Modul 5

Dôveryhodné zdroje blockchainu - komu dôverovať

Co-funded by the European Union

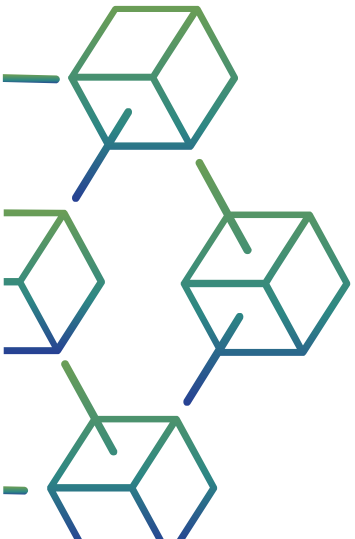
Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani EACEA za ne nepreberajú žiadnu zodpovednosť.

Popis modulu

- Téma: "**Dôveryhodné zdroje blockchainu - komu veriť**
- Význam: potenciál ilustrovať, do akej miery možno blockchain považovať za dôveryhodnú technológiu.
- Významné miesto v odbornej literatúre
- Odpovede na otázky o tom, do akej miery je používanie blockchainu v agropotravinárskom sektore dôveryhodné.

Výsledky štúdie

- **preukázanie** jasného pochopenia kľúčových vlastností technológie blockchain a jej dôveryhodnosti ako potenciálneho riešenia mnohých z týchto problémov
- **Analýza** úlohy technológie blockchain ako dôveryhodnej technológie
- **Posúdenie** dôveryhodnosti blockchainových technológií v agropotravinárskom dodávateľskom reťazci



obsah

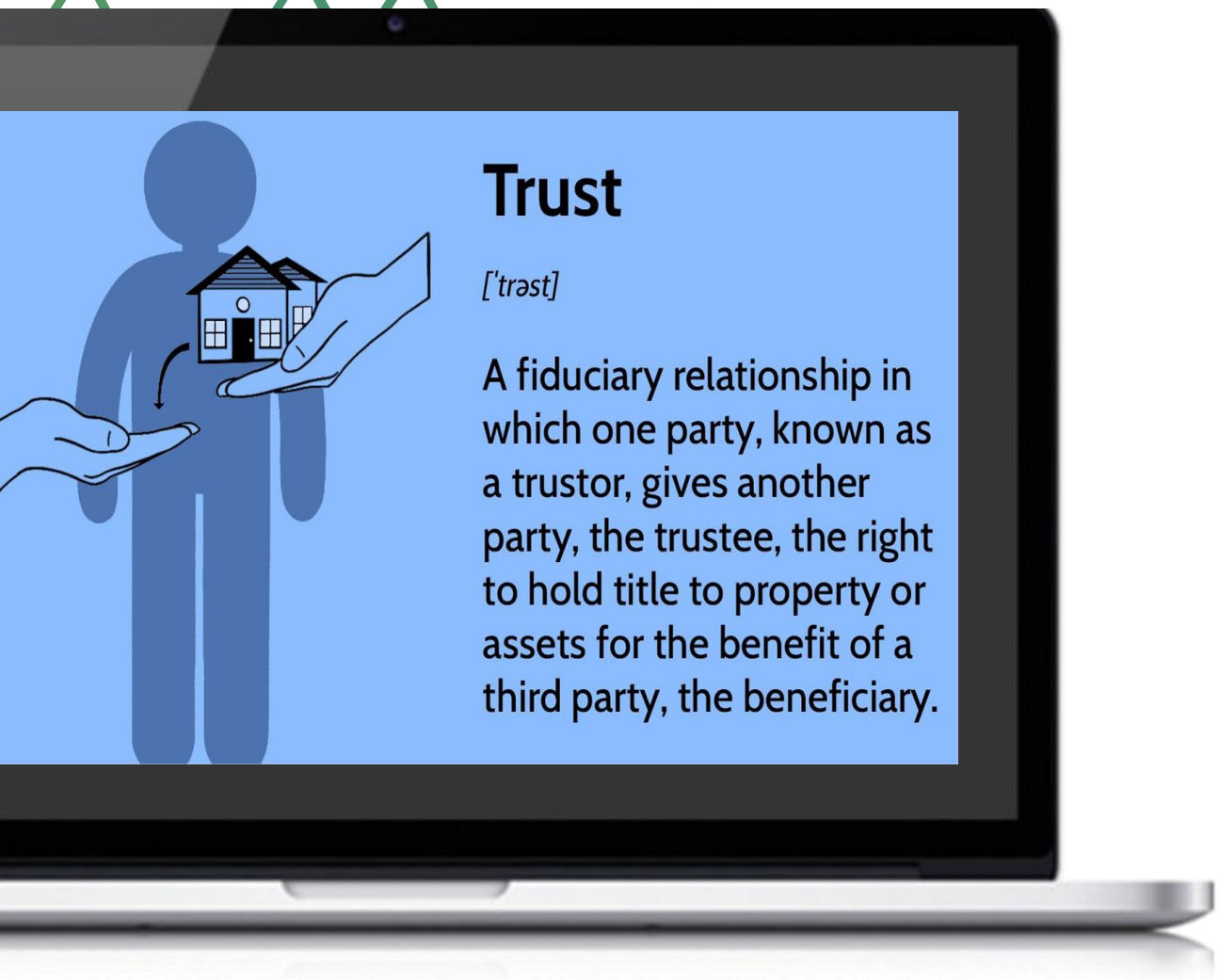
BLOCKCHAIN FOR AGRIFOOD EDU

Co-funded by the European Union

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani EACEA za ne nepreberajú žiadnu zodpovednosť.

01

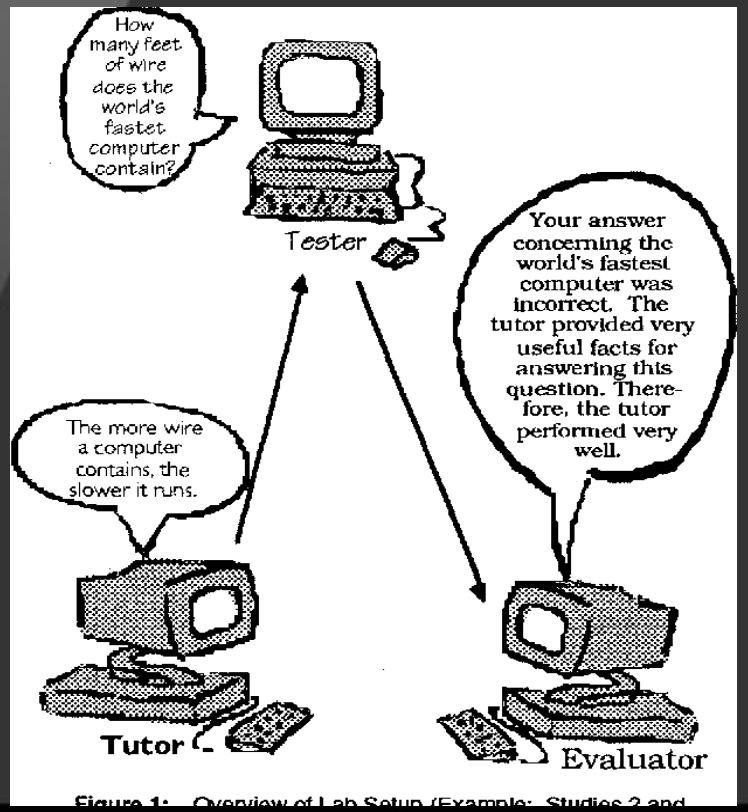
Úvod do modulu 5Dôveryhodné zdroje blockchainu - komu dôverovať



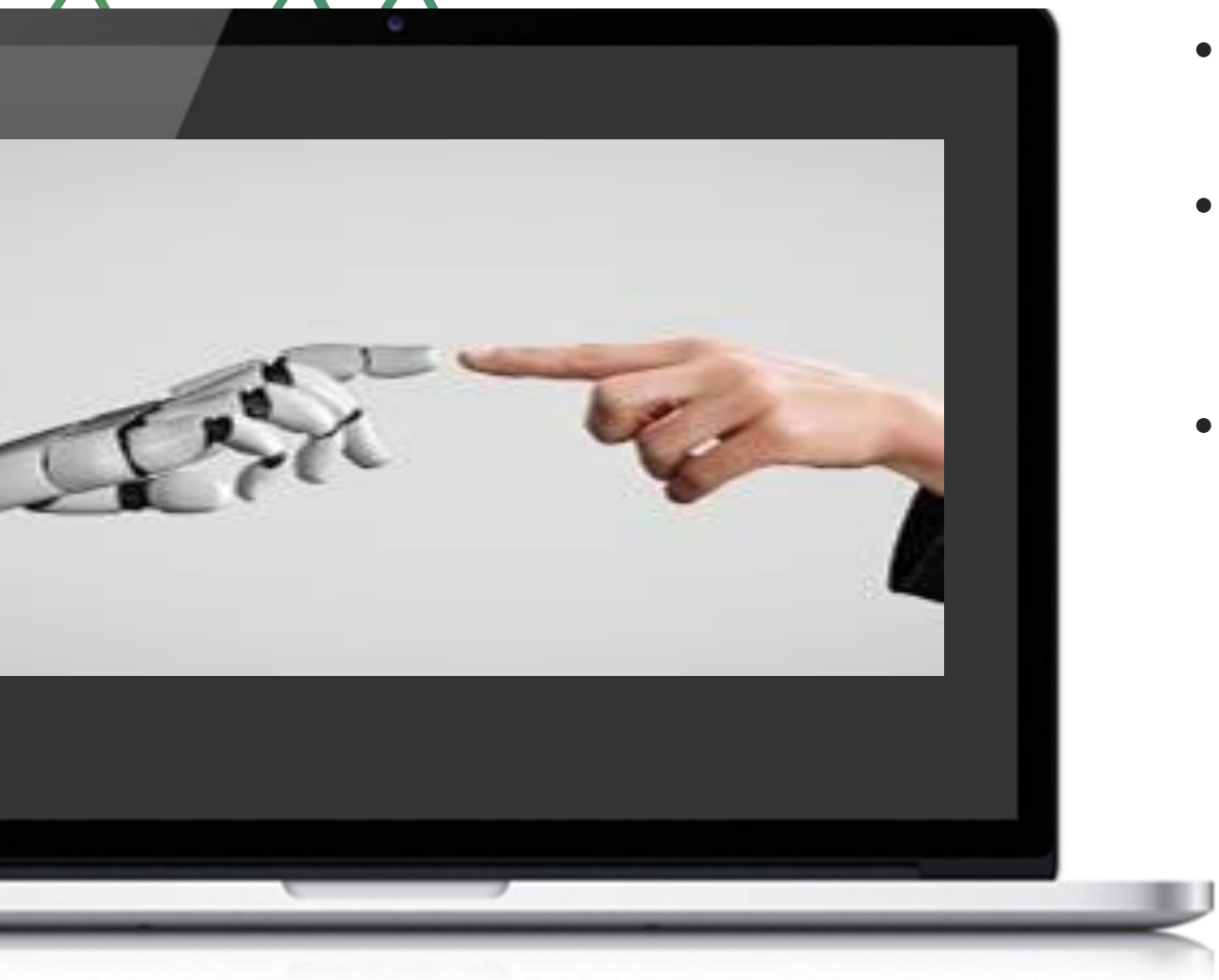
ÚVOD

- Dôvera bola podrobne preskúmaná z psychologického a organizačného hľadiska.
- Aj vo výskume informačných systémov (IS) bol vyvinutý koncept "vzťahu dôvery medzi človekom a technológiou" (Lankton, McKnight, & Tripp, 2015, s. 882).

Domov



- Paradigma počítačov ako sociálnych aktérov (CSA) vychádza z pozorovania, že ľudia vnímajú počítače ako spoluhráčov a pripisujú im osobnostné vlastnosti, ako je ústretovosť alebo dominancia (Reeves a Nass, 1996).
- Používatelia vnímajú IT artefakty ako "sociálnych aktérov" v zmysle virtuálnych poskytovateľov s ľudskými charakterovými vlastnosťami (Benbasat a Wang, 2005).



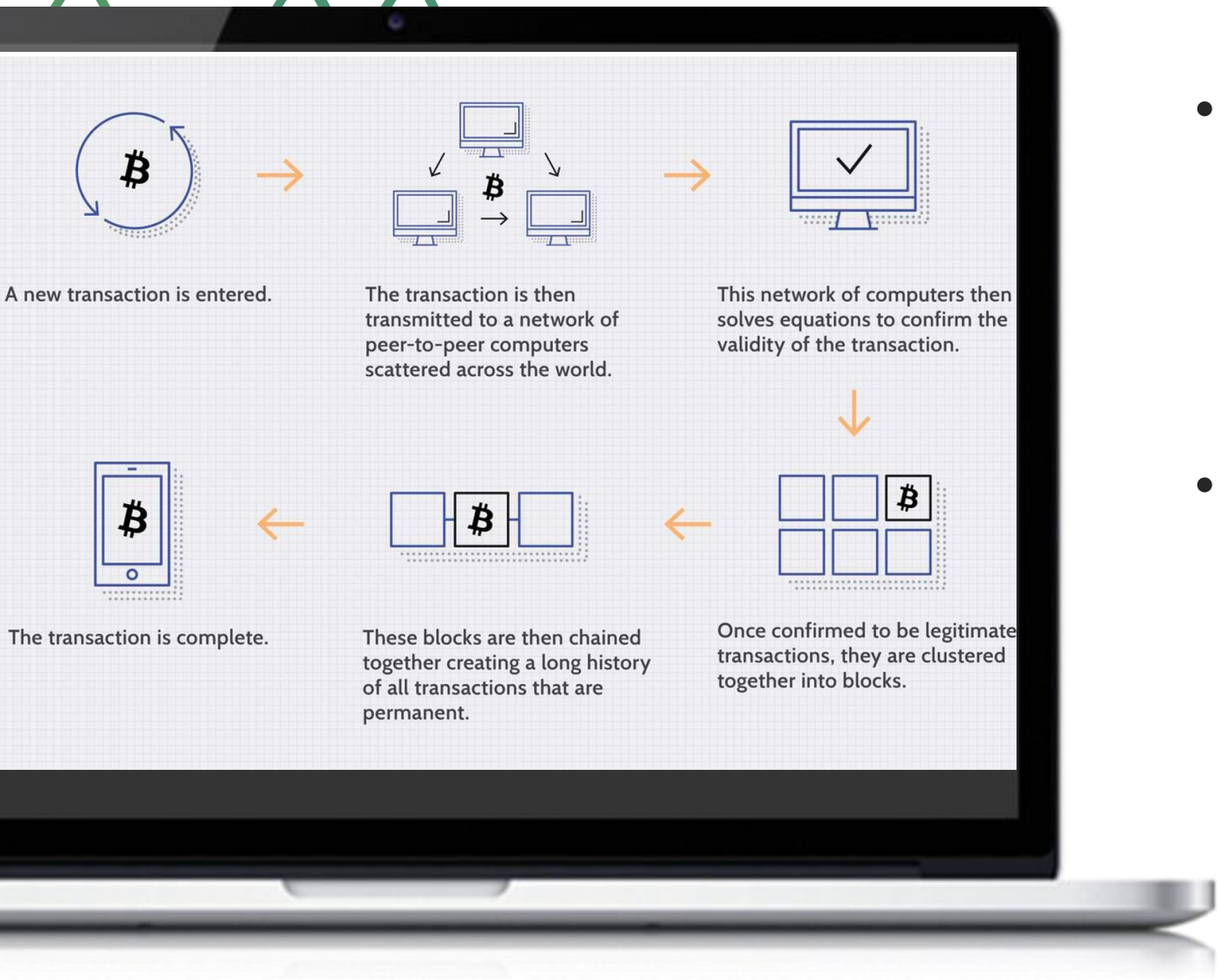
Domov

- Ľudia sa správajú k počítačom ako k sociálnym aktérom (Fussell a kol., 2008)
- Tento druh dôvery sa nazýva aj ľudská dôvera v technológie (Lankton a kol., 2015).
- Výskum informačných systémov (IS) opisuje dôveryhodnosť artefaktov IT (Benbasat a Wang, 2005).

02

FAKTORY DÔVERY

Ako funguje blockchain



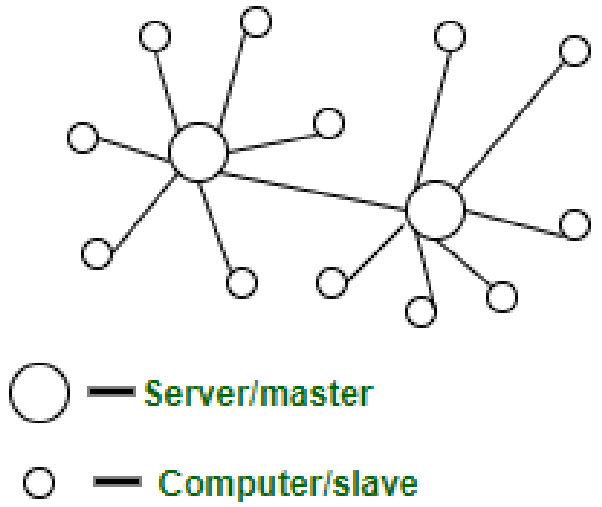
- Blockchain je súbor jednotlivých transakcií zoskupených do blokov, pričom každý blok obsahuje transakcie, ktoré sa uskutočnili od posledného pripojenia bloku k blockchainu.

- Každá transakcia je vydaná už registrovaným členským uzlom, ktorý ju rozošle všetkým členom blockchainu.

Blockchain sa skladá z niekoľkých prvkov, ktoré môžu vyvolať dôveru - ale nie úplnú.

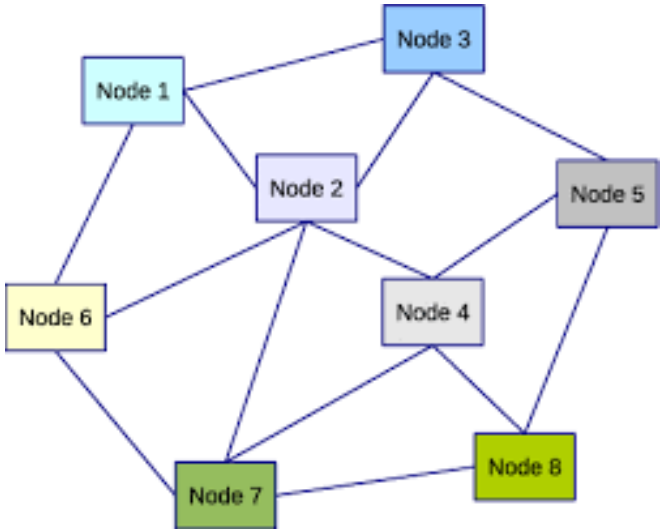
Decentralizovaná architektúra a neutralita vlády

- Po prvé, dôvera sa opiera o decentralizovanú architektúru s veľkým počtom uzlov patriacich rôznym organizáciám.
- Na rozdiel od centralizovanej architektúry, kde sa rozhodnutia môžu prijímať bez konsenzu, je potrebné buď vytvoriť určitú úroveň konsenzu, alebo spravovať viac ako 50 % uzlov (alebo výpočtového výkonu), aby sa ovplyvnil systém ako celok.



Decentralizovaná architektúra a neutralita vlády

- Keďže architektúra sa spolieha na mnoho uzlov, práca na overovaní a ukladaní transakcií v blockchaine, ako aj akékoľvek aktualizácie pravidiel, ktorými sa blockchain riadi, musia získať konsenzus širokej skupiny zainteresovaných strán, čo zabraňuje tomu, aby malá skupina získala príliš veľký vplyv na mechanizmy riadenia.



Decentralizovaná architektúra a neutralita vlády

- Dôvera si vyžaduje, aby boli výpočtové zdroje a úložná kapacita vyvážené medzi organizáciami, avšak v bitcoinovom blockchaine sme svedkami presne opačnej situácie, a to vytvárania ťažobných skupín.
- Tri najväčšie fondy niekoľkokrát vlastnili viac ako 50 % výpočtového výkonu siete.

Decentralizovaná architektúra a neutralita vlády

- Táto 50 % hranica je kritická, pretože umožňuje organizácii alebo koalícii organizácií uskutočniť 51 % útok: v podstate je možné kontrolovať históriu transakcií, ale nie nevyhnutne ukradnúť peňažné zisky alebo pridať škodlivé transakcie.

Decentralizovaná architektúra a neutralita vlády

- Po druhé, dôvera sa opiera o neutrálnu schému riadenia - blockchainový ekvivalent pojmu rovnováha moci. Pred investovaním času a peňazí do blockchainu je dôležité overiť, či je zaručená neutralita schémy riadenia: či obmedzený počet ľudí, ktorí riadia projekt a jeho protokol, je skutočne nezávislý pri rozhodovaní a odolný voči politickým alebo priemyselným tlakom.
- Ak to tak nie je, potom moc v blockchaine nie je v zásade vyvážená.

Decentralizovaná architektúra a neutralita vlády

- Navyše, ak tieto zainteresované strany kontrolujú viac ako polovicu výpočtového výkonu, neuplatňuje sa ani zásada konsenzu. Ak sa pravidlá fungovania blockchainu aktualizujú prostredníctvom aktualizácie kódu blockchainu, baníci a ich správcovia môžu aktualizáciu buď prijať, alebo odmietnuť.

Decentralizovaná architektúra a neutralita vlády

- Môže ísť o menšiu a spätne kompatibilnú aktualizáciu - tzv. soft fork - alebo o veľkú a spätne nekompatibilnú aktualizáciu - tzv. hard fork.
- Soft fork si vyžaduje len podporu väčšiny baníkov, zatiaľ čo hard fork si vyžaduje oveľa viac konsenzu.

Decentralizovaná architektúra a neutralita vlády

- V prípade, že sa nedosiahne veľký konsenzus, ale dostatočne veľké skupiny podporia obe riešenia, blockchain sa rozdelí na dva rôzne blockchainy, ktoré prežijú samostatne.
- Koalícia zainteresovaných strán, ktoré vlastnia väčšinu ťažobnej kapacity, by sa preto mohla dohodnúť, upraviť pravidlá riadenia, vytvoriť rozvetvenie a zmätok, vytvoriť dvojité výdavky (pozri nižšie) a riskovať znehodnotenie kryptomeny ako celku.

Dôvera závisí aj od transparentnosti.

Transparentnosť umožňuje lepšiu kontrolovateľnosť

Vysledovateľnosť a auditovateľnosť celého reťazca transakcií: Zverejnenie všetkých transakcií zaznamenaných z bloku Genesis umožňuje všetkým uzlom overiť integritu reťazca a získať všetky transakcie spojené s účtom. Teoreticky je teda podvod nemožný: všetko je verejné a transparentné v rámci limitov stanovených pseudonymom.

Transparentnosť umožňuje lepšiu kontrolovateľnosť

Algoritmická transparentnosť: ktokoľvek si môže prečítať kód používaný na ťažbu, interakciu s blockchainom a implementáciu inteligentnej zmluvy. Odborníci z komunity používateľov tak majú možnosť preskúmať kód a upozorniť naň, ak si všimnú niečo podozrivé. Dôvera sa preto vo veľkej miere spolieha na strážnych psov.

Blockchainy umožňujú dobré riadenie digitálnych rizík

Digitálne zabezpečenie

- Pevný reťazec odolný voči manipulácii: obsah blokov v blockchaine a ich poradie sú odolné voči manipulácii. To sa opiera o decentralizovanú architektúru a princíp konsenzu. Okrem toho môže existovať mechanizmus na stimuláciu pozitívneho správania, odrádzanie od negatívneho správania a kryptografický systém podporujúci silné technické záruky. PoW sa spolieha na konsenzus a kryptografický dôkaz, ktorý je nákladný z hľadiska výpočtového výkonu, zatiaľ čo PoS sa spolieha na konsenzus a motivačnú štruktúru a zatiaľ sa nepreukázalo, že je dôveryhodný vo veľkom rozsahu.

Digitálne zabezpečenie

Schopnosť overovať transakcie a zároveň chrániť digitálne identity:

- Blokové reťazce poskytujú súkromie (napr. prostredníctvom pseudonymov), ale implementujú prispôsobené bezpečnostné opatrenia na zabezpečenie platnosti transakcií a bezpečnosti účtov. Táto rovnováha medzi ochranou identity a riadením bezpečnosti je základom dôvery v blockchain.

Digitálne zabezpečenie

- Úrovne zabezpečenia je možné prispôsobiť: S vývojom nových technológií sa bezpečnostné mechanizmy, ktoré sú považované za dôveryhodné, stávajú zraniteľnými. Aby sa zachovala rovnaká úroveň dôveryhodnosti, viaceré blockchainy umožňujú dynamickú úroveň zabezpečenia.

Dôvera v blockchain nemôže byť nikdy úplná. Túto dôveru totiž spochybnilo niekoľko prvkov.

Digitálne zabezpečenie

- Chyby pri programovaní: programovateľné blockchainy predstavujú vysoké riziko ľudských programátorských chýb, ako sa stalo pri útoku na Ethereum v roku 2016.
- Decentralizovaná autonómna organizácia (DAO)12 , ktorá umožňuje svojej komunite investovať do rizikového kapitálu, získala za 4 týždne veľkolepých 150 miliónov dolárov na podporu startupov, ktoré chceli budovať prostredníctvom Etherea.

Digitálne zabezpečenie

- Skupina hackerov, ktorí zneužili zraniteľnosť v spôsobe implementácie inteligentných kontraktov, obrala DAO o 50 miliónov dolárov.
- Táto zraniteľnosť umožňovala útočníkom použiť funkciu určenú na viacnásobné "vyplatenie" účtu. Ako napísal spoluzakladateľ Etherea Vitalik Buterin v príspevku na blogu: "Ide o problém, ktorý sa týka konkrétne DAO; samotné Ethereum je úplne bezpečné."
- 13 V roku 2017 viedol ďalší útok na softvér Parity Wallet ku krádeži 30 miliónov dolárov v ethere.

Digitálne zabezpečenie

Dvojnásobné výdavky:

1. Problém dvojitých výdavkov vzniká vtedy, keď sa jedna mena používa pri dvoch rôznych transakciách, ktoré by sa za normálnych okolností mali navzájom vylučovať.
2. Ide o dobrovoľný a škodlivý čin, ktorý sa v procese extrakcie zvyčajne vymaže.
3. Môže sa však stať, že každá vzájomne sa vylučujúca transakcia bude zaznamenaná vo vidlicovom reťazci.
4. V tomto prípade môže príjemca zistiť, či transakciu prijal, až po opustení jedného z dvoch blockchainov.
5. V prípade bitcoinu je primeraný časový rámec 1 hodina, 6 blokov neskôr. Problém dvojitého míňania bol jedným z hlavných problémov online mien predtým, ako bitcoin ponúkol praktické riešenie: blockchain.

Digitálne zabezpečenie

Vhodné transakcie:

1. Môže byť v záujme ťažiara, aby sa o transakciu s vysokým poplatkom nepodelil s ostatnými ťažiarmi.
2. Ťažbou samotnej transakcie si ťažiar zabezpečí, že to bude on, kto dostane transakčný poplatok - môže však trvať dlhšie, kým sa transakcia zapíše do blockchainu.
3. Tento útok na retenciu je čoraz pravdepodobnejší, keďže poplatky za transakcie rastú, zatiaľ čo vložené odmeny klesajú.
4. Podobne sa môže dobre prepojený ťažiar rozhodnúť, že si blok ponechá, aby získal viac času na ťažbu, a odvysiela ho až vtedy, keď dostane blok od konkurencie. Tento typ útoku je výzvou pre motivačný systém a vyžaduje si zlepšenie.

Digitálne zabezpečenie

Pranie špinavých peňazí:

1. Problémy s praním špinavých peňazí vznikajú vždy, keď sa vytvorí nový spôsob výmeny peňazí. Na rozdiel od všeobecného presvedčenia transparentnosť transakcií nezabraňuje praniu špinavých peňazí, len ho sťažuje. Niektoré techniky sa skutočne dajú použiť na zníženie sledovateľnosti. Po prvé, možno vytvoriť veľký počet účtov (niektoré sa použijú len raz) a sieť transakcií medzi týmito účtami.
2. Druhý prístup, ktorý sa nazýva Coinjoin a používa sa v bitcoinoch, zahŕňa spojenie niekoľkých transakcií do jednej. Čím viac transakcií je zlúčených (vstupov a výstupov), tým ťažšie je prepojiť platiteľa s príjemcom platby.
3. Prístup Zerocash, ktorý opisujeme v časti 11.4, zabezpečuje, že transakcie sú nevystopovateľné a znemožňuje odhaliť pranie špinavých peňazí len na základe informácií získaných z blockchainu.

03

Transparentnosť a porušovanie súkromia v blockchaine

Po odhalení skutočnej totožnosti majiteľa účtu je možné odhaliť všetky transakcie vykonané z jeho účtu.

Transparentnosť a porušovanie súkromia v blockchaine

- Blockchain sa spolieha na pseudonymitu svojich účastníkov, čo znamená, že po odhalení skutočnej identity majiteľa účtu je možné odhaliť všetky transakcie, ktoré na svojom účte uskutočnil. Ako bolo vysvetlené vyššie, skutočnú identitu používateľov možno chrániť mnohými technikami vrátane vlastnenia viacerých účtov (niektoré sa používajú len raz) a spájania transakcií, ako je to možné v prípade Coinjoin.

Transparentnosť a porušovanie súkromia v blockchaine

- Vďaka transparentnosti blockchainu by mali byť tvorcovia služieb opatrnejší, pokiaľ ide o ochranu údajov. Akékoľvek súkromné informácie, či už ide o algoritmy alebo údaje (napr. osobné údaje, kryptografické kľúče...), by nemali byť v blockchaine uložené nezašifrované, napríklad počas transakcie. Keďže je však v každom prípade lepšie obmedziť veľkosť informácií uložených v blockchaine, aby sa obmedzili náklady, stále sa možno spoľahnúť na distribuované systémy ukladania.

Transparentnosť a porušovanie súkromia v blockchaine

- Takéto systémy sa môžu spoliehať na externú, potenciálne distribuovanú a neobmedzenú pamäť: môžu byť implementované tak, aby fungovali ako sieť peer-to-peer14 (napr. BitTorrent, GNutella, Napster alebo Kademlia). V tomto prípade je pamäť efektívne externalizovaná, keďže k obsahu sa pristupuje prostredníctvom kľúča distribuovanej hašovacej tabuľky (DHT) a v blockchaine sa treba odvolávať len na tento kľúč.15 V tejto pamäti sa potom môžu uchovávať buď šifrované, alebo nešifrované údaje - v prípade šifrovaných údajov je potrebné spravovať kryptografické kľúče.

Transparentnosť a porušovanie súkromia v blockchaine

- Zaujímavé riešenie decentralizovaných anonymných platieb ponúkla v roku 2014 iniciatíva Zerocash.16 Toto riešenie umožňuje transparentné a nevystopovateľné prevody bitcoinov v blockchaine: nie je možné zistiť zdroj, cieľ ani sumu. Riešenie sa opiera o protokoly s nulovou znalosťou (pri ktorých ani jedna strana neodhaľuje informácie druhej strane), ktoré umožňujú používateľovi dokázať tretej strane, že pozná tajomstvo bez toho, aby musel odhaliť samotné tajomstvo. To sa opiera o zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARK), ktoré sú obzvlášť účinné, pretože dokážu vytvoriť dôkaz o znalosti v priebehu niekoľkých milisekúnd. Na vysvetlenie toho, ako to funguje, sa často používa nasledujúca ilustrácia: všetci používatelia si pripnú svoje poznámky na stenu a pri vykonávaní transakcie ich odstránia.

Transparentnosť a porušovanie súkromia v blockchaine

- Napokon v roku 2015 MIT vyvinul riešenie s názvom Enigma, ktoré ponúka decentralizovanú cloudovú platformu, ktorá zabezpečuje dôvernosť všetkých spracúvaných údajov a výpočtových operácií.17 Na zabezpečenie sledovateľnosti operácií sa spolieha na blockchain a na peer-to-peer sieť Enigma na výpočet a ukladanie citlivých údajov. Podstata spočíva v tom, že každý uzol Enigmy má len neúplný a nezmyselný pohľad na spracovávané citlivé údaje a spracováva ich len čiastočne. Uzly preto nemôžu individuálne pristupovať k citlivým informáciám. Prostredníctvom Secure Multi-Party Computing (SMC) môžu spoločne vytvoriť výsledok požadovaný systémom.

Transparentnosť a porušenie súkromia v blockchaine - slovník pojmov

Sieť P2P (peer-to-peer) je sieť vybudovaná na internete a pozostávajúca z uzlov P2P, ktoré prideľujú časť svojich zdrojov službe P2P, zvyčajne aplikácii na zdieľanie súborov, ktorá sa má poskytovať komunite s myšlienkou, že rovnocenní používatelia sú v aplikácii rovnako privilegovaní a výkonní.

Kľúč DHT spojený s obsahom sa dá ľahko vypočítať použitím hashovacej funkcie na obsah. Tento kľúč musí byť známy, aby bolo možné pristupovať k súvisiacemu obsahu uloženému v sieti P2P. Ak chceme ísť do väčších podrobností, zúčastnené uzly P2P zdieľajú tabuľku DHT distribuovaným spôsobom, ktorá obsahuje pre každý záznam kľúč DHT (sám o sebe spojený s obsahom) a hodnotu užitočnú pre peerov na nájdenie uzla P2P, kde je obsah uložený. Všimnite si, že každý uzol je schopný vypočítať túto hodnotu hashovaním kľúča DHT.

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., (2014). Zerocash: Decentralized anonymous bitcoin payments, 2014 IEEE Symposium on Security and Privacy.

04

Aké sú súčasné limity blockchainu?

Technológie blockchain majú štrukturálne obmedzenia.

Aké sú súčasné limity blockchainu?

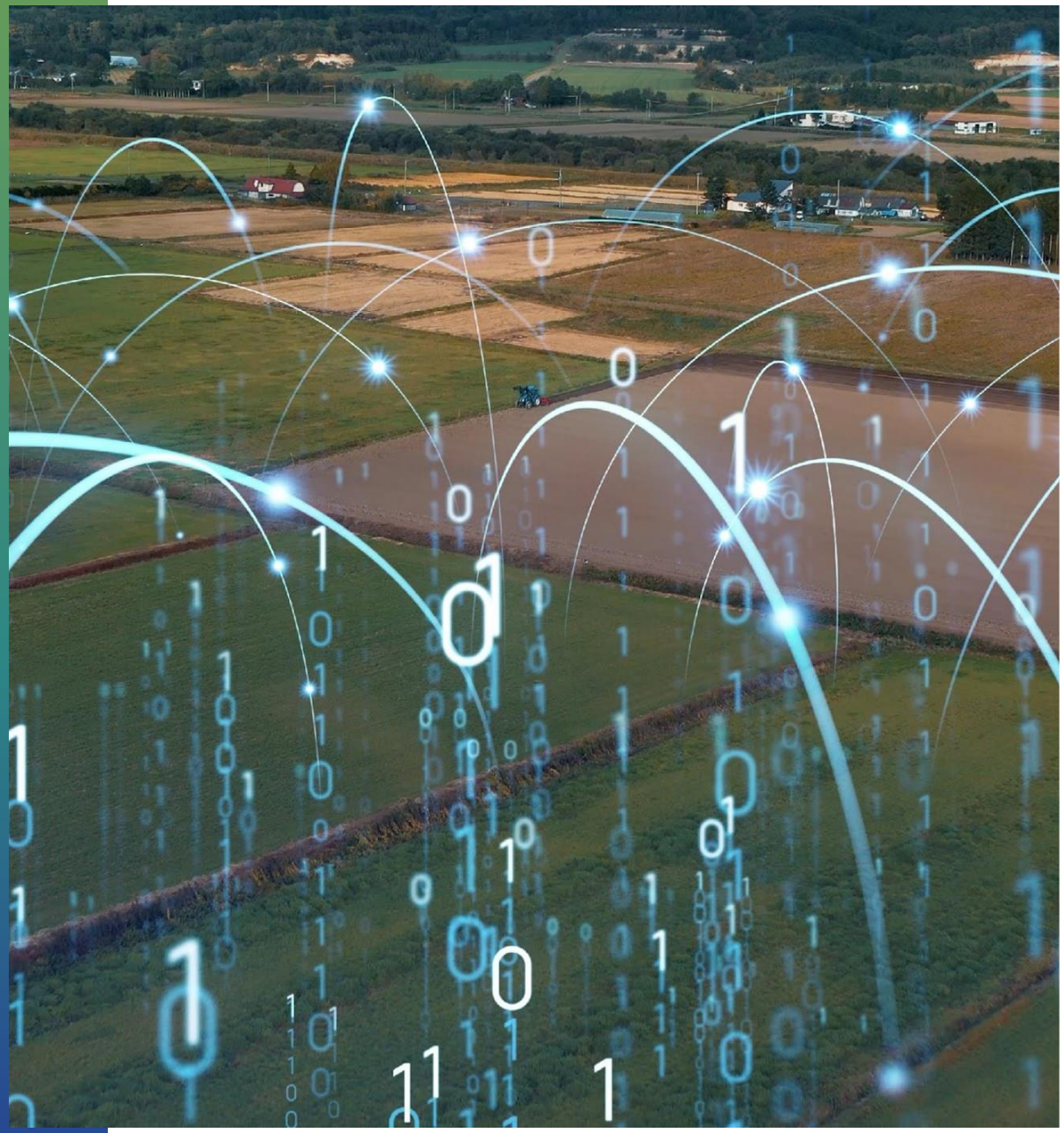
- Videli sme, že technológie blockchain majú štrukturálne obmedzenia. Nemožno ich považovať za dôveryhodný a plnohodnotný základ, a to ani čiastočne. Organizačné otázky súvisiace s dynamikou moci medzi aktérmi a privlastnením si používateľov, ako aj technické faktory totiž veľmi sťažujú štúdium skutočného rozsahu tejto technológie. Opätovne však zdôrazňujú, že samotná transparentnosť nemusí nevyhnutne znamenať úplnú dôveru a primeranú ochranu osobných údajov

Aké sú súčasné limity blockchainu?

- Na záver pripomeňme, že infraštruktúry verejných kľúčov (PKI) boli kedysi podobne prezentované ako revolučná technológia vzbudzujúca dôveru, kým sme začali chápať ich obmedzenia.
- Preto, a podobne ako v prípade označení v širšom zmysle, je použitie blockchainu zárukou určitých vlastností, ale malo by sa vnímať ako spôsob, ako vyzdvihnutím vhodných vlastností technológie vyvolať alebo naznačiť dôveru používateľov.

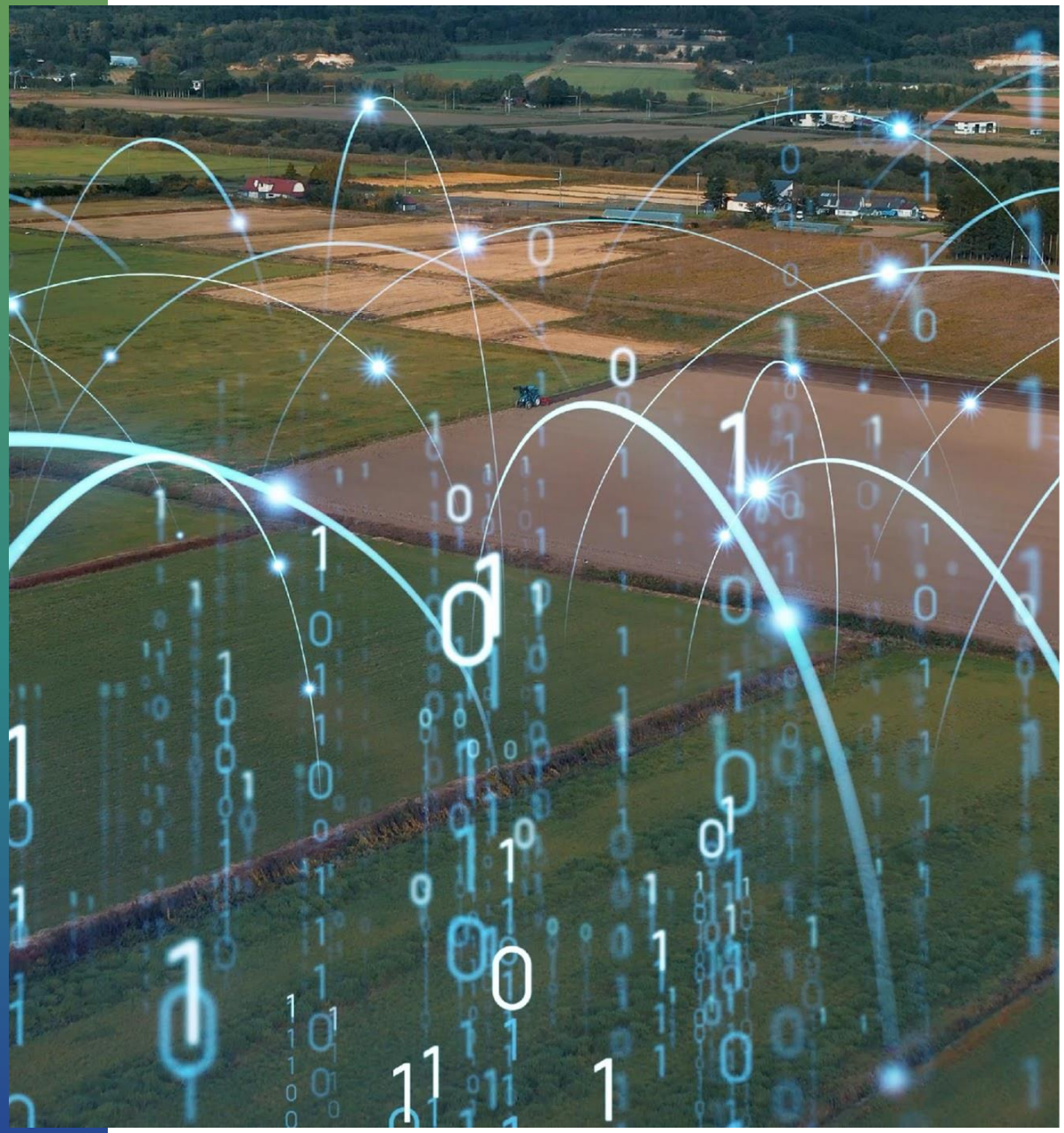
V ďalšom module sa naučíte

Kliknite na tlačidlo pre zadanie



V ďalšom module sa naučíte

Kliknite na tlačidlo pre zadanie



Literatúra

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 Úvod do špeciálneho čísla o nových perspektívach dôvery v informačných systémoch MIS Quarterly, 34 (2) (2010), s. 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), s. 880-918, 10.17705/1jais.00411

Söllner, M. (2015). Pochopenie dôvery v informačné systémy - vplyv dôvery v systém a v poskytovateľa. In *Zborník zo sedemdesiateho piateho výročného zasadnutia akadémie manažmentu.* AOM.

BLOCKCHAIN FOR AGRI FOOD EDU

Literatúra

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), s. 940-959

B. Reeves, C. Nass Mediálna rovnica: Ako ľudia zaobchádzajú s počítačmi televíziou a novými médiami ako so skutočnými ľuďmi a miestami, Cambridge University Press (1996)

Fussell, S. R., Kiesler, S., Setlock, L. D., & Yew, V. (2008). How people anthropomorphize robots. In *Zborník z tretej medzinárodnej konferencie ACM/IEEE o interakcii človeka s robotom* (s. 145-152). Association for Computing Machinery. Retrieved from

BLOCK CHAIN FOR AGRI FOOD EDU

https://blockchainforagrifood.eu/

Ďakujem

Priestor na otázky

Co-funded by the European Union

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie alebo Európskej výkonnej agentúry pre vzdelávanie a kultúru (EACEA). Európska únia ani EACEA za ne nepreberajú žiadnu zodpovednosť.