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.

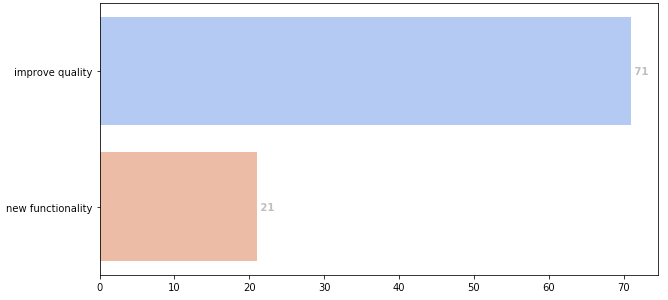
A blockchain system might also have some off-chain components. For instance, oracles help injecting context data. Key managers create and distribute key pairs among blockchain participants. Access services enforce access right of a blockchain.

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 enable novel features in IoT systems.* The most common functionality is to support ownership and exchange of IoT resources. On average, two out of ten surveyed research use blockchain technology to allow IoT device owners to own and sell their resources. Resources can come from IoT infrastructure that the owner deployed, such as electricity produced by solar panels and sensor data. The resources can also in form of data storage and computing capabilities that owner can share to IoT devices. The capability to support ownership and exchange of resource is inherent in blockchain and smart contract: blockchain records the transactions, while smart contract can be implemented to perform more complex business logic on the transactions. Challenges would be what stay on chain, what stay off chain, how to synchronise chain with devices, and how to optimise the throughput of blockchain to work with the massive influx of micro transactions from IoT devices.

The second functionality is to automate processes involving IoT devices. This functionality involves using smart contract to control IoT devices. For instance, AlkylVM for running smart contract on resource constrained devices. It also involves control the business processes that include IoT devices. Examples are applications in smart grid, which use blockchain as a ledger to store electricity production and consumption and use smart contract to control reward, penalties and rules to control the behaviour and operation of smart grid users.

The third functionality is to synchronize and form consensus amongst IoT devices. For example, they use blockchain as the single truth of time synchronise different IoT devices. [Fan:2018:2]. Alternatively, they can use characteristics of blockchain to prevent malicious nodes from introducing time error into the synchronisation process. The final functionality is to enable spatial and semantic discovery of IoT services. Specifically blockchains can be used as service registry, and smart contract can be used to handle the registry [Kim:2018:1].

## Problems posed by IoT systems

## Regardless the objective, each BC-IoT research prototype addresses a subset of sixteen technical problems of IoT systems.

## Distribution of technical problems

## These technical problems can be classified into five categories.

## Distributed of category of technical problems.

## A figure to depict the grouping of technical problems into categories.

## On average, seven out of ten surveyed BC-IoT systems use blockchains to decentralise the operation of IoT systems.

## On average, three out of ten surveyed works use blockchain to decentralise the security mechanisms of IoT systems.

## The first and most common category is to decentralise the operation of IoT systems

## Decentralising IoT systems means allowing IoT systems to operate without relying on a single controller and storage.

## This is the leading group of technical problem tackled by BC-IoT research.

## On average, seven out of ten surveyed BC-IoT systems use blockchain technology to decentralise the operation of IoT systems.

## In this group, Remove Trusted Third Party is the most common technical problem that BC-IoT systems aim to solve

## This problem aligns with the core feature of blockchain, namely decentralisation.

## Surveyed research work strived to solve this problem for different purposes

## They can be to increase the integrity of the system by removing the control of data from the hand of a centralised cloud backend.

## This is especially important for IoT systems that collect important data, that has large implication on the society, such as collecting the pollution data.

## They can be used to increase 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.

## They can be used to decrease the response time, in other word increase the performance, of IoT systems by moving data and logic closer to the edge of the network.

## Some research works focus especially on the problem of controlling IoT devices without relying on a centralised backend and keep tamper-proof record of their operations.

## Note that even though some works target the specific technical problem of controlling processes involving IoT devices, their improvement objective might not be to automate IoT system, but to pursue something else such as security or resource exchange

## The second problem category is to decentralise the security of IoT systems

## Security mechanisms include authentication, authorisation, and trust assessment.

## Authentication: whether a user or a device is the one that it claim to be.

## Authorisation: whether a user or a device is allowed to do a certain thing in an IoT system.

## Trust assessment: whether a user or a device is trustworthy.

## This trust rating can be dynamic.

## This trust rating should be tamper-proof and highly available.

## This raise a question whether a centralised, closed IoT cloud platform is trustworthy enough to assess trust and maintain trust ratings.

## The problem is how to still offer security mechanisms, such as authentication, authorisation, and trust management, without relying on a remote, closed party.

## This will remove a single point of failure in the security of the system.

## This will also remove the blind reliance on the centralised third party at the end.

## This problem is parallel with the security scandals that we see in this year, when big companies mismanage the sensitive information of users.

## For example, Facebook stores passwords in plain text files that are accessible by many employees.

## Usually, IoT systems rely on a cloud backend to secure itself.

## This cloud backend has to authenticate and authorise incoming IoT devices

## This cloud backend has to authenticate and authorise users wanting to access functionality and resources of IoT devices as well.

## Communication between different IoT systems living on different cloud backend is also tricky.

## Relying on a centralised backend for security is not a scalable solution, as it introduces a single point of failure.

## That’s why research has focus on securing IoT systems without relying on a centralised backend.

## Blockchain and smart contract have been investigated to solve this problem.

## They have some inherent characteristics that make them very useful for this task.

## Blockchains are immutable

## Blockchain network are decentralised.

## Ledger on blockchain then can be used as the source of trust.

## It can be used to store trust rating.

## it can be used to store access control policies.

## Smart contract on ledger then can be used to conduct authentication and authorisation, and calculate trust ratings, and similar tasks.

## The third problem category is to ensure the integrity of IoT systems and their data

## Prevent tampering of IoT devices

## IoT devices are open to tampering.

## Different from mainframe computers in data centres, IoT devices do not have such a degree of physical protection, therefore they are open to physical manipulation.

## IoT devices are also very limited in terms of computing capabilities, therefore they cannot run complex security checks.

## Their firmware can be modified.

## They might be affected by malware.

## The DDoS attack (Mirai) on Dyn that took down a large portion of the Internet was cased by infected IoT devices.

## Many IoT devices include sensors.

## Sensors can drift overtime and require calibration.

## Sensor can be damaged by malicious parties.

## Sensors can be tricked by malicious parties.

## In an open IoT, devices can join different IoT systems and support multiple IoT applications.

## Therefore, IoT systems must be able to protect themselves against malicious IoT devices.

## Blockchain has been explored as a solution to store the configuration of IoT devices.

## The key benefit of blockchain is still immutability and decentralisation.

## Decentralisation not only removes the reliance on a trusted third party, such as cloud platform at the backend.

## Decentralisation only improve the availability and potentially the response time of the tampering detection mechanism.

## Prevent tampering and provide provenance to at-rest IoT data

## IoT systems can generate a lot of sensory data.

## This data can have large implication, both socially and economically.

## For example, pollution data can cause large economical losses to corporation.

## There is strong incentives to modify IoT data.

## If IoT data can be tampered, then it cannot be a source of trust for many use cases.

## The benefit of the whole IoT system will be undermined.

## The data structure of blockchain makes it a potential solution for preventing tampering of data at rest.

## Prevent tampering of in-motion IoT data

## IoT data generally travel wirelessly over the Internet.

## Therefore, IoT data is widely open to tampering.

## Moreover, IoT devices are too limited in terms of computing capability to handle.

## Some works use blockchains as the communication channels between different parties in an IoT system

## Use the miners to verify announcement from devices

## Use miners to protect the integrity of messages.

## The forth problem category is to control and incentivise the distribution of IoT data and services

## The placement of data and services can help IoT systems to respond quicker to the external stimuli.

## Most of the problem is in moving the processing closer to the edge.

## Another problem that calls for blockchain is to enable a trustworthy, sustainable delivery of firmware to IoT devices.

## The number of IoT devices is large.

## The manufacturer of IoT devices cannot host the firmware updates forever.

## As a result, some devices will be outdated and receive no more update, yet they would be still operational.

## These deprecated devices then would become the weakest link of IoT systems.

## One solution is to have volunteers to host and share firmwares as mirrors.

## These mirrors might not synchronise with each other.

## There is no guarantee on the trustworthiness and integrity of these firmwares.

## There are no incentive to keep this model going.

## Some research works therefore consider using blockchain to keep and deliver the firmware to IoT devices.

## Blockchain can ensure the integrity of these firmwares.

## The fifth problem category is to build trusted communication channels

## These communications are for both intra- and inter-silo communication.

## Within an IoT system (i.e., intra-silo), the communication is still not secure because IoT systems involves the wireless communication and Internet.

## Researches have been conducted to create trusted communication channels from IoT devices to the backend over untrustworthy channels using blockchain technology.

## Blockchain and smart contract has been demonstrated to validate commands before execution

## Blockchain and smart contract has been demonstrated to verify the integrity of data coming from the backend.

## This is an interesting idea, because usually we assume that the backend is secure, and IoT device would be the one which are compromised.

## However, because communication happens over open channels, the data coming from the backend might be malicious themselves.

## Between-IoT systems communication is also tricky.

## One of the reasons is that IoT systems might have different data and operation model, and therefore are not compatible with each other.

## Another reason is that IoT systems cannot trust each other completely anyway.

## These systems might be compromised.

## These systems might act maliciously in a deliberate manner.

## However, IoT systems need to work together for orchestration.

## The simple use case would be smart home orchestration,

## Systems managing different types of devices, which belong to different companies must work together

## These systems work together to carry out a scenario predefined by the home owner.

## This situation is similar to the scenario of consortiums

## Blockchain has solution to this problem in terms of consortium blockchains.

## Some researches also explored the idea of creating cross-platform decentralised Identity and Access Management Systems using blockchain.

## Provide cross IoT platform identity management and authorisation without third party

## 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