Blokklánc technológiák és alkalmazások - telekommunikációs példákkal

Dr. Kocsis Imre
adjunktus, BME MIT
kocsis.imre@vik.bme.hu
HTE Infokom 2021’

MŰEGYETEM 1782

Budapest University of Technology and Economics
Department of Measurement and Information Systems
ftsrg Research Group

ftsrg

Blockchain@FTSRG

- **2016 IBM Faculty Award** (Prof. Pataricza)
- **Linux Hyperledger Foundation: associate membership**
- **Hyperledger Caliper, Hyperledger Summer Mentorship-ek**

- *Blockchain technológiák és alkalmazások* BME kurzus
- European Institute of Technology (EIT) Professional School
- Budapest Institute of Banking

- https://inf.mit.bme.hu/en/research/projects/blockchain
- Imre Kocsis: **ISO/TC 307** nemzeti delegált

R&D tevékenységünk

Verifikáció & validáció

- HL Fabric teljesítményelemzés
- Okosszerződés hibainjektálás
- Okosszerződések formális vizsgálata

Metodológia

- Követelményvezérelt tervezés
- “Blokkláncosítás”
- Folyamatmigráció

Alkalmazások

- Kiberfizikai rendszerek
- Szervezetközi folyamatok
- Digitális jegybankpénz

Technológia

- Hyperledger Caliper
- Modell -> HL Fabric, DAML, …

“Konzorciális blokkláncok”

Blokklánc…?

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

Distributed Ledger Technology - DLT

Felhasználó
k

Konszenzus: sorrend, tranzakció-validitás, *főkönyv* (DB) hatás

Közös főkönyv-
nézet

A mindenki által tárolt “blokklánc”

Kriptográfiailag aláírt tranzakciók

Hálózati konszenzus: ***blokkonként***

Következő blokk része az előző kriptográfiai ujjlenyomata

Első: ***genezis blokk***

Nem csak “blokklánc” DLT-k léteznek – bár ma még a leggyakoribb

A tárolt eljárásaink: okosszerződések

- Főkönyv: van natív adatmodell
  - publikus kulcs -> “pénz”
  - ...

Alfőkönyv: chocolateID -> lecturerID

Req.: sender, chocolateID, receiver

IF

(request.signature1 = sender

request.signature2 = receiver

chocolateID.owner = sender

chocolateID.bestBefore > now + 1w)

THEN

receiver

Nem minden blokklánc technológiában: ~2013 Ethereum/Hyperledger Fabric
A “tokenek” okosszerződéssel megírt adható-vehető “tantuszok”
Amit megírhatunk benne: “digitális hűtőmágnes” ... befektetési közösség

Replikált, elosztott adatbázis – de milyen?

Részvétel a konszenzusban	Hozzáférés	Főkönyv adatmodellje	Konszenzus	Protokoll/SW	Hálózat	Metafora
Nem jogosultságkezelt	**Publikus**	Kriptopénz tulajdonjog - kulcshoz kötve (+alkalmazások)	Részvételt kriptopénzzel díjazza	Bitcoin, Ethereum, Doge, …	Nagyon nagy	*"Decentralizált közmű"*
Jogosultságkezelt	**Publikus**	~ / ~	Használatért kriptopénzben fizetünk	Ethereum, …	< 100 csomópont	*"(Iparági) közös platform"*
Jogosultságkezelt	**Szervezetek konzorciuma**	Alkalmazás-főkönyv	*Kriptopénz…?*	**Hyperledger**, Ethereum, R3 Corda, …	Akár 2 szervezet is	**B2B / org2org**

Publikus blokklánc vs konzorciális

Konszenzus – hogy születik a következő blokk?

- **UNPERMISSIONED:**
  - Egy számítógép nyers próbálgatással véletlenül “megtör” egy hash-t:
    - Bizonyíték (**Proof of**), hogy elég sok,
    - csak hasonlóan “nagy” hálózattal replikálható,
    - sikertelen próbálkozás (**Work**) történt;
    - ő adja a következő blokkot (és tulajdonosa kap kriptopénzt)

  - **Proof of Stake**: csomópont-üzemeltetők letétbe helyeznek kriptopénzt,
    - Kiválasztásra kerülhetnek blokkképzésre,
    - Vagy megerősítenek blokkokat,
    - Kapnak ezért kriptopénzt,
    - Ha rosszindulatú blokkot hoznak létre/erősítenek meg, a letét elveszik.
  - ...

- **PERMISSIONED:**
  - **Proof of Authority**: ismert felek képezhetnek blokkokat (“a reputációjukkal játszanak”)
  - **(Practical) Byzantine Fault Tolerance**: támadástűrő többségi szavazás
  - Egyszerű n:m tranzakció-**szavazás** + crash-fault-tolerant blokképzés

- A támadási modellek/biztonságossághoz szükséges “elégséges többség” más-más

Publikus világ: *még mindig* PoW és kriptoeszközök

DeFi, AMM, decentralized exchanges, Bitcoin ETF, NFTs, wrapped coins…
Miközben: a “nagy” láncokon 10+ dollár egy tranzakció és magas a késleltetés

Szervezetközi kooperáció: “single source of truth”

- Együttes bejegyzéskövetés
- Többszereplős konszenzus
- Független validáció
- Hamisítás: evidens
- Hamisítással szemben ellenálló

Célszoftverek: Hyperledger Foundation (Linux Foundation)
Párhuzam: hiperkonvergens gazdaság és ipar

Egy tipikus Hyperledger Fabric hálózat

Az alkalmazások megérkeztek

https://www.hyperledger.org/learn/case-studies
Telecom SIG: https://wiki.hyperledger.org/display/TCSIG
Közszféra: EBSI használati esetek!

“Vállalati blokklánc” – üzleti érték

Egy kollaboratív gyártási példa – NIST AMS 300-10

Vásárló

- 3D nyomtattatni akar
- Egy köztes szolgáltatón keresztül

Gyártásszolgáltató

- Delegál a gyártók felé

Gyár

- 3D modellek alapján gyárt
- Részletes minőségellenőrzési riportot készít

Recommendations on Ensuring Traceability and Trustworthiness of Manufacturing-Related Data, https://doi.org/10.6028/NIST.AMS.300-10

On-chain *dokumentum* & *modell* munkafolyamatok

Kollaboratív gyártás – egy prototípus

- Integritásellenőrzés
- Hozzáférésadás
- Gyártási terv megosztása
- Minőségellenőrzés

- Integritásellenőrzés
- Gyártási terv validáció
- Minőségell. riport

Manufacturing Service App

Factory App

- Modelltulajdon deklarálása
- Hozzáférés adása

Hyperledger Fabric DLT

A DLT-alapú kooperatív Digitális Ikrek felé

Volkswagen: odometer csaláselkerülés

Deutsche Energie-Agentur: regiszter virtuális állomások és frekvencia-szabályozás támogatására

DB Systel: Decentralizált vonatbefolyásolás és -menesztés

A titkos(?) szósz:
garanciákat vállaló & intelligens kommunikációs hálózat

Blokklánc és telekom (szállító-függetlenül)

Blokklánc az 5G alkalmazásaiban

- Okos város, villamosirányítás (klasszikus és P2P), szállítmányozás, autonóm járművek, szenzoradat-piacterek…

5G szolgáltatások támogatása

- Federált tanulás, biztonság és privacy, erőforráskezelés, …

5G-t lehetővé tevő technológiák

- Mobil edge computing koordinációja, hálózati szeletek koordinált létrehozása, …
- UE/IoT eszközök identitásellenőrzésének bizalmi relációi

Klasszikus kooperációk

- Roaming menedzsment, data clearing, elszámolás

Lásd pl.: Nguyen, Dinh C., et al. "Blockchain for 5G and beyond networks: A state of the art survey." *Journal of Network and Computer Applications* 166 (2020): 102693.

Ha rendszerelem – szisztematikus tervezés kell

- **A konzorciális DLT-k ehhez már elég érettek**
- Pl. ISO/IEC 25000:2014 alapján
- **Konzorciális DLT-t tartjuk csak igazán kézben**

- **Teljesítmény** – erőforrások, konfig.?
- **Megbízhatóság -** okos szerződés kód?
- **Funkc. helyesség** – modellből kód?
- **Karbantarthatóság**
- **Privacy és titkosság**
- …

Source: E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, New York, NY, USA, 2018, pp. 30:1–30:15, doi: 10.1145/3190508.3190538.

Késleltetés: a TPC-C “warehousing” benchmark egy portja

Setups	New Order Transaction latencies (milliseconds)			
	Min	Average	90th perc.	Max
In-memory, centralized	102	**104**	**105**	495
Decentralized cluster	103	**127**	**160**	*5555*
Hyperledger Fabric	76	**316**	**387**	1238

Ellenállóképesség vizsgálata – injektált kódhibákkal

FIGURE 10. Fault detection in *protected contracts* without formal verification.

FIGURE 11. Fault detection in *protected contracts* with formal verification.

Nincs ingyenebéd (sőt): tesztelés, formális V&V, platform-védelmek, “tudatos kliens”

Hajdu, Á., Ivaki, N., Kocsis, I., Klenik, A., Gönczy. L., Laranjeiro, N. Madeira, H. & Pataricza, A. (2020): Using Fault Injection to Assess Blockchain Systems in Presence of Faulty Smart Contracts. *IEEE Access*, Early Access, DOI: 10.1109/ACCESS.2020.3032239, IEEE.

Komplex együttműködések – modellből kód!

P. Garamvölgyi, I. Kocsis, B. Gehl, and A. Klenik, "Towards Model-Driven Engineering of Smart Contracts for Cyber-Physical Systems," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, Jun. 2018, pp. 134–139, doi: 10.1109/DSN-W.2018.00052.

Közeljövő 1: integráció és “layer 2” megoldások

- “Internet of blockchains”?
  - Cél-blokkláncok robusztus összekötése
  - Centralizált megoldásoktól… (Hyperledger Cactus)
  - … a “blokkláncok blokkláncáig” (Polkadot)

- Layer 2: 4000+ TPS Ethereum mainneten. Ma.
  - Persze +1 “rollup” réteggel
  - És sokszor “moonshot” matematikával

Közeljövő 2: digitális jegybankpénz (CBDC)

- Blokklánc: “a hiányzó dollár problémája”
- CBDC: nem feltétlenül lesz DLT alapú; de ha az okosszerződések végre ***pénzt használhatnak…***

https://cbdctracker.org/

Közeljövő 3: decentralizált identitások

- Self-Sovereign Identity, Decentralized Identity, …
- Teljes szabvány-stack – W3C
- Technológia: Hyperledger Indy, Ursa
- Hálózatok: Sovrin, IDUnion, **EBSI**

"18+ éves, magyar állampolgár vagyok, min. 2 oltással."