Blockchain solutions for Internet of Things Systems

# Introduction

On the first days of 2009, Satoshi Nakamoto mined the genesis block of bitcoin and the number of Internet-connected devices exceeded the World’s population for the first time. On those days, two disruptive technologies were born: **Blockchain (BC)** and the **Internet of Things (IoT).** Blockchains allow parties who do not trust each other to exchange values and cooperate. Internet of Things technologies allow physical entities to listen and talk to other physical and digital entities which might not be trustworthy. The convergence of two technology is imminent. Its result is BC-integrated IoT systems (BC-IoT).

IoT systems pose challenging questions. For instance, how to establish reliable communications between IoT devices and digital services over untrusted channels? How to prevent IoT devices from joining Botnets? How to ensure the integrity of data generated by IoT devices? How to maintain evidences of misconducts in IoT systems? How to allow individuals to own and sell resources of IoT devices? How deliver firmware updates to IoT devices in a secured and scalable manner? *More importantly, how to do them all without relying on a trusted third party?*

Blockchain technologies offer some answers to those problems. *First, blockchains provide tamper-proof transaction storages* which can be used to guarantee the integrity of data generated by IoT systems. They can act as secure channels for interaction between and within IoT systems. They can also maintain forensic evidences of tampering of IoT systems. This integrity guarantee creates the necessary trust to employ IoT systems in critical situations such as tactical and operational planning, maintaining common operating pictures, pollution monitoring, city automation and smart health care. Second, *blockchains provide tamper-proof code execution* *in form of smart contracts*. These smart contracts can implement different types of logic, such as assessing the integrity of IoT devices, authorizing IoT devices to prevent them from joining botnets, and delivering software updates to IoT devices. These smart contracts also allow parties to exchange IoT resources, such as electricity, sensing data, and processing capability. Finally, *blockchains enable decentralized trustless systems*.

This work establishes a playbook to employ BC technology in IoT and similar systems. It describes technical problems of IoT that BC has been applied to solve; and the way BC network has been setup, optimized, and used in IoT system.

This playbook is synthesized from BC-related IoT systems in the academic literature. We assessed 374 related research works starting from the first IoT-BC paper in 2015 and studied in detail 90 prominent works. From these research prototypes, we extracted and synthesized three types of information: (i) The type of problem in an IoT system that they use BC to solve, (ii) how they use BC and SC to solve those problems, and (iii) optimizations that they need to bring BC and SC into IoT infrastructure.

# Blockchain-integrated IoT Systems

*A Blockchain-integrated IoT (BC-IoT) System is an IoT system that uses Blockchain and Smart Contracts.*

*An IoT System is a computer system that involves electronic tags, sensors, and actuators over the Internet.* These devices enable physical entities (Thing) to send data and events to generate insights and actions to improve business or processes [Microsoft:2018]. A distinctive feature of IoT Systems is that the communications within and between them happen over the Internet. This communication channel is open, not-trustworthy, potentially malicious. Multiple applications can share an IoT system’s sensing infrastructure, perhaps for a fee. This sharing emerges during the operation of an IoT infrastructure, differentiating it from traditional industrial control systems.

Most IoT systems revolve around a centralized IoT platform. This platform (i) monitors and configures IoT devices, (ii) provides an interface to interact with IoT devices, (iii) stores data generated by IoT devices, (iv) helps analyze and visualize IoT data for events and actions, and (v) secures IoT system from malicious data and requests. Cloud-based platforms make managing IoT system and developing IoT systems simpler. *On the flip side, IoT systems become dependent on the cloud platform.* This reliance creates a single point of corruption and failure. It also leads to silos where IoT devices do not talk to each other. Relying on the cloud also hampers the response time of IoT systems, as sensor data and control signal must travel multiple hops across the Internet.

Blockchains help decentralise IoT systems. With blockchains, all participants of an IoT system of can keep a local ledger and verify all all transactions themselves. Blockchains provide IoT systems non-repudiation of transactions. They also help remove the single point of failure and sole authority over IoT data. Finally, they can bring some intelligence of IoT systems to the edge in a secured and trusted manner.

What is Blockchain? *A Blockchain is a cryptographically secured transactional singleton machine with shared state.* [Ethereum yellow paper]. As a singleton machine with shared state, a blockchain system maintains a single truth for everyone in the network. For Bitcoin, the single truth the ledger of unspent transaction outputs (UTXO). For Ethereum, the state of all accounts on the network. As a transactional system, a blockchain system processes transactions to transit between states. Bitcoin uses a restricted script to process transactions, while Ethereum and Hyperledger Fabric in addition can use additional logic in form of Smart Contracts. As a cryptographically secured system, blockchains rely on cryptography for security. Each block contains the hash of the previous block, thus block “chain”. Users sign transactions with their private cryptography key. Addresses of users on blockchains are double-hashes of their public keys.

Blockchain systems differ in the ledger they maintain, their protocols, access rights, and off-chain elements around them. Ledgers records all transactions going through a blockchain. Ledgers vary in their data structure and the state that they maintain. Propagation protocols specify how transactions and blocks are spread across a peer-to-peer blockchain network.

Consensus protocols specify the rules that participants follow to maintain a blockchain. Specifically, they dictate how a transaction or a block can be considered valid. They also specify how to select a participant to add a block to the blockchain *(Mining)*. The purposes of this selection are to prevent Sybil attack and to make the system Byzantine Fault Tolerant. Proof-of-work, proof-of-stake, and Redundant Byzantine Fault Tolerance (RBFT) are some common miner selection protocols. Finally, consensus protocols also decide the main chain in case a blockchain forks. *Nakamoto consensus* is the most common protocol. It states that the blockchain with the most proof-of-work (longer) is the main chain.

Access rights of a blockchain specify who can read from and write to a blockchain on both block- and transaction-level. Based on access rights, blockchains can be classified into public, private, and consortium chains. *A public chain is open to everyone.* Its consensus protocols of a public chain are predetermined and open to everyone. Bitcoin is an example of a public chain. *A private chain is controlled by an organization.* This organization determines the consensus protocol and carries out the mining. *A consortium chain is a private chain which is controlled by a group of organizations*. These organizations agree on the consensus protocols and mine the blockchain together. Consortium members do not necessarily trust each other. However, they need to cooperate.

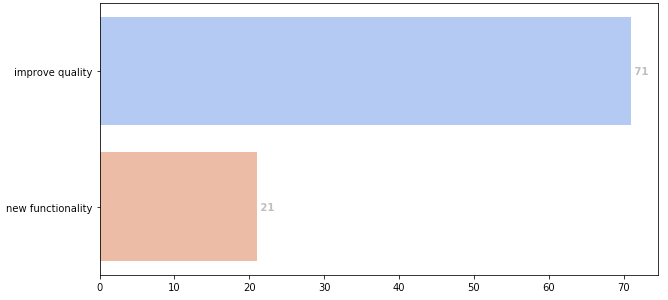
A blockchain system might also have some off-chain components. For instance, oracles help injecting context data. Key managers create and distribute key pairs among blockchain participants. Access services enforce access right of a blockchain.

A BC-IoT system can be described by how it uses blockchains and how those blockchains are built. The way an IoT-BC system uses blockchains can be described by three features: (i) the components of an IoT system that blockchains replace or enhance, (ii) the type of information stored in transactions and accounts on blockchains, and (iii) the type of logic that runs as Smart Contract on blockchains. The deployment structure of blockchains on an IoT infrastructure also describes the way a blockchain fits into an IoT system. The construction of a blockchain can be specified by its ledger, protocols, access rights, and off-chain elements.

# Blockchain solutions to IoT problems

## Objectives of blockchain integration

The surveyed research uses blockchains either to improve some qualities of IoT systems or to give them new functionalities.



*Eight out of ten reviewed research aim to improve the quality of IoT systems with blockchains*. Nearly all BC-IoT research prototypes aim to improve some aspects of IoT systems’ security. Blockchains can act as a tamper-proof source of truth of IoT systems. Because blockchain is immutable, it can keep indisputable records of interactions to and from IoT systems. Because blockchains are open for multiple parties to verify, they can detect and prevent tampering of data collected by IoT systems. Integrity, accountability, and non-repudiation improvements then can be achieved by placing sensitive IoT data and transactions directly on blockchains. Blockchains can even store hashes of devices’ configurations and firmwares to detect tampering. Authenticity improvement can be achieved by building authentication mechanisms on top of blockchains. For example, blockchains can act as a second channel for two-factor authentication. Confidentiality improvement can be achieved by building new authorization mechanisms on top of blockchains. For example, blockchains and smart contracts can be used to implement an OAuth-like mechanism.



*Around one out of ten BC-IoT research prototypes aim to improve the reliability of IoT systems with blockchains.* Availability is the degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system. This is also based on the inherent characteristic of blockchain, notably the decentralization. Availability might be increased by bringing blockchain to the edge of IoT systems. Data in the form of ledgers are available at the edge node instead of the cloud. Logic, in terms of smart contracts on blockchains, are also available at the edge of the network. By keeping data and logic at the edge and securing them with the consensus mechanism of blockchain, the availability of the IoT system can increases. Availability might also be increased by replacing the centralised cloud backend of IoT systems with decentralised blockchain, which negates the central point of failure in IoT systems.

*One out of ten BC-IoT research prototypes on average use blockchains to improve the performance of IoT systems.* Specifically, they improve the time behavior of IoT systems, which is the degree to which the response and processing time and throughput rates of a product or system, when performing its functions, meet requirements. The main idea is to use blockchain to push some processing capability and data closer to the edge, so that IoT systems can respond faster. Blockchain provide the decentralised mechanism to control the placement of computing components on the edge of IoT systems. Alternatively, blockchain can host the logic themselves with their on-chain smart contracts.

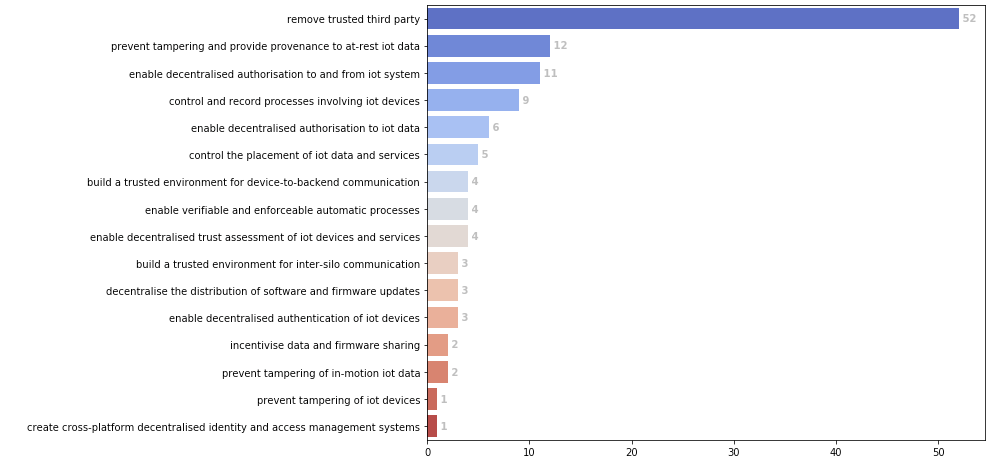
*One out of thirty BC-IoT research prototypes on average use blockchains to increase the compatibility between IoT systems*. Specifically, they target the interoperability of IoT systems, which is the degree to which two or more systems, products or components can exchange information and use the information that has been exchanged. Their focus is mostly on interoperability between IoT silos. They use blockchain to maintain trust assessment between parties so that they can communicate with each other. However, They do not use blockchain to perform data transformation or similar tasks to enable syntactic and semantic interoperability.

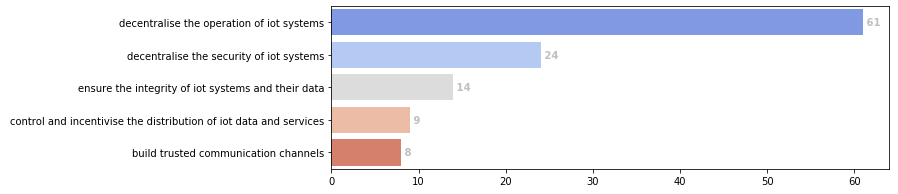


*Only two out of ten use blockchain to provide some functionality to IoT systems.* Blockchains help create market places for sensing data, electricity, as well as spare data storage and computing capability from private users. Smart contracts on blockchains can orchestrate and incentivise the exchange of resources. Blockchains can keep immutable records of transactions. Blockchains and smart contracts can also store and maintain registry for services that IoT devices offer (e.g., [Kim:2018:1]). Smart contracts running on blockchains can be also used to represent business processes that involve IoT devices in different platforms. Blockchains can act as a source of truth to synchronise distributed IoT devices. For instance, blockchains can store the “current time” of a distributed system and prevent malicious nodes from introducing time errors into the synchronisation process [Fan:2018:2].

## Problems posed by IoT systems

Regardless the objective, each BC-IoT research prototype addresses a subset of sixteen technical problems of IoT systems. These technical problems can be classified into five categories.





The first problem category is to operate IoT systems without relying on centralised backends that stores the data and control the devices. Some surveyed research aim to replace the centralised backends of IoT systems with blockchains and smart contracts [Xiong:2018:1,Zhang:2015:1,Huang:2018:1,Kang:2018:1]. Others use blockchains to regulate and keep the backends accountable [Yang:2018:1,Ali:2017:1]. These works pursue decentralisation for different objectives:

* Increasing the integrity data collected by IoT devices. This is critical for IoT systems whose data has large social and legal implications, such as pollution level [Niya:2018:1]
* Increasing the reliability of the system by replacing a single point of failure with a decentralised system that is arguably more resilient to failure and attacks.
* Increasing the performance of IoT systems by moving data and logic closer to the edge of the network.

The second problem category is to decentralise the security of IoT systems. The security mechanisms that existing BC-IoT systems decentralise include authentication, authorisation, and trust management. *Authentication* determines whether a user or a device is the one that it claim to be. *Authorisation* assesses whether a user or a device is allowed to do a certain thing in an IoT system. *Trust management* keeps track of incidents and reputation of users and devices to assess the trustworthiness of incoming messages. IoT systems generally rely on their centralised backends for security. This approach limits the scaling of IoT systems. It also reduces the reliability of the system, as devices would be unusable or vulnerable when losing connection to the backend. This approach also assumes that centralised, closed IoT cloud backends are secured and trustworthy. This might not always be the case.

On average, three out of ten surveyed research aim at decentralising the security mechanisms of IoT systems with blockchains. They use ledgers on blockchains an immutable, decentralised source of trust to store reputation rating [Yang:2018:3,Kalam:2018:1], incidents [Spathoulas:2018:1], or access requests [Saravanan:2018:1,Tapas:2018:1,Cha:2018:1,Dukkipati:2018:1]. Smart contracts then can use the trusted records in the ledger to authenticate, authorise [Ourad:2018:1], and assess the reputation of parties in IoT systems [Spathoulas:2018:1].

The third problem category is to ensure the integrity of IoT systems and their data. The first problem in this category is to detect and prevent tampering of IoT devices. These devices generally lack the protection against physical tampering and malware. Their compromise led to serious consequences. For instance, the DDoS attack (Mirai) on Dyn that took down a large portion of the Internet was caused by infected IoT devices. Tampering of camera sensors in a smart city can violate privacy of citizen and lead to legal repercussions [Gallo:2018:1]. Blockchains can help to detect tampering by maintaining immutable records of device configurations. The second problem in this category is to prevent tampering and provide provenance to at-rest IoT data. Due to its potential social and economic impacts, the incentive to modify it to cover up wrongdoings is strong. Existing BC-IoT research use blockchains to maintain immutable records [Afanasev:2018:1,Biswas:2018:1,Lunardi:2018:1] or signatures of IoT data [Gallo:2018:1,Lee:2018:1] to prevent tampering. The third problem in this category is to prevent tampering of IoT data as it moves through the networks. Existing IoT-BC research use blockchains as the communication channels between different parties in an IoT system [Qu:2018:2,Sharma:2018:1,Samaniego:2016:1]. Miners can verify the announcements from devices and ensure the integrity of messages.

The forth problem category is to control and incentivise the distribution of IoT data and services. One problem is controlling the placement of IoT data and services on fog- or edge-nodes to help IoT systems respond quicker to the external stimuli. Another is to enable a trustworthy, sustainable delivery of firmware to IoT devices [Leiba:2018:1]. Maintaining up-to-date firmware is critical to the security of IoT systems. However, manufacturers might be able to keep all operational devices up-to-date due to their large number, variety, and potentially long life-time. One solution is to have volunteers to host and share firmware, and use blockchains to orchestrate the process. Blockchains and digital signatures can guarantee the integrity of firmware in the absence of a central authority. Cryptocurrency and smart contracts can incentivize the volunteers and penalize malicious acts.

The fifth problem category is to build trusted communication channels within and between IoT systems. Within an IoT system, the communication might not be secured because it travels over wireless networks and the Internet. Essentially, the backend cannot trust the data from the devices and the devices cannot trust the commands from the backend. To address this problem, existing BC-IoT research use blockchains as the trusted intermediary to validate and audit the communication between devices and backends [Machado:2018:1,Samaniego:2018:1,Liang:2017:1]. Similarly, the interactions between IoT systems are also unsecured yet unavoidable in many applications of IoT. Blockchains, specifically consortium variation, can act as a trusted communication to orchestrate various IoT systems [Biswas:2018:1,Yang:2018:1,DiPietro:2018:1].

## Blockchain solutions for IoT systems

WIP

## IoT-specific optimizations to blockchains

WIP

# Discussion

WIP

# Methodology

To be moved from the previous draft with some updates.

# Related work

WIP

# Conclusions