Managing Private Information through Use of A Blockchain Network

Casey Clark

Faculty Advisor: Dr. John Marsh

SUNY POLYTECHNIC INSTITUTE
COLLEGE OF ENGINEERING

BACKGROUND

What is a blockchain?

- Decentralized and public ledger
- Each network node has a copy of the blockchain or pubic ledger
- Public ledger contains history of transactions
- Each block contains a timestamp & link to previous block[7]

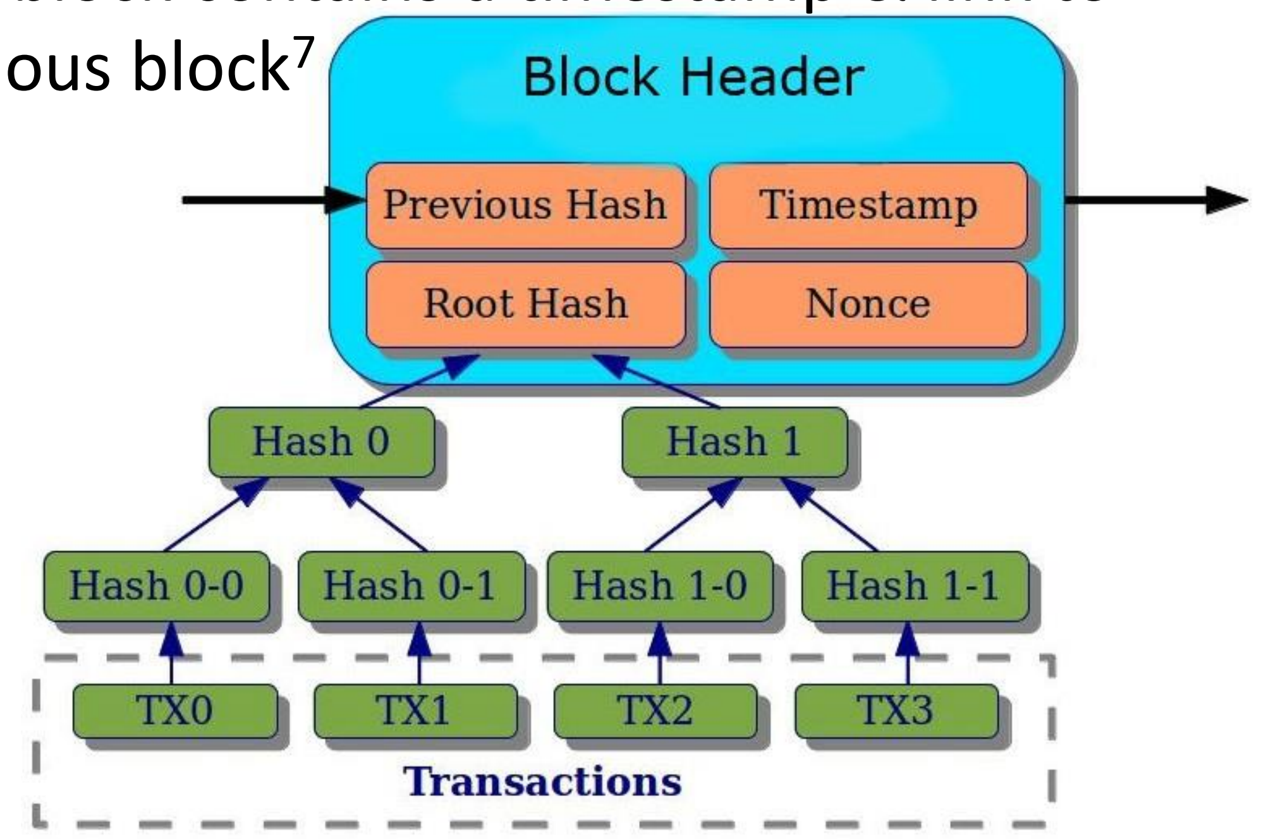

Figure 1.0 – Contents of a single FULL block[1]

Well Known for use in Bitcoin

- Transactions disputes between parties can be easily resolved
- Bitcoin transactions are hashed with other transactions to created a root hash[7]
- Bitcoins rewarded for solving computational hashes that calculate the nonce[7]

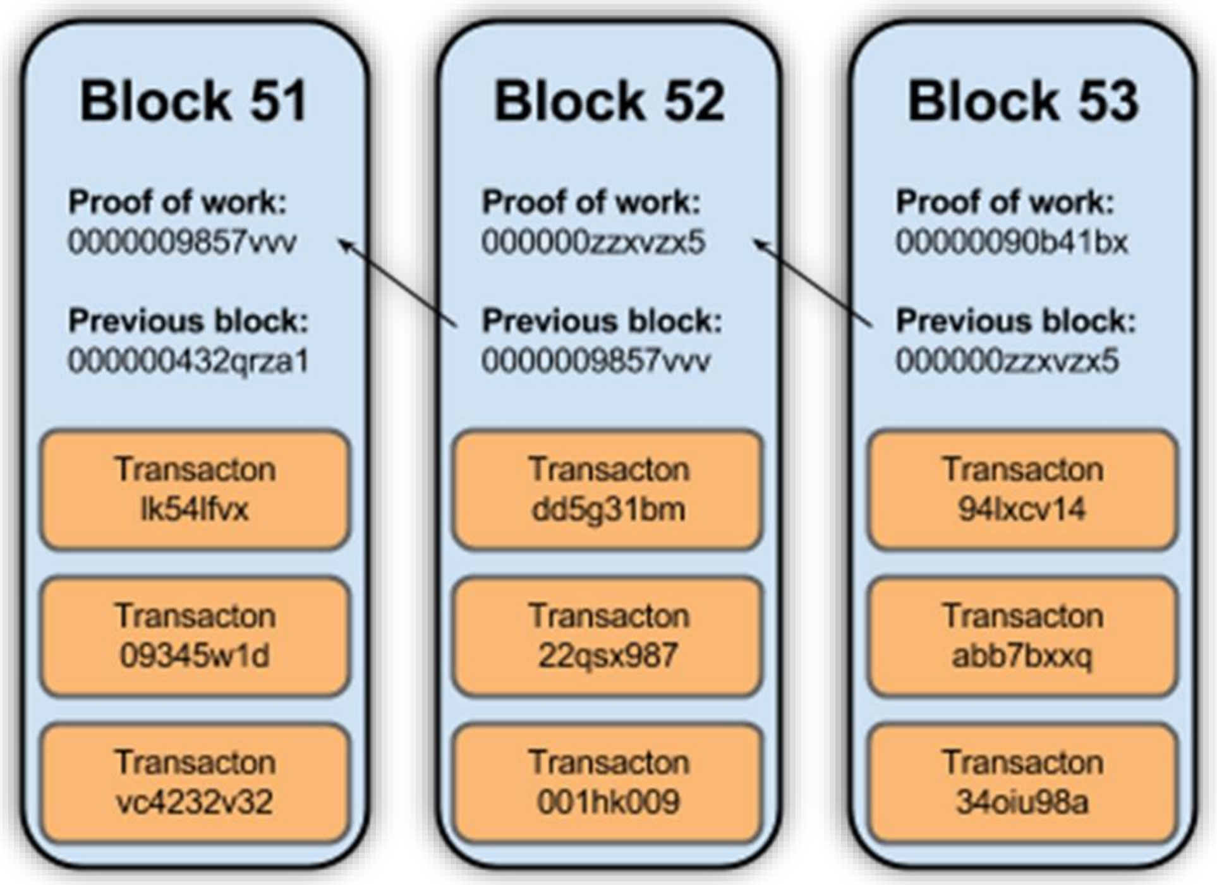

Figure 1.1 – Contents of several linked blocks[2]

Has the success of Bitcoin overshadowed uses for the revolutionary system that made it successful?

RESEARCH & APPLICATION

Supply Chain Management and Auditing[5]

- IoT devices capture detailed data for the origin of a product
- Blockchain has potential to offer secure and undeniable access to supply chain data
- Indisputable origin of each individual material can be established

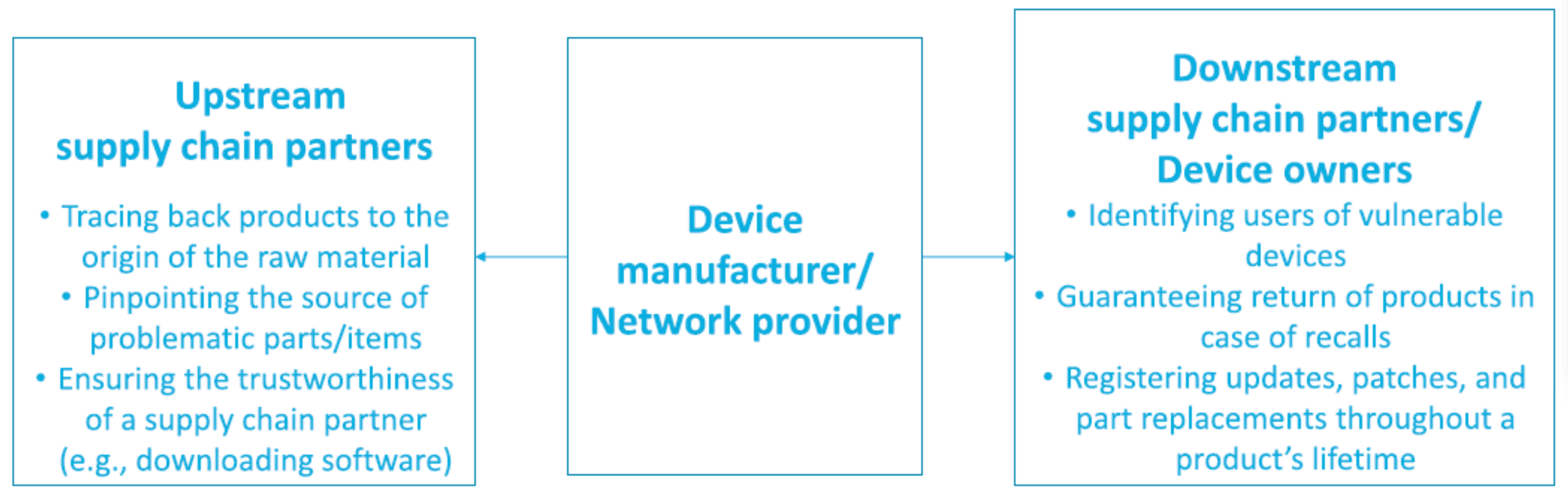
Upstream supply chain partners
• Tracing back products to the origin of the raw material
• Pinpointing the source of problematic parts/items
• Ensuring the trustworthiness of a supply chain partner (e.g., downloading software)
Device manufacturer/ Network provider
Downstream supply chain partners/ Device owners
• Identifying users of vulnerable devices
• Guaranteeing return of products in case of recalls
• Registering updates, patches, and part replacements throughout a product's lifetime

Figure 1.2 – Supply chain management[4]

Challenge of cloud-based platforms[4]	Potential solutions implemented by a blockchain[4]
Cost & capacity constraints to handle growing IoT platforms	• No centralized "entity" storing the data. • Exchange of information occurs through smart contracts.
Architecture constraints	• Authentication occurs through cryptography keys • Information ONLY comes from originator.
Downtime and unavailable services	• No single point of failure if data is stored in blockchain. • Records are stored IN the blockchain.
Vulnerabilities to attacks	• Devices are interlocked. • If one blockchain is breached, the network rejects it.

Figure 1.3 – Blockchain can solve many problems of current "cloud-based IoT" based on ideas from Kshteri (2017)[4]

Blockchain in IoT devices

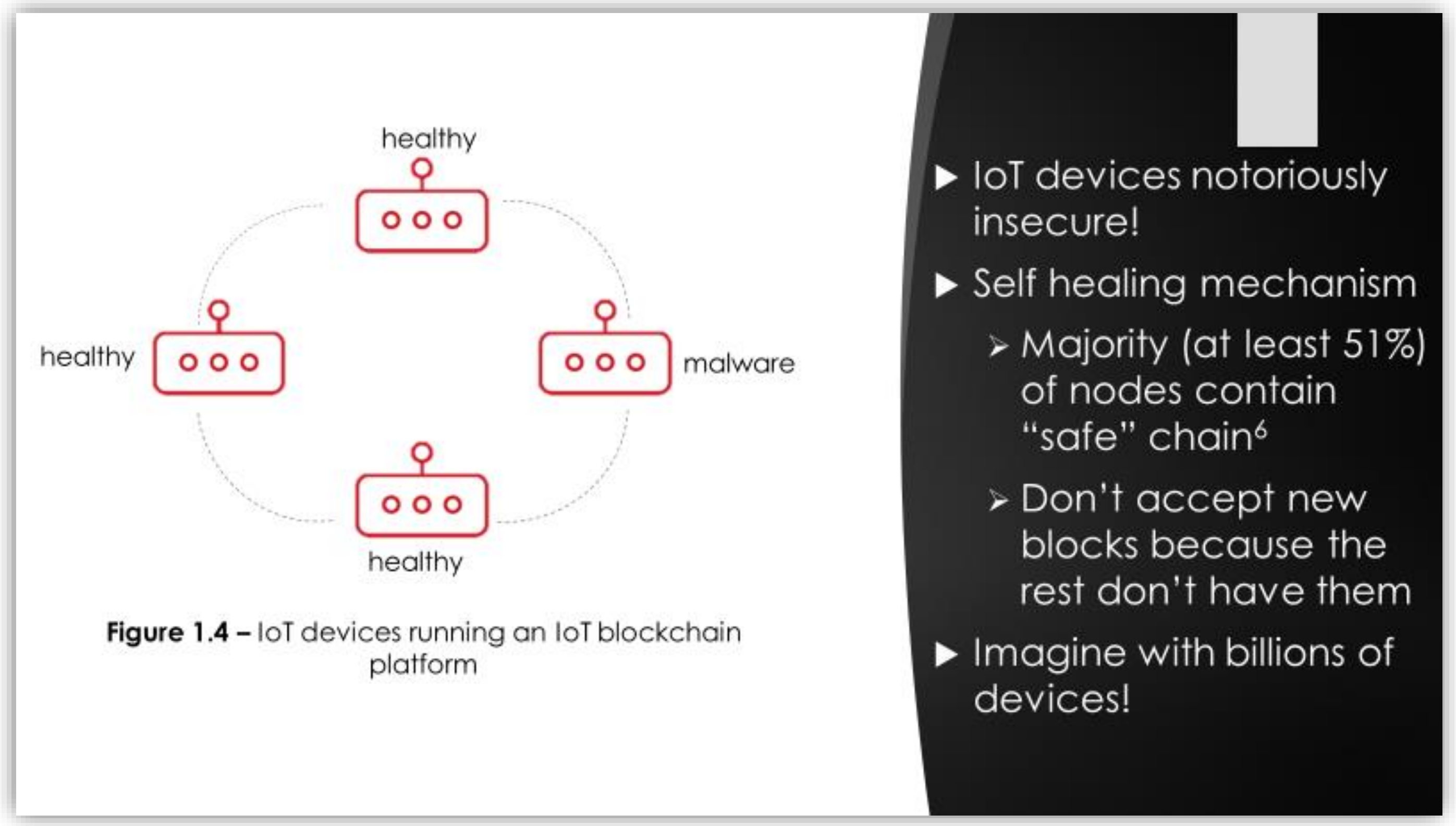

Figure 1.4 – IoT devices running an IoT blockchain platform

- IoT devices notoriously insecure!
- Self healing mechanism
  - Majority (at least 51%) of nodes contain "safe" chain[6]
  - Don't accept new blocks because the rest don't have them
- Imagine with billions of devices!

Data Storage in a Blockchain Network[3]

- **Figure 1.5** displays an example of a system that is used to store a patient's medical records
- 3 requirements to access stored in 3 different locations
- Data stored off the blockchain
- Blockchain used for authentication and auditing of the transaction

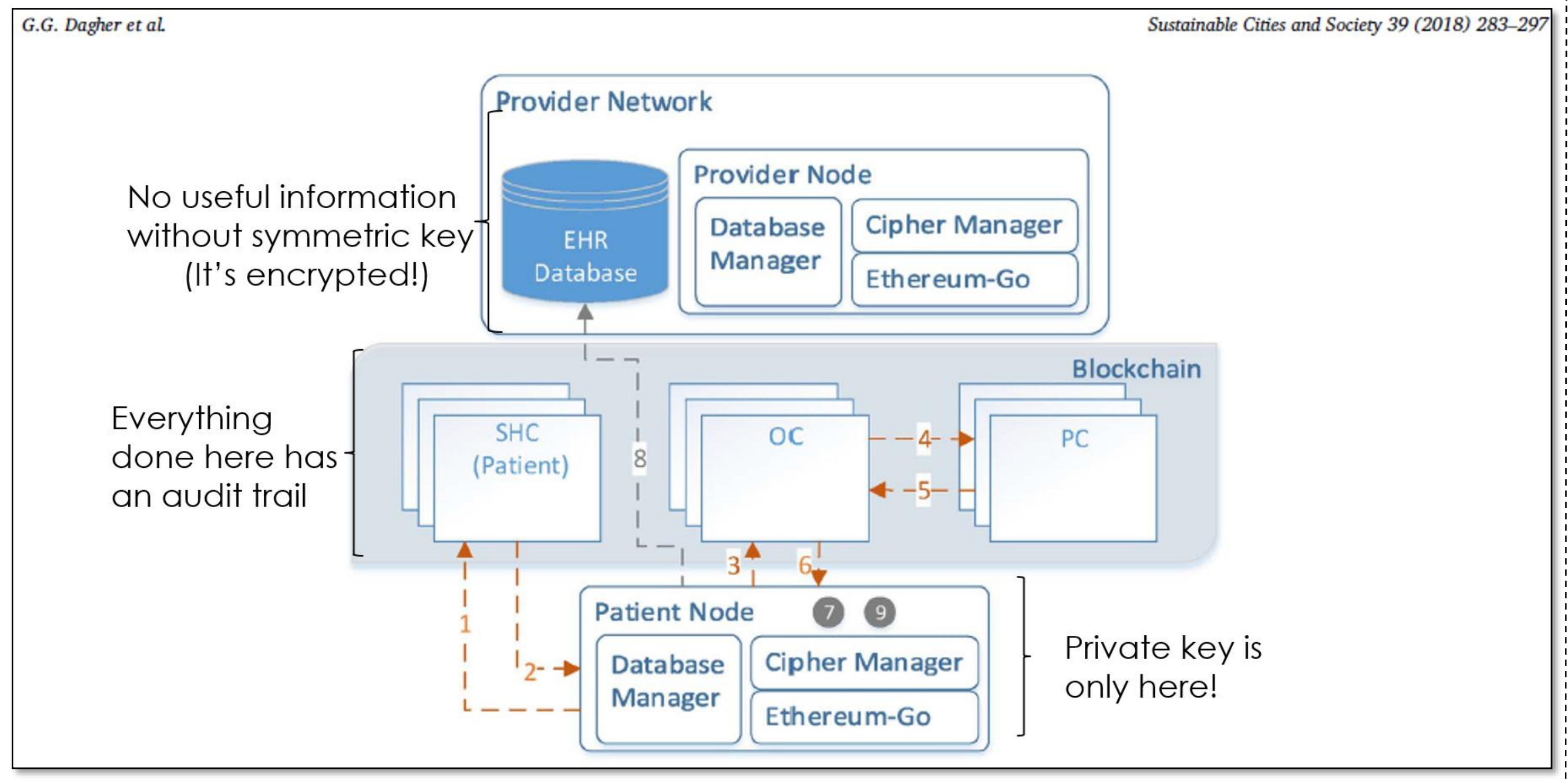
G.G. Dagher et al. Sustainable Cities and Society 39 (2018) 283–297

Figure 1.5 – Storing significant data off the blockchain[3]

- Complete data doesn't have to be stored on the blockchain
- Stored completely through use of "full nodes"
- Light nodes only store block header
- Only necessary to store hash of data
- Hash can verify that data has NOT changed

CONCLUSION

Traditional model[4]	Blockchain model[4]
Service providers (e.g. Facebook) can use private information for purposes consumer does not expect	Private information is controlled through private and public keys
No guaranteed protection for personal identifiable information that may be disclosed	Owner has control over information that is released
Users are not aware of data being stored	"Smart contracts" ensure consumers transactions are carried out
Lack of audit trail which means lack of accountability	Audit trail is included in blockchain ledger

Figure 1.6 – Blockchain model promotes privacy and security compared to a non-blockchain model[4]

REFERENCES

1. https://computersecuritypgp.blogspot.com/2016/05/what-is-blockchain.html
2. https://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/
3. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283-297.
4. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027-1038.
5. Kim, H. M., & Laskowski, M. (2016). Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance. *SSRN Electronic Journal*. doi:10.2139/ssrn.2828369
6. Xage Security. (2017, December). Decentralized and Adaptive Security for the new Industrial Edge. http://xage.com
7. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.