A Review on the Use of Blockchain for the Internet of Things

Presented by
Jeong hun Cha

OUTLINE

1. Introduction
2. Blockchain
3. Blockchain-based Internet of Things(BIoT)
4. Architecture
5. Cryptographic Algorithms
6. Consensus Mechanisms
7. Protocol Stack
8. Current Challenges for BIoT Aplications
9. Further Challenges and Recommendations
10. Conclusions
11. Opinion

1. Introduction

- The Internet of Things (IoT) is expanding at a fast pace and some reports [1] predict that IoT devices will grow to 26 billions by 2020, which are 30 times the estimated number of devices deployed in 2009.

- it is necessary to build an IoT stack, standardize protocols and create the proper layers for an architecture that will provide services to IoT devices. Currently, most IoT solutions rely on the centralized server-client paradigm, connecting to cloud servers through the Internet.

- Blockchain technologies are able to track, coordinate, carry out transactions and store information from a large amount of devices, enabling the creation of applications that require no centralized cloud.

1. Introduction

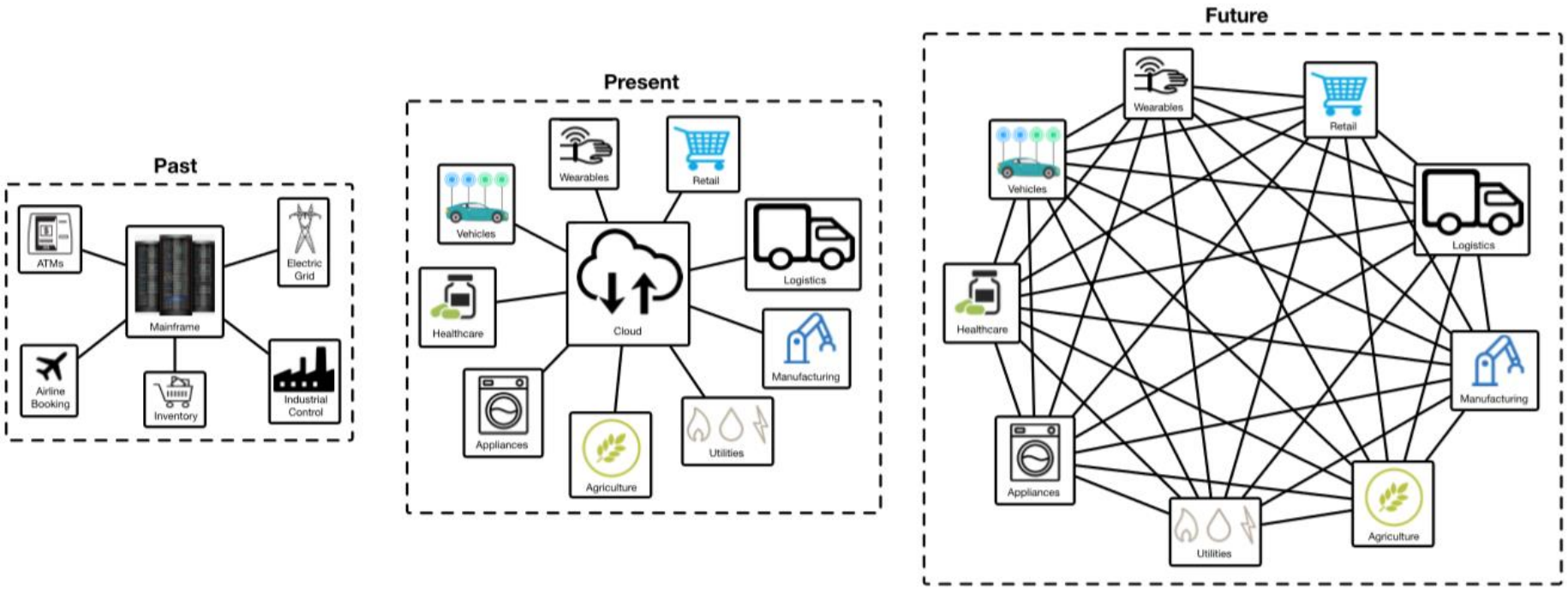

FIGURE 1. Past, present and future IoT architectures.

SEOULTECH

1. Introduction

- Many IoT solutions are still expensive due to costs. Related to the deployment and maintenance of centralized clouds and server farms.
- Maintenance is also a problem when having to distribute regular software updates to millions of smart devices.
- Lack of trust is also fostered by closed-source code. To increase trust and security, transparency is essential, so open-source approaches should be taken into account when developing the next generation of IoT solutions
- the key contribution of blockchain is that it provides a way to carry out transactions with another person or entity without having to rely on third-parties

SEOULTECH

2. Blockchain

- A blockchain is like a distributed ledger whose data are shared among a network of peers

- As it was previously mentioned, it is considered as the main contribution of Bitcoin, since it solved a longer-lasting financial problem known as the double-spend problem

- The solution proposed by Bitcoin consisted in looking for the consensus of most mining nodes, who append the valid transactions to the blockchain. Although the concept of blockchain was originated as a tool for a cryptocurrency, it is not necessary to develop a cryptocurrency to use a blockchain and build decentralized applications

- A blockchain, as its name implies, is a chain of timestamped blocks that are linked by cryptographic hashes

2. Blockchain

- In order to use a blockchain, it is first required to create a P2P network with all the nodes interested in making use of such a blockchain

- Every node of the network receives two keys: a public key, which is used by the other users for encrypting the messages sent to a node, and a private key, which allows a node to read such messages

- the private key is used for signing blockchain transactions (i.e., to approve such transactions), while the public key works like a unique address. Only the user with the proper private key is able to decrypt the messages encrypted with the corresponding public key

2. Blockchain

- When a node carries out a transaction, it signs it and then broadcasts it to its one-hop peers.
- The fact of signing the transaction in a unique way (using the private key) enables authenticating it (only the user with a specific private key can sign it) and guarantees
- As the peers of the node that broadcasts the transaction receive the signed transaction, they verify that it is valid before retransmitting
- it to other peers, thus, contributing to its spread through the network. The transactions disseminated in this way and that are considered valid by the network are ordered and packed into a timestamped block by special nodes called miners. The election of the miners and the data included into the block depend on a consensus algorithm

3. Blockchain-based Internet of Things(BIoT)

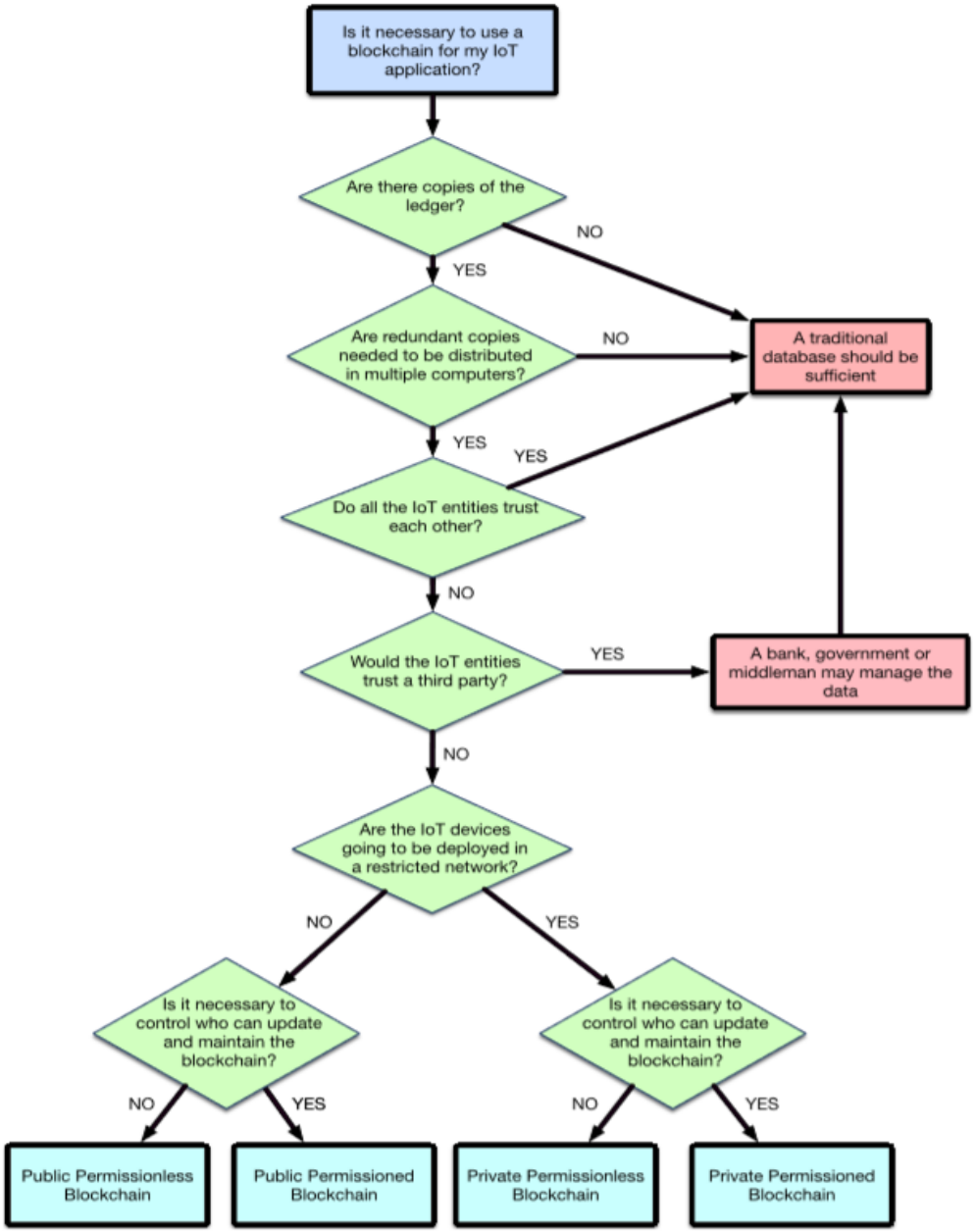

FIGURE 3. Flow diagram for deciding when to use blockchain in an IoT application.

SEOULTECH

3. Blockchain-based Internet of Things(BIoT)

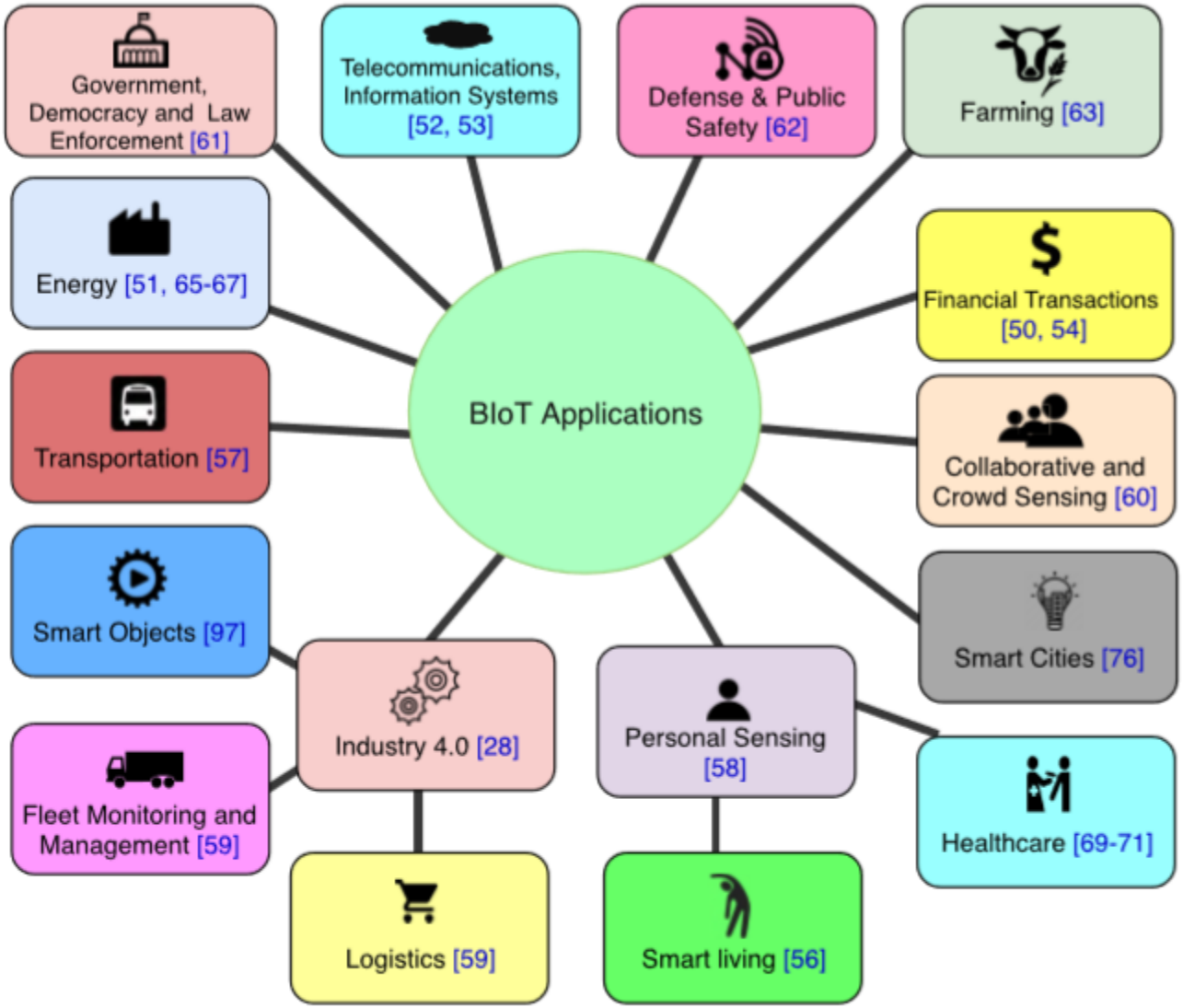

FIGURE 4. BIoT applications.

SEOULTECH

4. Architecture

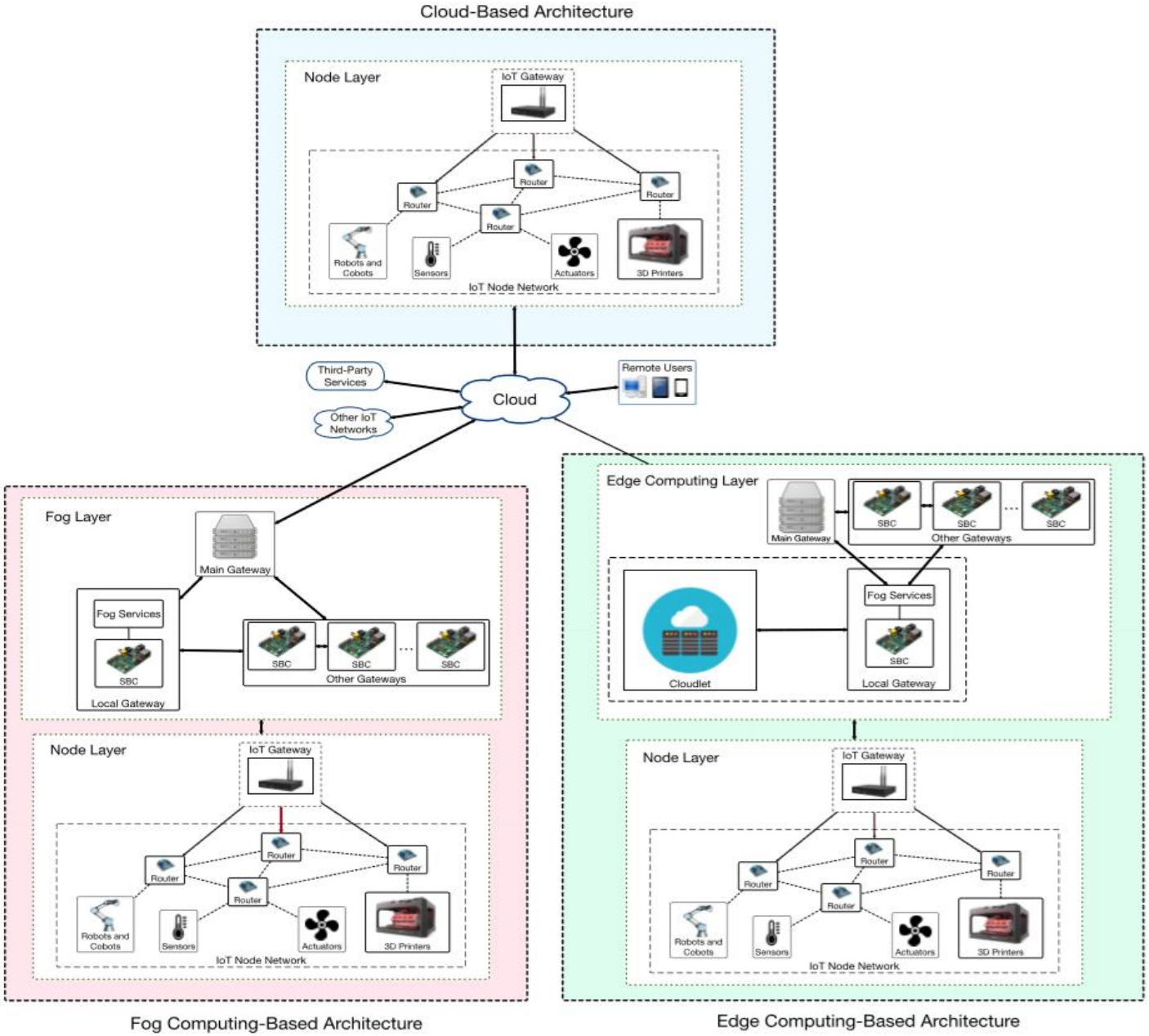

FIGURE 5. Traditional IoT architecture evolution.

SEOULTECH

5. Cryptographic Algorithms

- Public-key cryptography is essential for providing security and privacy in a blockchain. However, resource-constraint IoT devices struggle with the computing requirements of modern secure cryptographic schemes

- Specifically, asymmetric cryptography based on Rivest–Shamir–Adleman (RSA) is slow and power consuming when implemented on IoT devices [41]. Therefore, when choosing the right cryptographic scheme, it should be taken into account not only the computational load and the memory requirements, but also the energy consumed

- In contrast, Elliptic Curve Cryptography (ECC) represents a much lighter alternative to RSA . It has already been shown that, when implemented on resourceconstrained devices, ECC outperforms RSA in terms of speed and power consumption .

SEOULTECH

5. Cryptographic Algorithms

- Therefore, hash functions for IoT applications have to be secure (i.e., they should not generate collisions), fast and should consume the smallest possible amount of energy.

- The most popular blockchain hash functions are SHA-256d (used by Bitcoin) and SHA-256 (used by Swiftcoin). However, researchers that evaluated the footprint and energy requirements of SHA-256 in ASICs, concluded that, for low-power secure communications, it is more efficient to make use of Advanced Encryption Standard (AES).

- Due to such power limitations, other researchers suggested using ciphers like Simon, but further research and empirical evaluations on real BIoT applications are still needed.

6. Consensus Mechanisms

- Consensus is key for the proper functioning of a blockchain. It basically consists in a mechanism that determines the conditions to be reached in order to conclude that an agreement has been reached regarding the validations of the blocks to be added to the blockchain

- In the case of the Bitcoin blockchain, mining consists in finding a random number (called nonce) that will make the SHA-256 hash of the block header to have at the beginning certain number of zeros (Proof of Work: PoS)

- this mining process makes the blockchain inefficient in throughput, scalability, and in terms of energy consumption, what is not desirable in an IoT network.

6. Consensus Mechanisms

- Proof-of-Stake (PoS) is a consensus mechanism that requires less computational power than PoW, so it consumes less energy. Since this scheme seems unfair, because the wealthiest participants are the ones ruling the blockchain, other variants have been proposed

- Delegated Proof-of-Stake (DPoS) is similar to PoS, but stakeholders instead of being the ones generating and validating blocks, they select certain delegates to do it. Since less nodes are involved in block validation, transactions are performed faster than with other schemes.

- PBFT is a consensus algorithm that solves the Byzantine Generals Problem for asynchronous environments. PBFT assumes that less than a third of the nodes are malicious. For every block to be added to the chain, a leader is selected to be in charge of ordering the transaction. Such a selection has to be supported by at least 2/3 of the all nodes, which have to be known by the network.

6. Consensus Mechanisms

- Delegated BFT (DBFT) is a variant of BFT where, in a similar way to DPOS, some specific nodes are voted to be the ones generating and validating blocks.

- Stellar Consensus Protocol (SCP) is a implementation of a consensus method called Federated Byzantine Agreement (FBA). It is similar to PBFT but, whilst in PBFT every node queries all the other nodes and waits for the majority to agree, in SCP the nodes only wait for a subset of the participants that they consider important.

- Proof-of-Personhood (PoP) [143] is a consensus mechanism that makes use of ring signatures [144] and collective signing [145] to bind physical to virtual identities in a way that anonymity is preserved. A very similar concept is Proof-of-Individuality (PoI), which is currently being developed on Ethereum by the PoI Project.

7. Protocol Stack

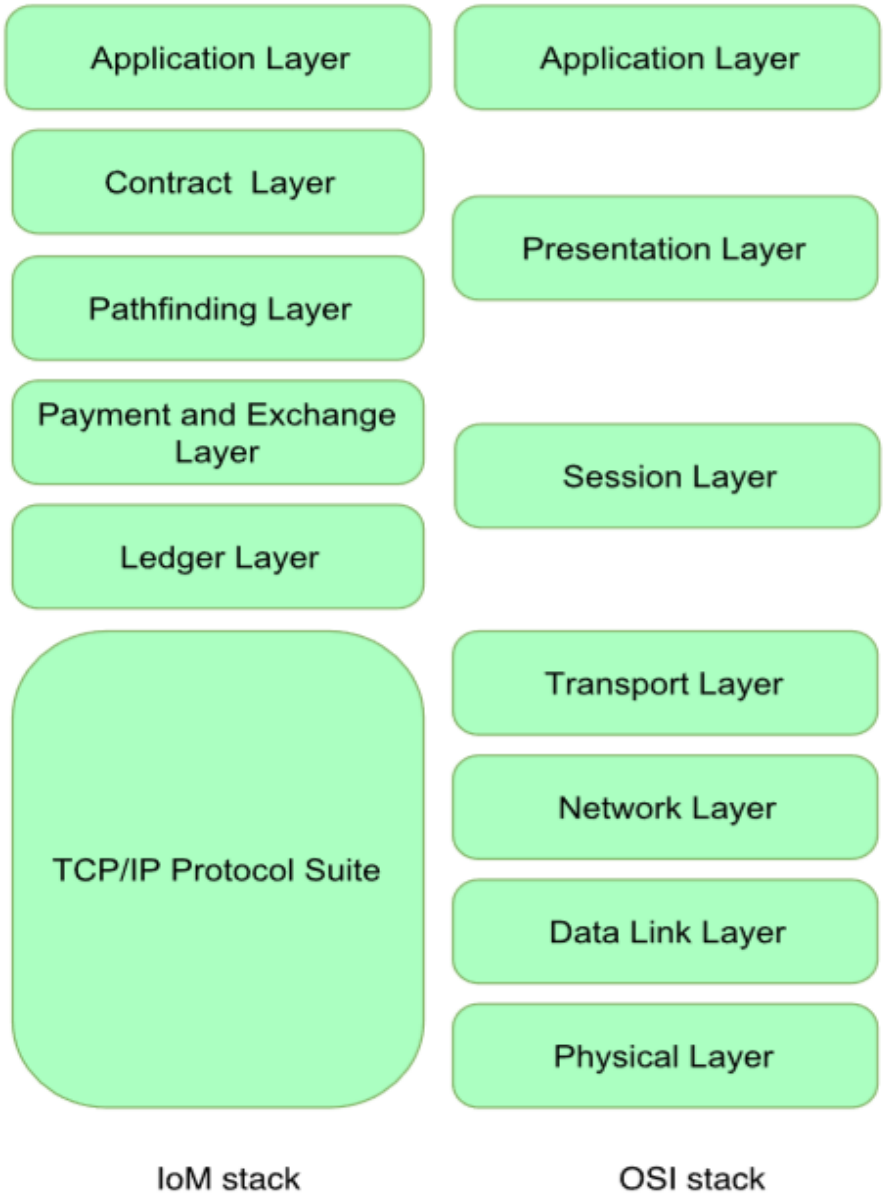

FIGURE 6. IoM versus traditional OSI protocol stack.

SEOULTECH

8. Current Challenges for BIoT Aplications

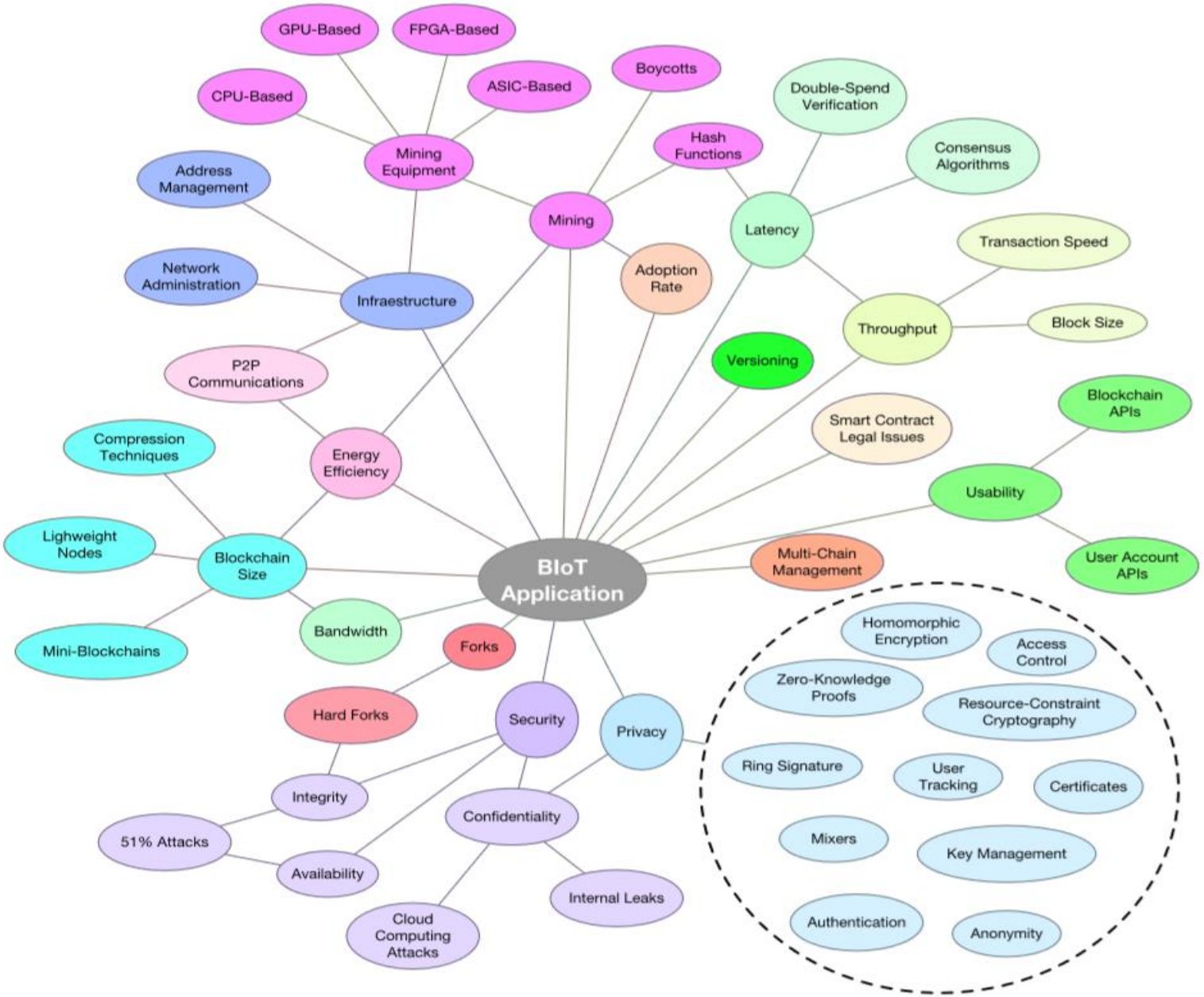

FIGURE 7. Most relevant factors that condition the development of a BIoT application and their main relationships.

SEOULTECH

8. Current Challenges for BIoT Aplications

A. Privacy

- All the users of a blockchain are identified by their public key or its hash. This means that anonymity is not guaranteed and, since all transactions are shared, it is possible for third-parties to analyze such transactions and infer the actual identities of the participants.

- Privacy can also be increased through zero-knowledge proving techniques like the ones used by Zerocoin, Zerocash or Zcash. A zero-knowledge proof is a method that allows for proving to a counterparty that a user knows certain information without revealing such an information

8. Current Challenges for BIoT Aplications

B. Security

- Google's Certificate Transparency provides a framework for monitoring and auditing SSL certificates in almost real time. The solution uses a distributed system based on Merkle hash trees that allows third-parties to audit and verify whether a certificate is valid.

- The third characteristic of security is availability, but it is actually the most straightforward to be fulfilled by blockchains, since they are conceived by design to be distributed systems, what allows them to keep on working even when some nodes are under attack.

- The most feared attack is a 51-percent attack (also called majority attack), where a single miner can control the whole blockchain and perform transactions at wish. Obviously, this kind of attack also affects data integrity.

8. Current Challenges for BIoT Aplications

C. Energe Efficiency

- IoT end-nodes usually make use of resource-constrained hardware that is powered by batteries. Therefore, energy efficiency is key to enable a long-lasting node deployment

- requirements of a full node. In terms of hashing algorithms, SHA-256 is the reference due to being the one used by Bitcoin, but new algorithms like Scrypt or X11 are faster and thus can reduce mining energy consumption.

8. Current Challenges for BIoT Aplications

D. Other Relevant Issues

- Blockchain compression techniques should be further studied, but the truth is that most IoT nodes would not be able to handle even a small fraction of a traditional blockchain. Moreover, note that many nodes have to store large amounts of data that are of no interest for them, what can be regarded as a waste of computational resources. This issue could be avoided by using lightweight nodes, which are able to perform transactions on the blockchain.

- While a few large ones may involve big payloads that cannot be handled by some IoT devices. Regarding the infrastructure, certain elements are required to make the blockchain work properly, including decentralized storage, communication protocols, mining hardware, address management or network administration

9. Further Challenges and Recommendations

- Complex technical challenges: there are still issues to be addressed regarding the scalability, security, cryptographic development and stability requirements of novel BIoT applications. methods to solve the tendency to centralized approaches should be introduced.

- Blockchain infrastructure: it will be needed to create a comprehensive trust framework or infrastructure that can fulfill all the requirements for the use of blockchain in IoT systems. Many state-of-the-art approaches that address issues such as trust depend on inter-domain policies and control.

- Organizational, governance, regulatory and legal aspects: besides technological challenges, shaping the regulatory environment (i.e., decentralized ownership, international jurisdiction) is one the biggest issues to unlock the potential value of BIoT.

10. Conclusion

- The aim of this work was to evaluate the practical limitations and identify areas for further research

- some recommendations were provided with the objective of giving some guidance to future BIoT researchers and developers on some of the issues that will have to be tackled before deploying the next generation of BIoT applications.

- We can conclude that, as in any technological innovation, there is no one-size-fits-all solution for a BIoT application.

- We can conclude that BIoT is still in its nascent stage, and beyond the earliest BIoT developments and deployments, broader use will require additional technological research advances to address the specific demands, together with the collaboration of organizations and governments.

SEOULTECH

11. Opinion

- Like IoM(5 Stack Layer), there is a need for simpler, more practical studies on the development and research of block-chain technology by layer.
- Much research is needed to optimize the block chain technology in the IoT environment.
- There is a need to study sustainable energy efficiency in limited IoT environments.
- In addition, Research is needed to optimize the privacy function of block chain in IoT environment safely.

SEOULTECH

Thank you.

SEOULTECH