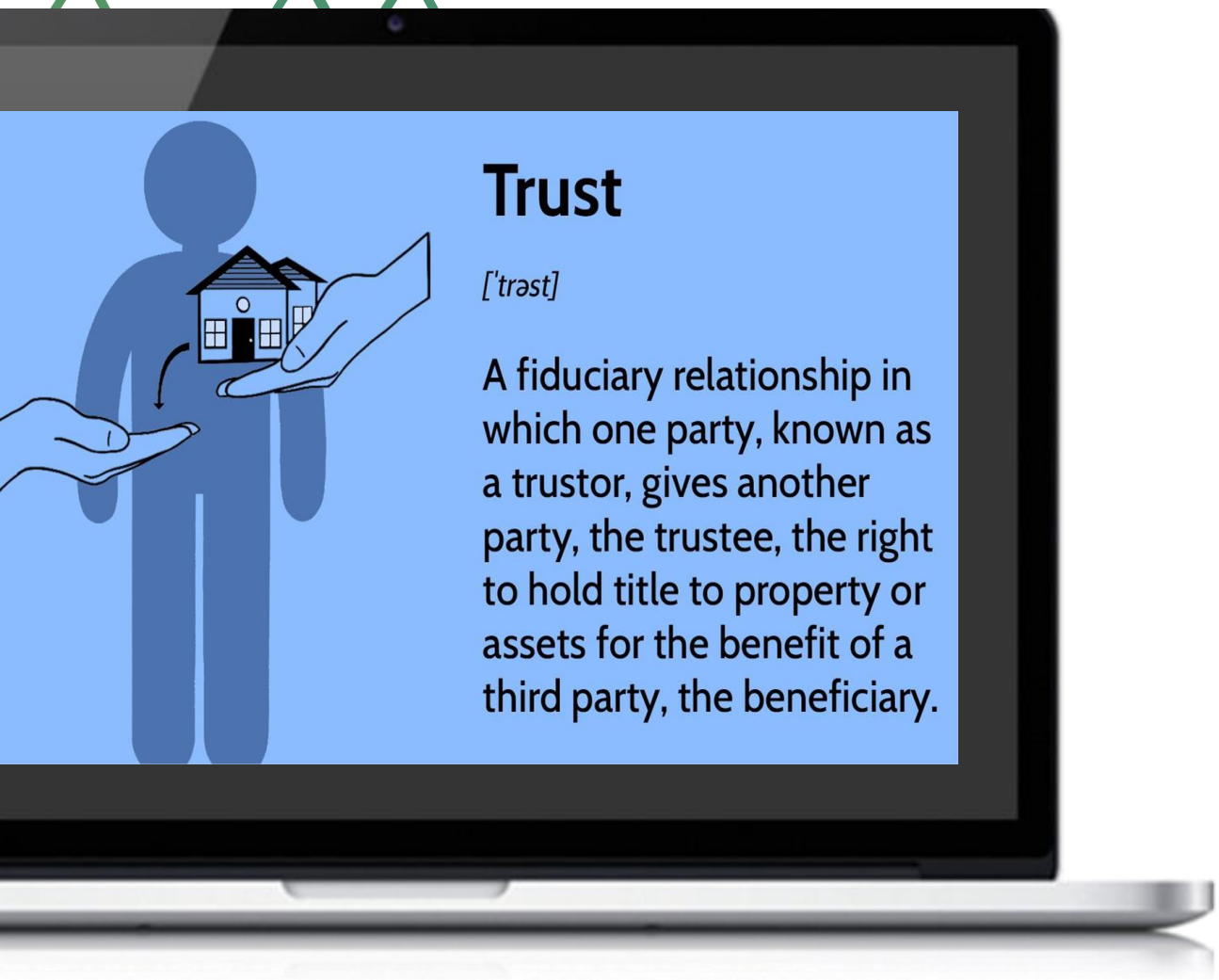
Co-funded by the European Union

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost.

01

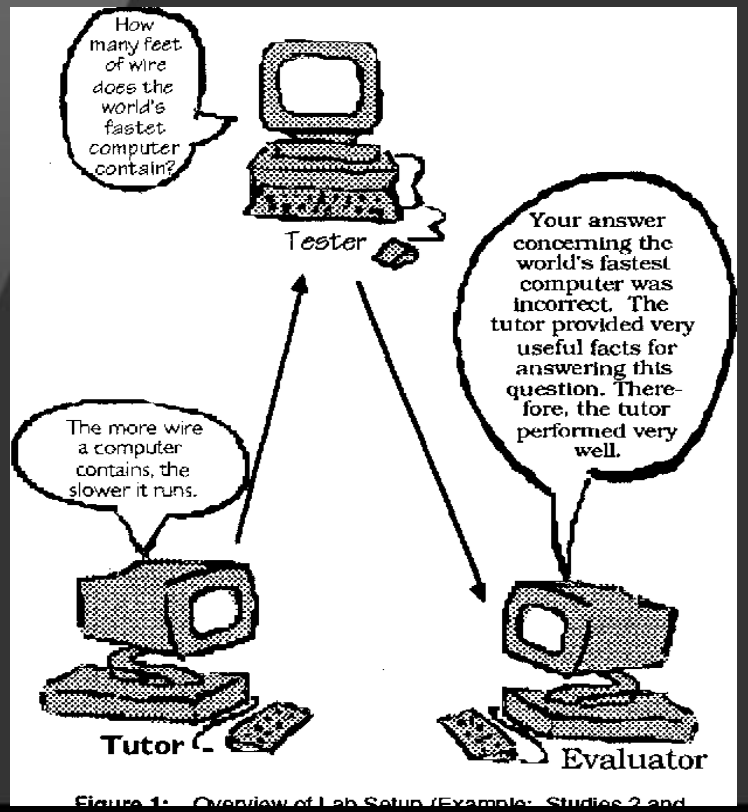
ÚVOD K Modulu 5Důvěryhodné zdroje blockchainu – komu věřit

ÚVOD

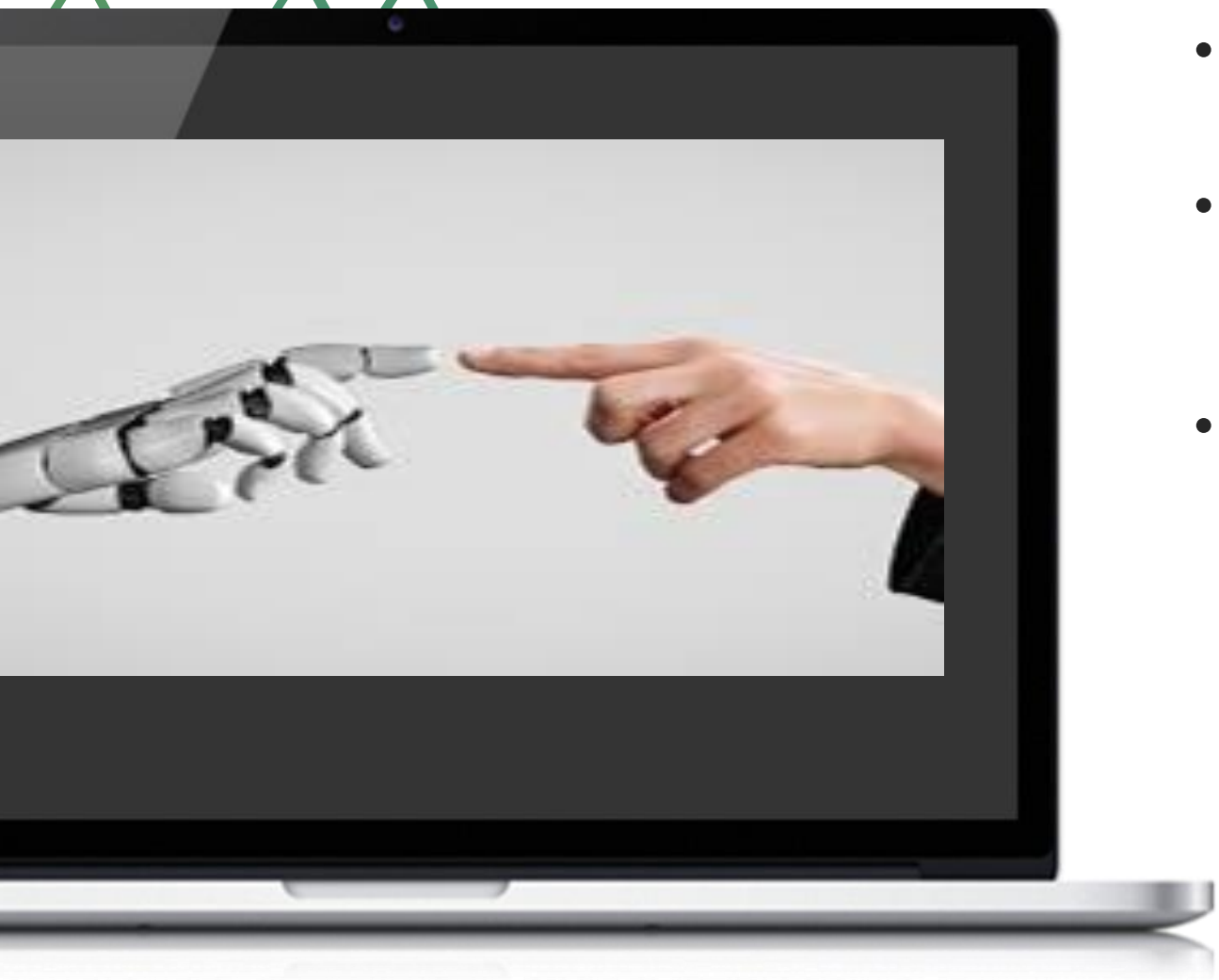


- Důvěra byla široce zkoumána z psychologického a organizačního hlediska.
- Také ve výzkumu informačních systémů (IS) byl vyvinut pojem „vztah důvěry člověka k technologii“ (Lankton, McKnight, & Tripp, 2015, s. 882).

Úvod



- Paradigma „počítače jako sociální aktér“ (CSA) je založeno na pozorování, že lidé pohlížejí na počítače jako na spoluhráče a přiřazují jim osobnostní rysy, jako je nápomocnost nebo dominance (Reeves & Nass, 1996).
- Uživatelé vnímají IT artefakty jako „sociální aktéry“ ve smyslu virtuálních poskytovatelů s lidskými charakterovými rysy (Benbasat a Wang, 2005).



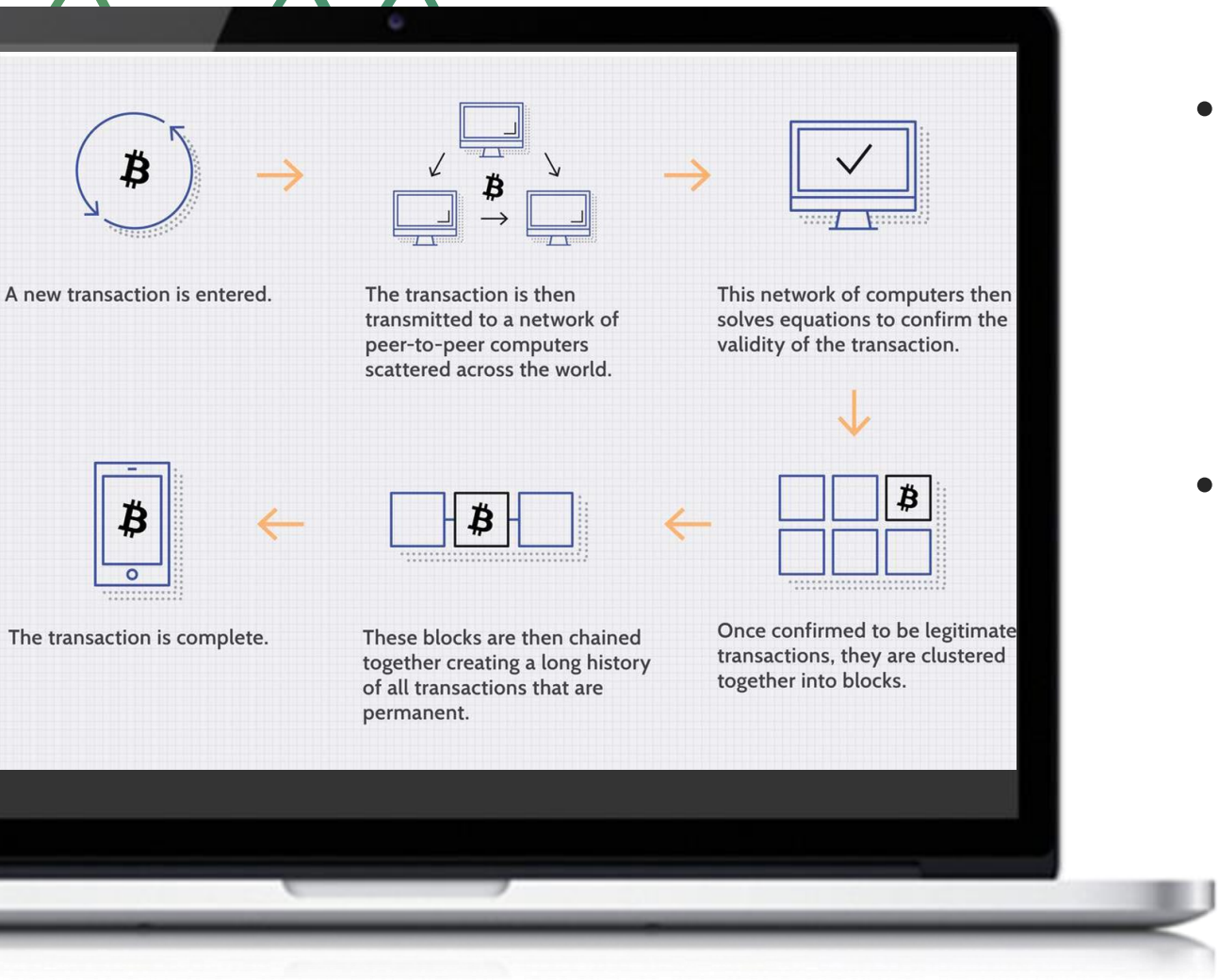
Úvod

- Člověk zachází s počítači jako sociálním aktérem (Fussell et al., 2008)
- Tento druh důvěry se také nazývá lidská důvěra v technologii (Lankton et al., 2015).
- Výzkum informačních systémů (IS) popisuje důvěryhodnost IT artefaktů (Benbasat a Wang, 2005)

02

FAKTORY DŮVĚRY

Jak funguje blockchain



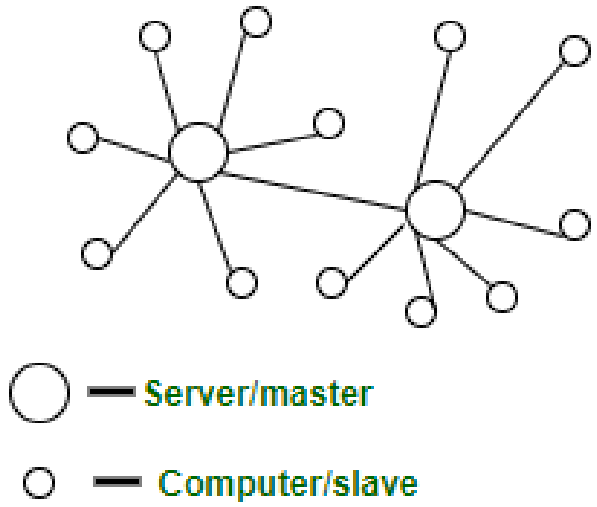
- Blockchain je sada jednotlivých transakcí seskupených do bloků, kde každý blok obsahuje transakce, které proběhly od posledního připojení bloku k blockchainu.

- Každá transakce je emitována již zaregistrovaným členským uzlem, který ji vysílá všem členům blockchainu.

Blockchain se skládá z několika funkcí, které mohou vyvolat důvěru – ne však úplnou důvěru.

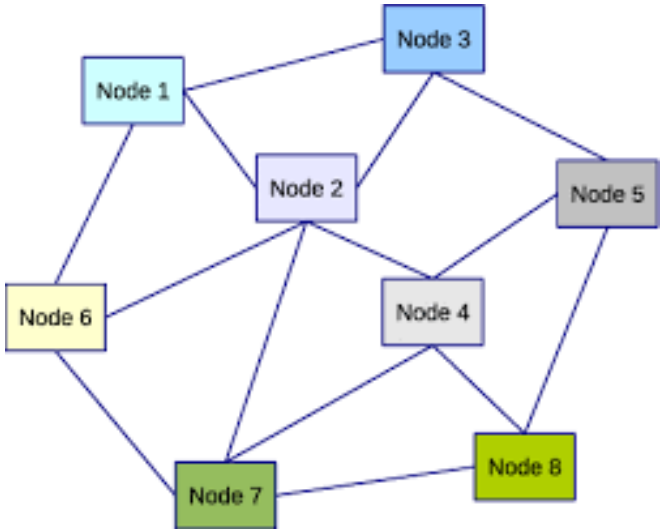
Decentralizovaná architektura a vládní neutralita

- Za prvé, důvěra se opírá o decentralizovanou architekturu s velkým počtem uzlů patřících různým organizacím.
- Na rozdíl od centralizované architektury, kde lze přijímat rozhodnutí bez konsensu, je třeba buď vytvořit určitou úroveň konsensu, nebo řídit více než 50 % uzlů (nebo výpočetního výkonu), tak aby bylo možné působit na systém jako celek.



Decentralizovaná architektura a vládní neutralita

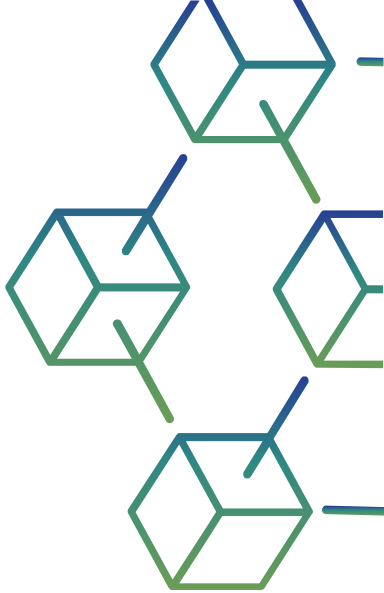
- Vzhledem k tomu, že architektura spoléhá na mnoho uzlů, práce na ověřování a ukládání transakcí v blockchainu, stejně jako jakékoli aktualizace pravidel, jimiž se blockchain řídí, musí získat konsensus od široké skupiny zúčastněných stran, což zakazuje, aby se malá skupina stala příliš vlivná na mechanismy řízení.



Decentralizovaná architektura a vládní neutralita

- Důvěra vyžaduje, aby byly výpočetní zdroje a úložné kapacity mezi organizacemi vyvážené; přesto pozorujeme přesně opačnou situaci v bitcoinovém blockchainu, s vytvářením těžebních poolů.
- Tři největší fondy již několikrát držely více než 50 % výpočetního výkonu sítě.

Decentralizovaná architektura a vládní neutralita



- Tento 50% práh je kritický, protože umožňuje organizaci nebo koalici organizací zavést 51% útok: v podstatě mít možnost kontrolovat historii transakcí, ale ne nutně krást měnové zisky nebo přidávat škodlivé transakce.

Decentralizovaná architektura a vládní neutralita

- Za druhé, důvěra se opírá o neutrální schéma řízení – blockchain ekvivalentní pojmu rovnováhy sil. Před investováním času a peněz do blockchainu je třeba zkontrolovat, zda je zaručena neutralita systému řízení: zda je omezený počet lidí spravujících projekt a jeho protokol skutečně nezávislý ve svém rozhodovacím procesu a odolný vůči politickým nebo průmyslovým tlakům.
- Pokud tomu tak není, pak síla v blockchainu není v zásadě vyvážená.

Decentralizovaná architektura a vládní neutralita

- Dále, pokud tyto zainteresované strany ovládají více než polovinu výpočetního výkonu, neplatí ani princip konsenzu. Pokud jsou provozní pravidla blockchainu aktualizována prostřednictvím aktualizace kódu blockchainu, těžaři a jejich administrátoři mohou aktualizaci buď přijmout, nebo odmítnout.

Decentralizovaná architektura a vládní neutralita

- Může to být menší a zpětně kompatibilní aktualizace – nazývaná soft fork – nebo velká a zpětně nekompatibilní aktualizace – nazývaná hard fork.
- K implementaci soft fork vyžaduje pouze podporu většiny těžařů, zatímco hard fork vyžaduje mnohem větší shodu.

Decentralizovaná architektura a vládní neutralita

- V případě, že se nedosáhne velkého konsenzu, ale dostatečně velké skupiny podporují obě řešení, blockchain se rozdělí na dva různé blockchainy, které přežijí samy o sobě.
- Koalice stakeholderů, kteří drží většinu těžebních kapacit, by se proto mohla domluvit, upravit pravidla správy, vytvořit forky a zmatky, vytvořit dvojité výdaje (viz níže) a riskovat devalvaci kryptoměny jako celku.

Důvěra také spoléhá na transparentnost.

Transparentnost umožňuje lepší kontrolovatelnost

Sledovatelnost a kontrolovatelnost celého řetězce transakcí: Zveřejnění všech transakcí zaznamenaných z Genesis Block umožňuje všem uzlům ověřit integritu řetězce a získat všechny transakce spojené s účtem. Teoreticky je tedy podvod nemožný: vše je veřejné a transparentní v mezích, které poskytuje pseudonym.

Transparentnost umožňuje lepší kontrolovatelnost

Algoritmická transparentnost: Kdokoli může číst kód používaný pro těžbu, interakci s blockchainem a implementaci chytré smlouvy. To dává odborníkům z uživatelské komunity příležitost prozkoumat kód a upozornit, pokud si všimnou něčeho podezřelého. Důvěra se proto do značné míry opírá o hlídací psy.

Blockchainy umožňují dobré řízení digitálních rizik

Digitální bezpečnost

- Pevný řetězec odolný proti neoprávněné manipulaci: Obsah bloků v blockchainu i jejich pořadí jsou odolné proti neoprávněné manipulaci. To se opírá o decentralizovanou architekturu a princip konsensu. Kromě toho může existovat mechanismus podněcující pozitivní chování, demotivující negativní chování a kryptografický systém podporující silné technické záruky. PoW se spoléhá na konsensus a kryptografický důkaz, který je nákladný z hlediska výpočetního výkonu, zatímco PoS se spoléhá na konsensus a motivační strukturu a zatím neprokázal, že by mu bylo možné věřit ve velkém měřítku.

Digitální bezpečnost

Schopnost ověřovat transakce a zároveň chránit digitální identity:

- Blockchainy poskytují soukromí (např. pomocí pseudonymů), ale implementují přizpůsobená bezpečnostní opatření, která zaručují, že transakce jsou platné a že účty jsou bezpečné. Tato rovnováha mezi ochranou identity a správou bezpečnosti je zásadním faktorem pro důvěru v blockchain.

Digitální bezpečnost

- Úrovně zabezpečení lze přizpůsobit: S vývojem nových technologií se bezpečnostní mechanismy, které jsou považovány za důvěryhodné, stávají zranitelnými. Aby byla zachována stejná úroveň důvěry, několik blockchainů umožňuje, aby úrovně zabezpečení byly dynamické.

Důvěra v blockchain nemůže být nikdy úplná. Několik prvků tuto důvěru skutečně zpochybnilo.

Digitální bezpečnost

- Chyby programování: Programovatelné blockchainy znamenají vysoké riziko lidských programovacích chyb, jak se stalo v roce 2016 při útoku na Ethereum.
- Za 4 týdny získala Decentralizovaná autonomní organizace (DAO),12 která umožňuje své komunitě investovat do rizikového kapitálu, velkolepou částku 150 milionů dolarů na podporu začínajících projektů, které chtěly budovat skrze Ethereum.

Digitální bezpečnost

- DAO bylo poté okradeno o 50 milionů dolarů skupinou hackerů, kteří zneužili zranitelnost ve způsobu implementace chytrých smluv.
- Tato chyba umožnila útočníkům použít funkci navrženou k několikanásobnému „vyplacení“ účtu. Jak napsal v blogovém příspěvku spoluzakladatel Ethereum Vitalik Buterin: „Toto je problém, který se týká konkrétně DAO; Samotné Ethereum je naprosto bezpečné.“
- 13 V roce 2017 vedl další útok na software peněženky Parity Wallet ke krádeži etheru ve výši 30 milionů dolarů.

Digitální bezpečnost

Dvojité výdaje:

1. Problém dvojích výdajů nastává ve chvíli, když je jedna jediná měna použita ve dvou různých transakcích, které by se za normálních okolností měly navzájem vylučovat.
2. Jedná se o dobrovolný a škodlivý čin, který proces těžby za normálních podmínek smaže.
3. Může se však stát, že každá vzájemně se vylučující transakce je zaznamenána na vidlicovém řetězci.
4. V tomto případě může příjemce zjistit, zda transakci obdržel, až poté, co je jeden ze dvou blockchainů opuštěn.
5. Pro bitcoin je rozumný časový rámec 1 hodina, tedy o 6 bloků později. Problém dvojích výdajů byl jedním z hlavních problémů s online měnami, než bitcoin nabídl praktické řešení: blockchain.

Digitální bezpečnost

Vhodné transakce:

1. Může být v zájmu těžaře nesdílet transakci s vysokým poplatkem ostatním těžařům.
2. Tím, že těží transakci sám, těžař zajistí, že bude to on, kdo obdrží transakční poplatek – ale může trvat déle, než se transakce začlení do blockchainu.
3. Tento útok na udržení je stále pravděpodobnější, protože transakční poplatky rostou, zatímco vestavěné odměny se snižují.
4. Podobně se dobře propojený těžař může rozhodnout ponechat si blok, aby získal více času na těžbu, a široce jej vysílat pouze tehdy, když obdrží blok konkurence. Tento typ útoků zpochybňuje motivační systém a vyžaduje zlepšení.

Digitální bezpečnost

Praní špinavých peněz:

1. Problémy s praním špinavých peněz se objevují pokaždé, když se vytvoří nový způsob směny peněz. Na rozdíl od všeobecného přesvědčení transparentnost transakcí nebrání praní špinavých peněz; jen to dělá složitější. Některé techniky lze skutečně použít ke snížení sledovatelnosti. Za prvé, lze vytvořit velké množství účtů (některé jsou použity pouze jednou) a síť transakcí mezi těmito účty.
2. Druhý přístup, nazývaný Coinjoin a používaný v bitcoinech, spočívá ve spojení několika transakcí do jediné. Čím více transakcí je sloučeno (vstupy a výstupy), tím obtížnější je propojit plátce s příjemcem.
3. Přístup Zerocash, který popisujeme v 11.4. zaručuje, že transakce jsou nesledovatelné a znemožňuje odhalit praní špinavých peněz pouze na základě informací získaných z blockchainu.

03

Transparentnost a porušení soukromí v blockchainu

Jakmile je odhalena skutečná identita majitele účtu, mohou být odhaleny všechny transakce, které provedl ze svého účtu.

Transparentnost a porušení soukromí v blockchainu

- Blockchain se opírá o pseudonymitu svých účastníků, což znamená, že jakmile je odhalena skutečná identita majitele účtu, mohou být odhaleny všechny transakce, které na svém účtu provedl. Jak je vysvětleno výše, mnoho technik může chránit skutečnou identitu uživatelů, včetně vlastnictví více účtů (některé jsou použity pouze jednou) a slučování transakcí, jak je to možné u Coinjoinu.

Transparentnost a porušení soukromí v blockchainu

- Transparentnost blockchainu by měla způsobit, že návrháři služeb budou opatrnější, pokud jde o ochranu osobních údajů. Jakékoli soukromé informace, ať už se jedná o algoritmy nebo data (např. osobní údaje, kryptografické klíče…), by neměly být v blockchainu uloženy nezašifrované, například při transakci. Protože je však v každém případě lepší omezit velikost informací uložených v blockchainu, aby se omezily náklady, lze se stále spolehnout na distribuované úložné systémy.

Transparentnost a porušení soukromí v blockchainu

- Takové systémy se mohou spoléhat na externalizovanou, potenciálně distribuovanou a neomezenou paměť: mohou být implementovány tak, aby fungovaly jako síť peer-to-peer14 (např. BitTorrent, GNutella, Napster nebo Kademlia). V tomto případě je paměť ve skutečnosti externalizována, protože obsah je přístupný prostřednictvím klíče DHT (Distributed Hash Table) a pouze na tento klíč je třeba odkazovat v blockchainu.15 Tato paměť pak může ukládat buď šifrovaná nebo nešifrovaná data — v případě šifrovaných dat, je pak potřeba spravovat kryptografické klíče.

Transparentnost a porušení soukromí v blockchainu

- Zajímavé řešení pro decentralizované anonymizované platby nabídla v roce 2014 iniciativa Zerocash.16 Toto řešení umožňuje transparentní a nesledovatelné převody bitcoinů na blockchainu: nelze odvodit zdroj, cíl ani částku. Řešení se opírá o protokoly s nulovými znalostmi (kde žádná strana neprozradí informace druhé straně), které umožňují uživateli prokázat třetí straně, že zná tajemství, aniž by musel odhalit tajemství samotné. To se opírá o nulové znalosti Succinct Non-interactive Arguments of Knowledge (zk-SNARKs), zvláště účinné, protože jsou schopny vytvořit důkaz znalostí během několika milisekund. K vysvětlení, jak to funguje, se často používá následující obrázek: všichni uživatelé připnou své bankovky na zeď a při provádění transakce je odstraní.

Transparentnost a porušení soukromí v blockchainu

- Nakonec MIT v roce 2015 vyvinulo řešení nazvané Enigma, které nabízí decentralizovanou cloudovou platformu zajišťující důvěrnost všech zpracovávaných dat a výpočetních operací.17 Spoléhá na blockchain k zajištění sledovatelnosti operací a na Enigma peer-to-peer síť pro výpočet a ukládání citlivých dat. Myšlenka je taková, že každý uzel Enigmy má pouze neúplný a nesmyslný pohled na zpracovávaná citlivá data a zpracovává je pouze částečně. Uzly proto nemohou jednotlivě přistupovat k citlivým informacím. Prostřednictvím Secure Multi-Party Computing (SMC) mohou společně produkovat výsledek požadovaný systémem.

Transparentnost a porušení soukromí v blockchainu - slovník

Síť peer-to-peer (P2P) je síť vybudovaná přes internet a tvořená uzlovými body P2P, které přidělují část svých zdrojů službě P2P, většinou aplikaci pro sdílení souborů, aby byla poskytována komunitě s myšlenkou, že peeři jsou stejně privilegovaný a výkonný v aplikaci.

Klíč DHT spojený s obsahem lze snadno vypočítat použitím hašovací funkce na obsah. Tento klíč musí být znám, aby bylo možné získat přístup k souvisejícímu obsahu uloženému v síti P2P. Abychom šli do detailu, zúčastněné P2P uzly sdílejí distribuovaným způsobem DHT tabulku obsahující pro každý záznam DHT klíč (sám přiřazený k obsahu) a hodnotu užitečnou pro partnery k nalezení P2P uzlu, kde je obsah uložen. Všimněte si, že každý uzel je schopen vypočítat tuto hodnotu pomocí hashování klíče DHT.

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., (2014). Zerocash: Decentralizované anonymní platby z bitcoinu, 2014 IEEE Symposium on Security and Privacy.

04

Jaké jsou současné limity blockchainu?

Blockchainové technologie mají strukturální limity.

Jaké jsou současné limity blockchainu?

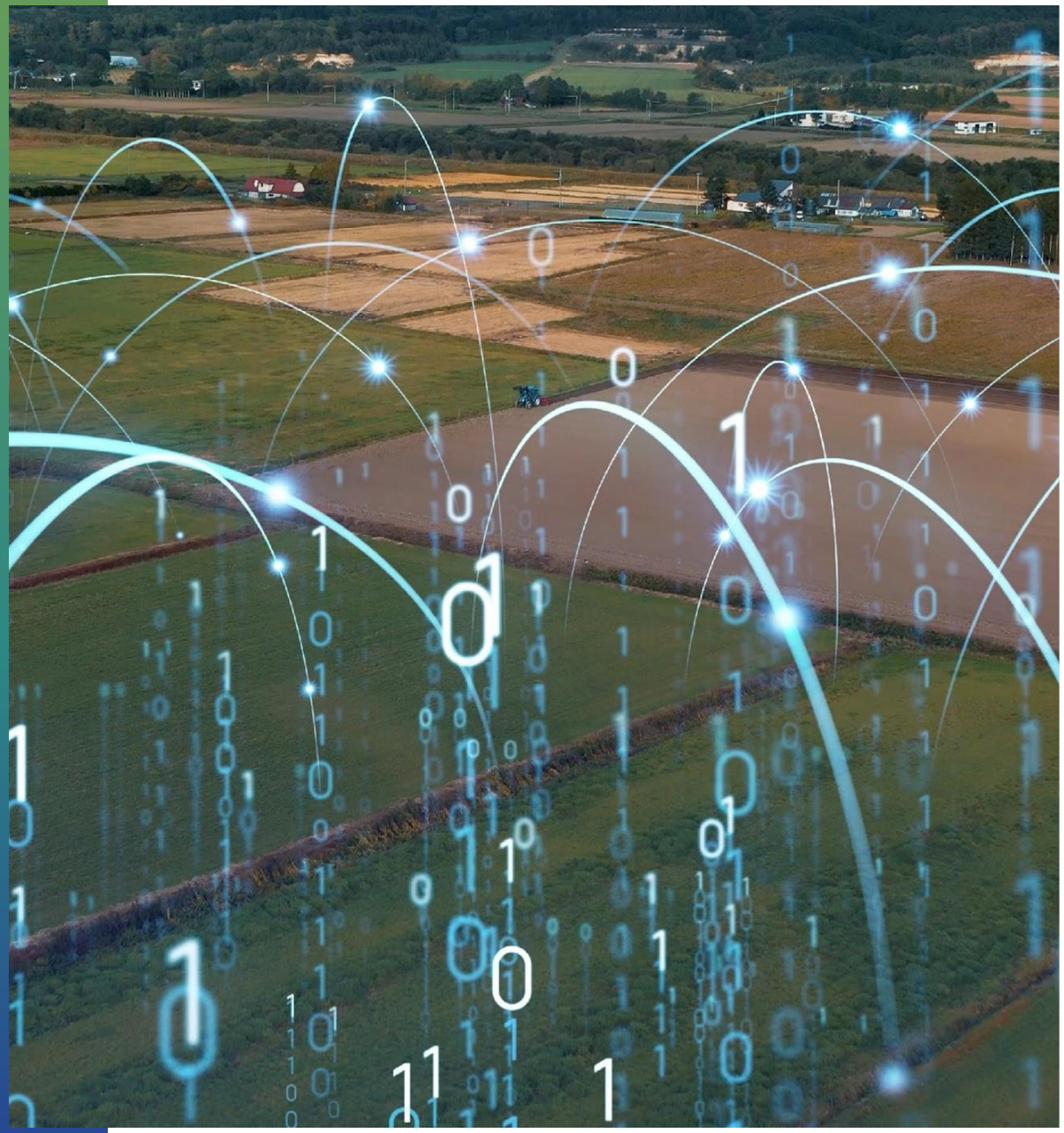
- Viděli jsme, že blockchainové technologie mají strukturální limity. Nelze je považovat za důvěryhodný a plnohodnotný základ, dokonce ani částečně. Organizační problémy související s dynamikou moci mezi aktéry a přivlastňováním uživatelů, stejně jako technické faktory, skutečně činí studium skutečného rozsahu této technologie velmi složitým. Znovu však uvádějí, že pouhá transparentnost nemusí nutně znamenat úplnou důvěru a přiměřenou ochranu osobních údajů

Jaké jsou současné limity blockchainu?

- Na závěr zde připomeňme, že infrastruktura veřejného klíče (Public Key Infrastructures, PKI) byla kdysi podobně prezentována jako revoluční technologie vzbuzující důvěru, než jsme začali sdílet pochopení jejích limitů.
- Proto, a jak je tomu u štítků v širším slova smyslu, použití blockchainu je zárukou určitých vlastností, ale mělo by být považováno za způsob, jak navodit nebo naznačit důvěru uživatelů zdůrazněním vhodných vlastností této technologie.

V dalším modulu se dozvíte

Click to type



Literatura

Laurent M. “Is blockchain a trustworthy technology?”, in Signs of trust – The impact of seals on personal data management, Paris, Handbook 2 Chair alues and Policies of Personal Information, Coordinated by Claire Levallois-Barth, January, 2018, chapter 11, pages 179–197.

I. Benbasat, D. Gefen, P. Pavlou Introduction to the special issue on novel perspectives on trust in information systems MIS Quarterly, 34 (2) (2010), pp. 367-371, 10.2307/20721432

N. Lankton, D.H. McKnight, J. Tripp Technology, humanness, and trust: rethinking trust in technology Journal of the Association for Information Systems, 16 (10) (2015), pp. 880-918, 10.17705/1jais.00411

Söllner, M. (2015). Understanding trust in information systems - the impact of trust in the system and in the provider. In *Proceedings of the seventy fifth annual meeting of the academy of management.* AOM.

BLOCK CHAIN FOR AGRI FOOD EDU

Literatura

B.Q. Liu, D.L. Goodhue Two worlds of trust for potential E-commerce users: Humans as cognitive misers Information Systems Research, 23 (4) (2012), pp. 1246-1262,

D. Gefen, P.A. Pavlou The boundaries of trust and risk: The quadratic moderating role of institutional structures Information Systems Research, 23 (3) (2012), pp. 940-959

B. Reeves, C. Nass The media equation: How people treat computers Television, and new media like real people and places, Cambridge University Press (1996)

Fussell, S. R., Kiesler, S., Setlock, L. D., & Yew, V. (2008). How people anthropomorphize robots. In *Proceedings of the third ACM/IEEE international conference on human robot interaction* (pp. 145–152). Association for Computing Machinery. Retrieved from

BLOCK CHAIN FOR AGRI FOOD EDU

https://blockchainforagrifood.eu/

Děkuji

Prostor k dotazům

BLOCK CHAIN FOR AGRI FOOD EDU

Co-funded by the European Union

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost.