Neštandardné využitia technológie blokových reťazcov

Riešiteľ: Bc. Matúš Revický

Vedúci práce: doc. RNDr. Jozef Jirásek, PhD.

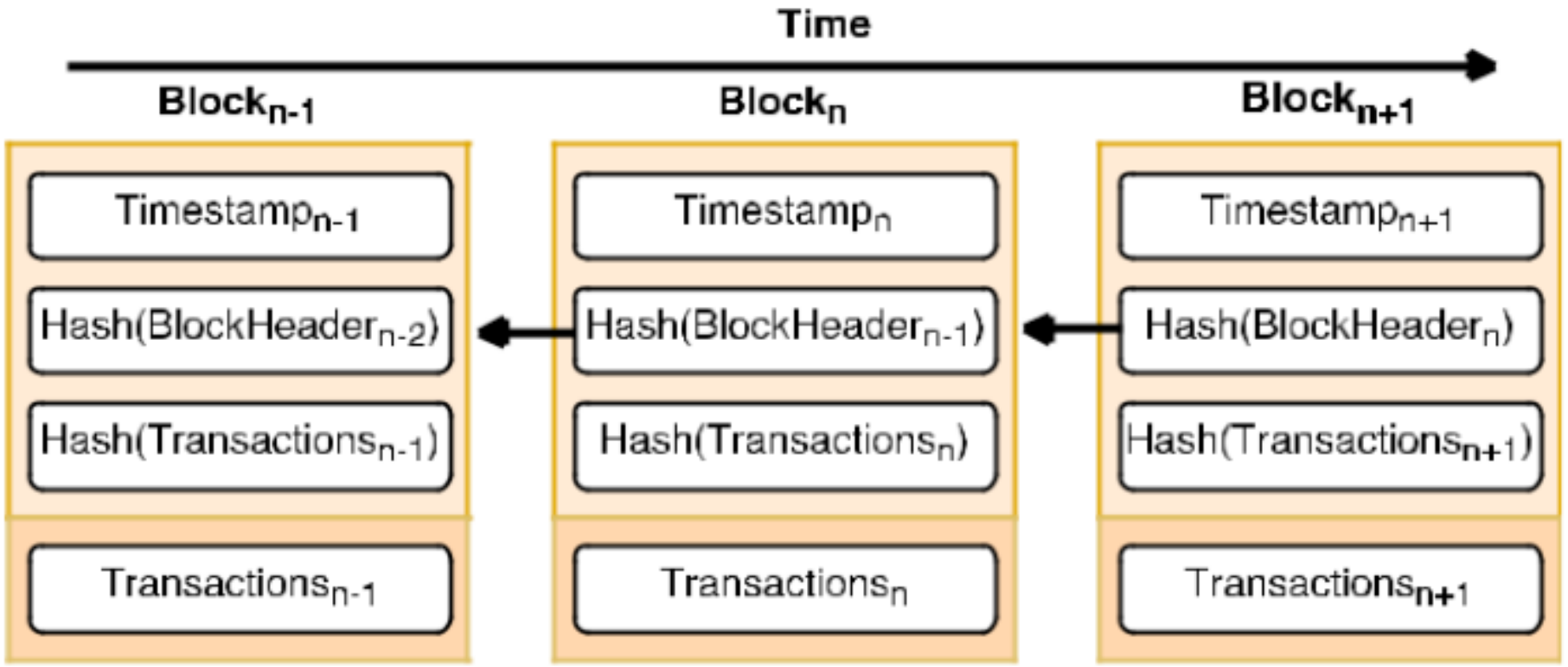
Ciele a motivácia

Prehľadne a dôsledne popísať mechanizmus blokových reťazcov v realizácii kryptomien.

Zvážiť možnosti využitia týchto techník na zabezpečenie distribuovanej dôvery v prostredí IoT.

Navrhnúť konkrétnu implementáciu vo zvolenej oblasti.

Blockchain



Timestamp$_n$: Timestamp of block *n*

Transactions$_n$: All transactions in block *n*

Hash(x) : Hash function, *sha256(sha256(x))* for Bitcoin

Blockchain

Consensus algorithm/ blockchains	Number of transactions per second	Confirmation latency	Features
Proof-of-Work (PoW)/ Bitcoin, Ethereum	Tens	6–60 min	High security Low throughput Low scalability
Proof-of-Stake (PoS)/ Peercoin	Tens	10–60 min	High security Low throughput Low scalability
Byzantine fault tolerance (BFT)/Hyperledger	Thousands	1–60 s	Low security High throughput High scalability
Delegated Proof-of-Stake (DPoS)/EOS	Thousands	<1 s	Low security High throughput High scalability
Proof-of-Formulation (PoF)/FLETA	More than 10,000	<1 s	High security High throughput High scalability

Cryptographic Digital Signature:

- Kryptografia verejného kľúča
- Vytvorenie transakcie súkromným kľúčom

Distributed Ledger:

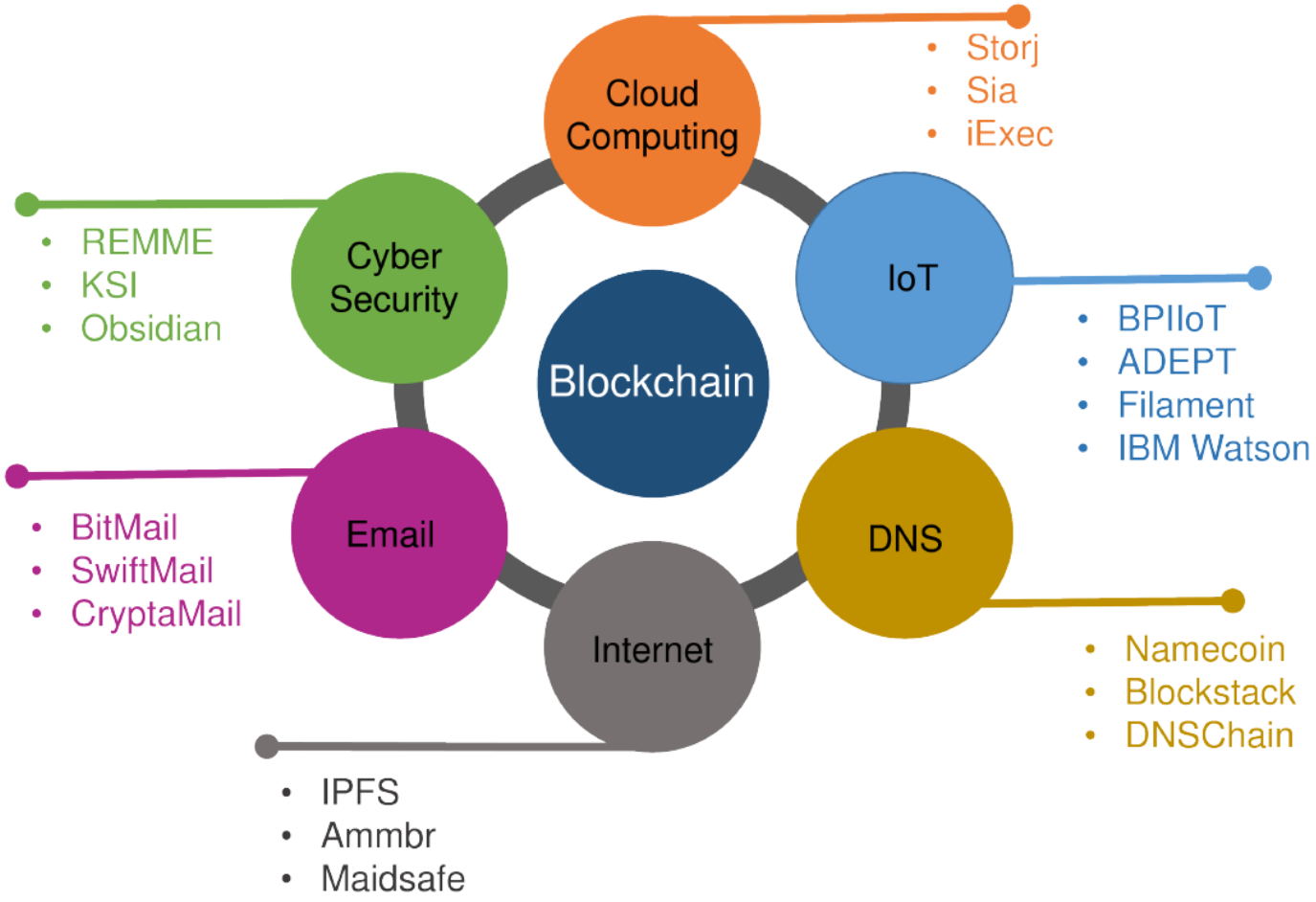
- Uloženie transakcii
- Používa konsenzusové algoritmy
- Nemenné

Consensus algorithm:

- Žiadna centrálna autorita
- P2P Model

Výzvy v oblasti IoT

- Obmedzené zdroje
- Požiadavky na šírku pásma
- Transakčné poplatky
- Latencia
- ...



Analýza dostupných riešení

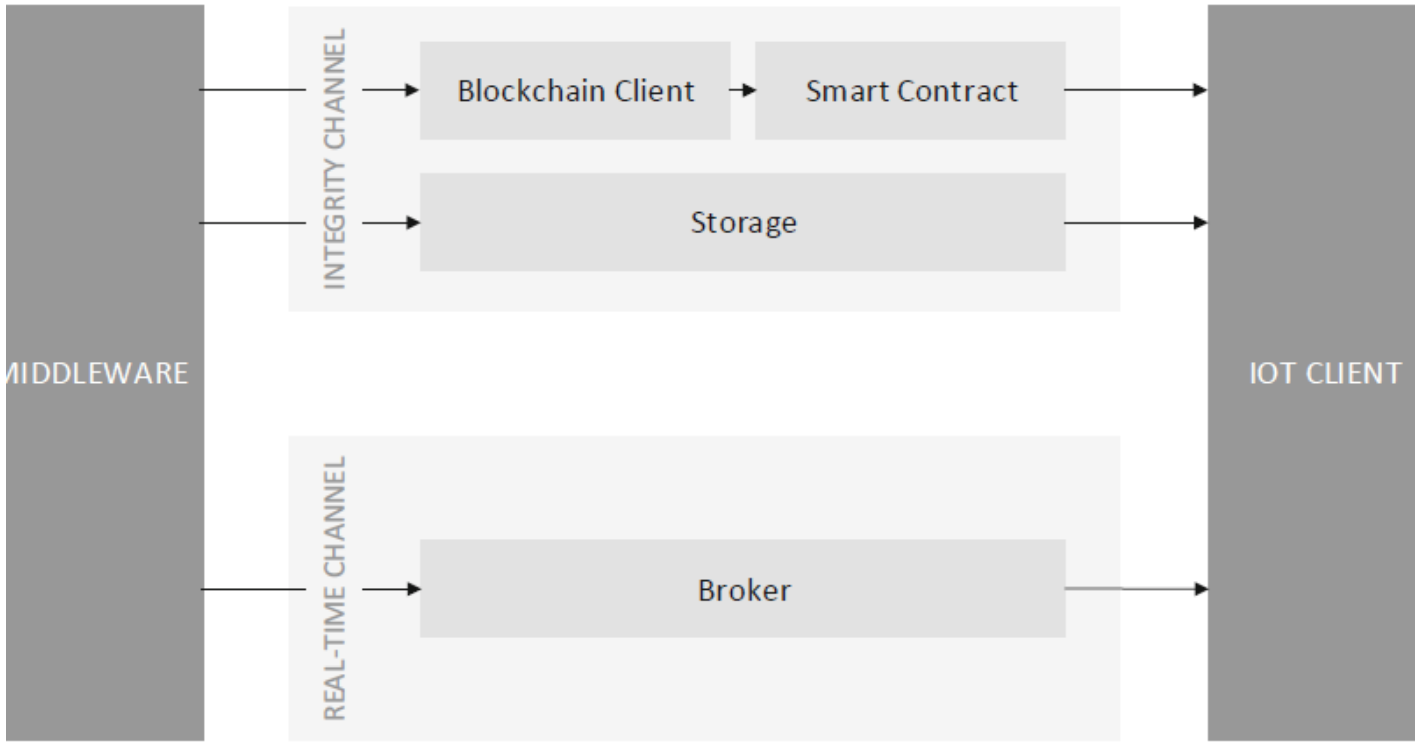


Fig. 1. Architecture overview

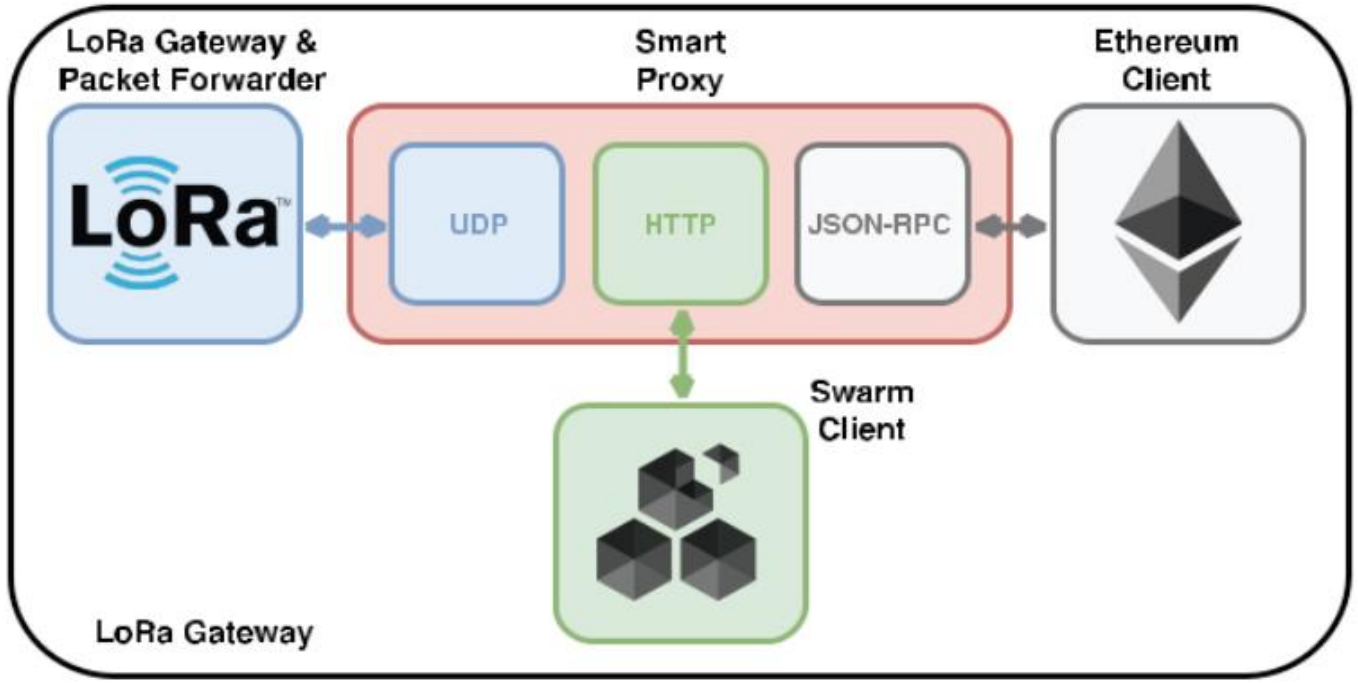
IPFS-Based Data Distribution for the IoT

(Simon Krejci, Marten Sigwart, and Stefan Schulte)

- Middleware, ktorý sa pripája k zariadeniam IoT a využíva blockchain na distribúciu dát IoT s garanciou integrity.
- Middleware ponúka, distribuované dáta v reálnom čase cez druhý kanál.
- Implementácia pomocou blockchainu Ethereum a systému InterPlanetary File System (IPFS).

https://link.springer.com/chapter/10.1007%2F978-3-030-44769-4_14 str. 177-191

Analýza dostupných riešení



Designing a blockchain-based IoT infrastructure with Ethereum, Swarm and LoRa (Kazım Rıfat Özyılmaz Arda Yurdakul)

- Úložisko Swarm
- Sieťová technológia LoRa
- Blockchainová platforma Ethereum
- Neefektívnosť

Zdroje

1. R. Wattenhofer: The Science of the Blockchain, CreateSpace IndependentPublishing Platform, 2016, ISBN-13: 978-1522751830

2. M. Swan: Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015, ISBN-13: 978-1491920497

3. D. Tapscott , A. Tapscott : Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Portfolio, 2016,ISBN-13: 978-1101980132

4. Chris Dannen: Introducing Ethereum and Solidity; Foundations of Cryptocurrency and Blockchain Programming for Beginners, Apress, Berkeley, 2017, ISBN 978-1-4842-2534-9, https://doi.org/10.1007/978-1-4842-2535-6

5. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, A Survey onthe security of blockchain systems, In Future Generation Computer Systems, 2017 , ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.08.020.

6. Steve Huckle, Rituparna Bhattacharya, Martin White, Natalia Beloff, Internet of Things, Blockchain and Shared Economy Applications, In Procedia Computer Science, Volume 98, 2016, Pages 461-466, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2016.09.074.

Ďakujem za pozornosť