A Decision Framework for Blockchain Platforms for IoT and Edge Computing

Claus Pahl, Nabil El Ioini, Sven Helmer
Faculty of Computer Science, Free University of Bozen/Bolzano, Piazza Domenicani 3, Bolzano, Italy
{*claus.pahl, nabil.elioini, sven.helmer*}*@unibz.it*

Keywords: Blockchain, Internet of Things, Edge Computing

Abstract: Blockchains started as an enabling technology in the area of digital currencies with the introduction of Bitcoin. However, blockchains have emerged as a technology that goes beyond financial transactions by providing a platform supporting secure and robust distributed public ledgers. We think that the Internet of Things (IoT) can also benefit from blockchain technology, especially in the areas of security, privacy, fault tolerance, and autonomous behavior. Here we present a decision framework to help practitioners systematically evaluate the potential use of blockchains in an IoT context.

1 Introduction

A blockchain is a distributed, immutable ledger to record a transaction history by allowing all participants, whether they are humans or devices, to append immutable records that are publicly available to everyone [Antonopoulos, 2014]. Blockchains allow users to interact with each other (using digital tokens) without the need of a trusted third party. In fact, an important scenario for blockchains is a situation in which there is a degree of mistrust between the participating parties, such as business partners or anonymous entities. By design, blockchains add a level of transparency, traceability, and security to this kind of environment.

Blockchains have already demonstrated their great potential in many different areas, and we believe that they can also play a major role in the Internet of Things (IoT). The IoT is about connecting a large number of devices to the Internet and taking advantage of their interactions and exchange of information and services. Devices as diverse as cars, refrigerators, or washing machines can all be connected to the Internet using the concepts of IoT, making it possible to automate many daily tasks without any human intervention. However, currently there are still important unresolved issues. Assuring privacy and security is crucial to the general acceptance of IoT and major concerns in these areas stand in the way of a mass adoption of IoT devices, as they collect vast amounts of sensitive information related to our health, environment, and location.

There have been a few attempts to investigate the importance of blockchains in the context of IoT, but many important questions still remain unanswered. The aim of our study is to systematically identify blockchain characteristics that would add value to or create strategic advantages for IoT applications.

The remainder of the paper is organized as follows. Section 2 introduces the basic concepts of blockchain technology and IoT. Section 3 discusses the advantages of blockchains for IoT. Section 4 sketches our decision framework. Section 5 presents use cases applying blockchain technology in an IoT context. Section 6 presents related work and Section 7 draws our conclusions.

2 Background

Here, we briefly introduce the main concepts of blockchains and IoT, highlighting their general properties. For more details on blockchains and IoT, see [Bashir, 2017] and [Greengard, 2015], respectively.

2.1 Blockchain overview

At its core, a blockchain is a distributed database with very interesting properties. Blockchains are based on three well-known technologies, *i)* public key cryptography, *ii)* distributed peer-to-peer networks, and *iii)* consensus mechanisms, which have been blended in a unique and novel way. Since a blockchain operates

in an untrusted environment, public key cryptography is used to establish a secure digital identity for every participant. Each participant is equipped with a pair of keys (one public, one private) to be able to participate in the blockchain. This digital identity is used to enforce control of ownership over the objects managed by the blockchain. A peer-to-peer network is employed to be able to scale up the network, to avoid a single point of failure, and to prevent a single or small group of players to take over the network. A consensus protocol allows all participants, i.e., all copies of the blockchain, to agree on a single version of the true state without the need of a trusted third party.

The main building blocks of a Blockchain are [Cachin, 2016]:

- *Transactions*, which are signed pieces of information created by the participating nodes in the network then broadcast to the rest of the network;
- *Blocks*, that are collections of transactions that are appended to the blockchain after being validated
- A *blockchain* is a ledger of all the created blocks that make up the network;
- The blockchain relies on *Public keys* to connect the different blocks together (similar to a linked list);
- A *consensus mechanism* is used to decide which blocks are added to the blockchain.

Other properties, such as scalability, security, privacy, validation time, and transactions fee, have been considered [Macdonald et al., 2017] when evaluating the use of a blockchain, or comparing existing blockchain platforms. Nevertheless, for someone not overly familiar with this topic, it may not be clear which properties to consider when comparing existing platforms and choosing one of them. In general, there are three types of blockchain platforms defined as follows:

2.1.1 Public permissionless blockchains

Public permissionless blockchains serve a 'low trust' environment where anyone can run a node and join the network which has the following characteristics:

- Access to the network is open to everyone;
- All nodes (can) participate in the consensus protocol;
- Anyone can read the full ledger of transactions;

Examples: Bitcoin, Ethereum

2.1.2 Public permissioned blockchains

Permissioned blockchains provide a hybrid model between the 'low-trust' environment of public blockchains and the 'single highly-trusted entity' model of private blockchains with the following characteristics:

- Access to the network is controlled by a preselected set of nodes;
- The consensus protocol is controlled by a preselected set of nodes;
- The right to read can be public or restricted;

Examples: Hyperledger Fabric, Ripple

2.1.3 Private blockchains

Generally, in private blockchains the participants are added and validated by a central organization. It resembles a traditional centralized system running cryptographic protocols that can be useful for auditing [Thompson, 2015]. Private blockchains exhibit the following characteristics:

- Access to the network is controlled by a single organization;
- The consensus protocol is controlled by a single organization;
- The right to read is restricted;

Examples: Multichain, Eris

2.2 IoT

IoT is about connecting a wide range of devices, from kitchen appliances to cars, to the Internet with the goal of automating a lot of daily tasks without any human intervention. Using Machine-to-Machine interaction (M2M) to communicate with many other devices over the Internet allows a device to act in a (semi-)autonomous way. Typical scenarios are refrigerators restocking themselves by ordering food when running out of supplies or cars informing a garage about some issues they may be experiencing with certain components.

This usually means devices communicating with other devices belonging to many different parties, between which no clear trust relationship has been established. This immediately raises concerns about privacy (what kind of data is sent and what happens to the data) and security (how well are IoT devices protected against malicious attackers). Additionally, the large scale of IoT networks requires efficient mechanisms to tolerate faults and to be able to operate reliably in a wide range of configurations (e.g., limited

connectivity, denial of service (DoS) or jamming attacks).

3 Blockchain advantages for IoT

Currently, IoT/Edge ecosystems adopt a client/server architecture with centralized trust brokers and Secure protocols such as SSL and TLS. For years this model has worked very well. However, the centralized approach can become a bottleneck due to the continuous growth of IoT devices in terms of numbers and applications, causing delays and failures due to the excessive congestion of the network.

Blockchains have already demonstrated a great potential in many areas beyond the financial sector and we believe that the IoT domain can also benefit from blockchain technology to address some unique challenges. Gubbi et al. [Gubbi et al., 2013] have identified a significant number of challenges faced by IoT applications today. We focus on three challenges that could be solved by applying blockchain technology.

3.1 Confidentiality and integrity

Almost all IoT devices integrate some form of sensor functionality, i.e., one of their main tasks is to collect and ship large amounts of data relating to their environment, location, and current state. However, in contrast to traditional computing devices, IoT devices are connected to a much higher degree with the physical world and our daily lives (e.g. in the form of wearable devices, smart homes, and cars). In addition to the concerns about sharing sensitive data with other parties, this adds a whole new level of security concerns, as a successful attack on these devices could cause bodily harm to their users.

The lack of standards and the rush to produce as many innovative IoT gadgets as quickly as possible to gain market shares are among the reasons why these concerns do not receive the attention they should at the moment. For some applications users may decide that the benefits outweigh the security and privacy concerns, but if we want to introduce IoT devices into more sensitive domains such as health care, we cannot ignore these concerns anymore. Applying blockchain technology to IoT devices makes it much harder to corrupt the devices by *i)* using immutable cryptographically verifiable data that is shared by all the participants in the network, and *ii)* validating the integrity of the network transactions before accepting them. Also, the linked nature of the blocks in a blockchain makes the schema hard to break. When it comes to confidentiality, some blockchains allow the encryption of the payload data to add another layer of security.

3.2 Autonomous behavior

By looking at how IoT devices are developed, we observe that devices are becoming ever smarter and more autonomous. With the increase of the number of deployed devices and the complexity of their interactions, some form of intelligence needs to be embedded into each IoT device to make it work autonomously (e.g., fog computing). Blockchains offer functionality allowing the management of infrastructure for autonomous agents in the form of smart contracts, which are self-executing programs residing on the blockchain itself. Smart contracts encapsulate business logic and conditions determining when a contract is going to be executed [Bartoletti and Pompianu, 2017]. So, the behavior of an IoT device can be specified by a set of smart contracts that allow it to interact with the rest of the network (e.g. releasing certain information after receiving payment). Crucially, smart contracts are protected by cryptographic protocols and, like the other data residing on a blockchain, cannot be easily manipulated.

3.3 Fault tolerance

In case of malfunctioning devices or attacks on an IoT network, the network needs to be resilient to avert security breaches or a network shutdown. The peer-to-peer nature of blockchain technology increases fault-tolerance and availability of the system as the failure of some nodes will not paralyze the whole network [Asharaf and Adarsh, 2017]. The decentralized architecture of blockchain also allows for lighter, faster, more reliable, and secure communication between nodes (e.g., for the distribution of software updates).

4 The decision framework

When a potential user is confronted with blockchain technology, the two most important questions that need to be answered are: i) do I actually need blockchains and ii) if yes, which platform is the most suitable for me? In our effort to answer these questions, we have developed a decision framework to help practitioners decide when to use blockchain and which type of platform to choose. Our framework builds on the knowledge gathered from existing studies and real use cases of blockchain applica-

tions, especially in the IoT context [Wüst and Gervais, 2017, Xu et al., 2016, Conoscenti et al., 2016], as an understanding of the application domain and the characteristics of each blockchain platform is crucial in deciding what platform to adopt.

The framework is divided in two parts. The goal of the first part is to answer the question when to use blockchains and what platforms to use. The second part investigates a set of properties that can be used to compare existing systems.

4.1 When to use (which) blockchain

The upper half of Figure 1 helps a potential user in deciding whether a blockchain makes sense for their application, while the lower half guides them when choosing a specific platform.

The first criterion checks whether multiple parties are involved. The involved parties can assume similar roles (e.g., readers/writers/validators) or different roles (e.g., some are readers and others are writers). Except for auditing purposes, a single party does not need blockchain functionality to manage data, as this will merely add overhead. The second criterion is the degree of interaction between the different parties. If there is no interaction, a blockchain is reduced to a simple log of independent records added by independent parties. The third criterion is the existence of a trusted third party. Blockchains are designed for environments in which trusted third parties are not available, so it will not add much value to an arbitrated protocol run by a trusted third party.

If a potential user has identified the need for blockchain technology by traversing through the upper half of the flowchart, the next step consists of determining which platform to use. The first criterion here is the anonymity of users. In an environment in which participants do not know each other, a public permissionless blockchain, such as e.g. Bitcoin, would be the best fit, as no information about the participants is required. In the other case, i.e. participants do know each other, we recommend a permissioned blockchain, as it restricts access to this group of people and provides a higher transaction rate and a faster consensus process. The choice between the public and private version of this blockchain depends on whether we need public verifiability and/or public read access.

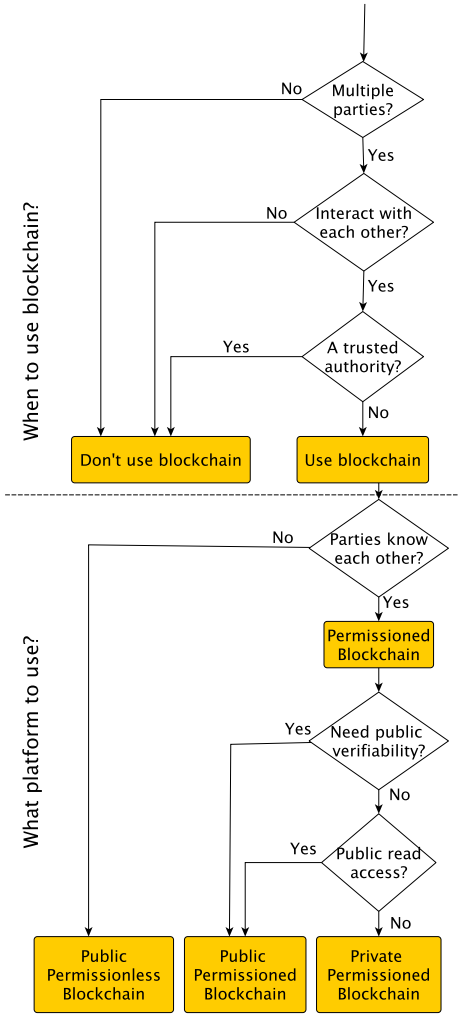

Figure 1: Blockchain platform Decision flow

4.2 Blockchain comparison properties

Once the decision for a certain platform has been taken, there is still a bewildering mix of concrete systems and implementations to choose from. In Table 1 we present major players for the different platforms and summarize their most important characteristics. Here we only show systems that have a fairly high level of support, as investing into a certain blockchain technology is a mid- to long-term commitment. Some of the existing systems are backed by a large number of independent developers, others by companies. For instance, Ethereum is managed by the Ethereum Foundation, a non-profit entity based in Switzerland, while the Bitcoin project has a large open source developer community. Hyperledger Fabric is supported by IBM and the Linux Foundation with extensive documentation and sample applications. In the following, we take a closer look at important characteristics of blockchain implementations, highlighting their strengths and weaknesses.

Table 1: Blockchain platforms and relevant properties, with an indication of their relative impact on quality in an IoT context (⋆: Least favorable, ⋆⋆: Less favorable, ⋆⋆⋆: More favorable, ⋆⋆⋆⋆: Most favorable)

Type	Name	Scalability	Consensus	Network size	Anonymity	Fee	Block size	Smart contract	Security
Public permissionless	Bitcoin	⋆	⋆⋆⋆⋆	⋆⋆⋆⋆	⋆⋆⋆	⋆⋆	⋆	⋆	⋆⋆⋆
	Ethereum	⋆⋆⋆	⋆⋆⋆⋆	⋆⋆⋆⋆	⋆⋆⋆	⋆⋆⋆	⋆⋆⋆⋆	⋆⋆⋆⋆	⋆⋆⋆
Public permissioned	Hyperledger Fabric	⋆⋆⋆⋆	⋆⋆⋆⋆	N/A	⋆⋆⋆⋆	N/A	⋆⋆⋆⋆	⋆⋆⋆⋆	⋆⋆⋆⋆
	Ripple	⋆⋆⋆⋆	⋆⋆⋆⋆	⋆⋆⋆⋆	⋆⋆⋆⋆	N/A	⋆⋆⋆⋆	⋆⋆⋆⋆	⋆⋆⋆⋆
Private	Multichain	⋆⋆⋆⋆	⋆⋆⋆⋆	N/A	⋆⋆⋆⋆	N/A	⋆⋆⋆⋆	⋆	⋆⋆⋆⋆
	Eris	⋆⋆⋆	⋆⋆⋆⋆	N/A	⋆⋆⋆⋆	N/A	⋆⋆⋆⋆	⋆⋆⋆⋆	⋆⋆⋆⋆

4.2.1 Scalability

In the context of blockchains, scalability refers to different aspects: the throughput in number of transactions per second, the types of transactions a system can process, and the interoperability with other systems. Although Bitcoin is currently one of the largest networks, it is actually one of the least scalable: the Proof of Work (PoW) scheme and block size limits result in a low transaction rate. While Ethereum, with its smart contracts allowing the execution of complex logic, supports many different types of transactions and variable block sizes, the validation time for transactions is still relatively long. Public permissioned platforms provide much higher transaction rates: Hyperledger Fabric handles 100,000 transactions per second, while Ripple can still achieve a thousand per second. Private blockchains do not have an advantage in terms of transaction rates over public permissioned ones. Nevertheless, Multichain has the advantage of being compatible with the Bitcoin network, whereas Eris relies on the Ethereum virtual machine.

4.2.2 Consensus

In order to guarantee the integrity and consistency of transactions and their related data, a blockchain relies on decentralized consensus mechanisms to validate the transactions [Baliga, 2017]. All of the systems in Table 1 employ some form of consensus protocol. The different techniques impact the systems in different ways, though. One of the first, and expensive mechanisms, is Proof of Work (PoW), which is used by Bitcoin and Ethereum. Ethash, the version used by Ethereum, is quite memory-intensive and there are plans to switch to another consensus mechanism called Proof of Stake (PoS). Hyperledger follows a more open and flexible approach by allowing users to deploy their own consensus mechanisms. By default, Hyperledger comes with two different mechanisms: Byzantine Fault Tolerance (BFT) and an augmented version more suitable for business applications called SIEVE. Ripple also uses a variation of BFT combined with an iterative consensus process. As it is a permissioned blockchain, we do not need to consider a (financial) incentive. Multichain uses a protocol close to Practical Byzantine Fault Tolerance (PBFT), but instead of multiple validators per block, there is only one, determined in a round-robin fashion. Again, since Multichain is a permissioned blockchain, it is possible to do this. The Eris consensus mechanism depends on which component is used (e.g., Tendermint uses a variation of BFT). Additionally, Eris is a private blockchain in which only certain nodes have the job of validating transactions.

4.2.3 Transaction fees

When it comes to transaction fees, public blockchains tend to be more expensive. For instance, Bitcoin is considered to have a relatively high transaction fee. This does not come as a surprise, as a financial incentive has to be provided for the nodes that are involved in the process of finding a distributed consensus. Compared to Bitcoin the fees for Ethereum are lower [Ethernodes, 2017], but they still add up to a substantial amount. Aggregating multiple transactions into one larger transaction is a possibility for a user to lower the fees.

For permissioned blockchains, the finding of a distributed consensus is not as CPU-intensive, as other, cheaper protocols can be used due to the fact that the nodes know each other. In fact, in most cases, the fees can be agreed upon between the participants a priori.

4.2.4 Network size

Ethereum is considered to be the largest network in terms of active nodes with nearly 25,000 reachable nodes spread across the world [Ethernodes, 2017], with more than 284,878 active addresses and 18,239 transactions per hour on average. Bitcoin is in second place with more than 9,200 reachable nodes [Bitnodes, 2017], more than 700,300 active addresses [bitinfocharts, 2017] generating 11,500 transactions per hour on average. Ripple has approximately 25,000 active accounts with more than 1,000,000 transaction per day. We were not able to find any information regarding Hyperledger Fabric. For the private blockchains the size can vary a lot, since it is up to the network owner to decide the size of the network.

4.2.5 Anonymity

Anonymity is a big concern for blockchain platforms when it comes to privacy, and it can be a major decision criteria for choosing one platform over the other. The main problem is that transactions are publicly logged and anyone can see them. If the transactions can be linked to their owners or the identity of the owners is disclosed, then the adopted anonymity scheme has failed. In an ideal scenario no-one in the network should be able to identify the owners of transactions or addresses using the publicly available information. Different strategies have been adopted by the existing systems with various degrees of anonymity. Public blockchains generally demand a higher level of privacy, as the identities of the users are not known and should not become known. Bitcoin relies on the use of different addresses for different transactions to increase the level of anonymity. This technique is known as *change address* [Conoscenti et al., 2016]. The Ethereum team is collaborating with zcash[1] to bring zero-knowledge Succinct Non-interactive ARgument of Knowledge (zkSNARK) to their transaction mechanism. The technique provides the possibility to hide a transaction, making it completely private [Blum et al., 1988].

4.2.6 Block size

Validating a newly generated transaction means adding it to a block in the blockchain. The size of the block can affect the time required for insertion and validation. The existing platforms have adopted different strategies when it comes to block size. Bitcoin is one of the platforms with the smallest block size, since it is limited to 1Mb, and any block that passes the limit is considered invalid. This limit affects the number of transactions that can be contained in every block, which in turn starts a competition between transactions, biasing the inclusion of transactions based on higher fees. Multichain has extended this limit by having block sizes of 32Mb and they are planning to increase it even further [Multichain, 2017]. Other platforms such as Ethereum and Hyperledger Fabric have decided to go with blocks of variable length.

4.2.7 Smart Contracts

Smart contracts enable the automation of legally binding agreements stored on the blockchain. This concept allows a blockchain to move from a narrow application area, such as financial transactions, to the management of more general types of transactions and assets. Here we are particularly interested in IoT-based applications. Bitcoin and Multichain do not provide any built-in support for smart contracts, while the other systems do so to various degrees. Ethereum even supports a full Turing-complete programming language called *Solidity* that runs on the Ethereum Virtual Machine (EVM). Eris uses the same type of contracts, since it is based on the Ethereum VM. For Ripple the situation is not very clear, as the network does not support smart contracts natively, a project called `Codius` started to add support for smart contracts. However, the project has been discontinued and it is not clear whether a different mechanism will be provided or not.

4.2.8 Security

All blockchains use cryptographic protocols to secure their data and operations, but that does not mean that there are no vulnerabilities. For Bitcoin, wallet applications are one source of vulnerabilities that can disclose transaction information [Gennaro et al., 2016]. Data and contracts in Ethereum are encoded but not encrypted. Ethereum also exhibits many of the same weaknesses as the Bitcoin blockchain (e.g. weak against 51% attacks) [Macdonald et al., 2017]. Hyperledger Fabric dedicates a large portion of its protocol to solve security issues such as ensuring that transactions cannot be linked to users, digital signatures, and access control mechanisms. However, not all of these features are implemented yet [Macdonald et al., 2017]. The Ripple network takes advantage of Transport Layer Security (TLS) to ensure that communication between all nodes is secure. All payment data is transmitted over secure HTTPS using OAuth 2.0. The actual transaction data is encrypted and shared only between the two involved parties. Multichain pro-

[1] https://z.cash

vides an integrated management of user permissions to *i)* make sure that only the chosen participants are able to see the transactions, *ii)* control the type of permitted transactions, and *iii)* mine new blocks securely with no PoW and related costs [Greenspan, 2015]. Eris provides an optimized BFT protocol, making the consensus finding process not only fault-tolerant but also adding accountability: in the case of a fork, the responsible party can be identified.

5 Use-case-based validation

We now take a closer look at three different IoT companies and the environment they operate in. We check the different aspects of each context with the help of our framework and then reveal whether a company uses blockchain technology or not. In the following we make use of the decision framework introduced in Figure 1 and the summary of system characteristics in Table 1.

5.1 Filament

Filament[2] has developed a technology stack, starting all the way from the hardware layer, to build secure devices for industrial IoT. In their white paper, which is available on their web site, they stress the point that an important goal is to have devices that are autonomous economic actors, as they expect devices to participate in the Internet economy (e.g. they envision a car itself paying for parking). This is clearly an environment in which multiple parties interact with each other without relying on a trusted third party. And, indeed, Filament leverages blockchain technology in their stack.

When it comes to the platform/system, they are currently using Bitcoin, but their CEO points out that the Filament framework is blockchain-agnostic. Although Bitcoin has limitations when it comes to block size, validation time, and smart contract support, according to the CEO this choice was made as Bitcoin is the most mature and battle-hardened blockchain implementation currently available. The data for contracts is stored using 40 Bytes of extra data added to Bitcoin transactions [Coindesk, 2017] and Filament devices only require the validated OP_RETURN data from Bitcoin transactions, since all smart contract processing happens on the devices themselves.

[2]https://filament.com

5.2 Slock.it

The goal of slock.it [3] is to provide an infrastructure that allows people to rent, sell, or share objects by fitting the objects with smart locks that are released when certain conditions (such as receiving a payment) are met. This allows the automation of renting out Airbnb apartments, vehicles, or any other underused asset that people are willing to share. Again, we have an environment in which blockchains make sense, as we have a large number of parties who want to interact with each other without having to go through trusted authorities.

As it turns out, slock.it are employing blockchain technology in the form of Ethereum. Using a public permissionless blockchain makes sense, as slock.it assumes that their IoT platform of smart locks will be used by persons who do not know each other. Each device has a unique identity, that allows it to interact and engage autonomously in complex processes with other objects using smart contracts (e.g., sign contracts, receive payments). The need for smart contracts made Ethereum the system of choice for slock.it. Once an agreement is signed, it is saved in the blockchain, and then the locked object can be used by the renting party for the period of time agreed in the contract. To reduce the transaction fees of using Ethereum, the transactions are only used for renting and releasing an object, while a free-of-charge messaging system provided by Ethereum, called *whisper messages*, is used for locking and unlocking of the rented items.

5.3 Telit

Telit[4] is an enabler of IoT, with a range of products that include cellular modules, positioning and timing sensors, IoT infrastructures and platforms, helping other companies build large-scale solutions (see the web site for an overview of Telit's use cases). In all their use cases, the IoT infrastructure is managed by a single organization or multiple parties that know and trust each other. Even though Telit relies on high security and privacy standards, such as encryption, permissions mechanisms, authentication management, and auditing, they currently do not leverage blockchain technology.

5.4 Evaluation Summary

We applied our framework to three use cases in order to demonstrate its efficacy in supporting decisions

[3]https://slock.it

[4]https://www.telit.com

whether and in which form to use blockchains for IoT settings. In two cases, already existing evidence supported the result of applying our framework, which demonstrate the validity of the framework. In one case, we have presented a company that could benefit from blockchain to increase the level of security and traceability.

6 Related work

With the emergence of blockchains, many organizations have seen its potential for increasing trust, security, and privacy in digital transactions. However, blockchains are not a silver bullet that will automatically resolve any security-related issue. In the following, we look at previous attempts to identify or characterize scenarios in which the use of a blockchain would be adequate (and in which it would not be). [Wüst and Gervais, 2017] describe different classes of application scenarios and how to take advantage of blockchain technology in these classes. They also provide a framework for analyzing scenarios and making the decision on whether to use blockchains or not. [Xu et al., 2016] view blockchains as a software connector and investigated real-world scenarios in terms of design decisions and quality measures that help in choosing a blockchain platform. A more general view is taken by [Xu et al., 2017] and [Macdonald et al., 2017]. The former present a taxonomy of blockchain-based systems, while the latter compare five general-purpose blockchain platforms, focusing on criteria such as usability, flexibility, performance, and, briefly, security. However, all these findings cover general environments, not IoT specifically. In our work, we use the existing studies as a basis and address the specific needs of IoT.

7 Conclusion

Deciding whether to use a blockchain in an IoT setting is not an easy question to answer. Although blockchains offer advantages in terms of trust, security, and privacy, there are also downsides in terms of overheads or performance issues. A positive answer to this first question immediately leads to a follow-up question: which platform/system should we use?

In our work we illustrate how blockchains can contribute to making IoT a safer and more trustworthy place. Additionally, we developed a decision framework to guide a potential user when making the decision whether to use blockchains and choosing a particular platform and system. We have also shown how blockchain technology is already leveraged by companies in their IoT operations. These use cases allowed us to demonstrate the usefulness of our framework.

As future work, we plan to develop and refine this decision framework further into a recommender tool that takes a wider range of categories into account. Security needs, for instance, can be subdivided. In IoT settings, concerns such as (sensor) data provenance are important as a specific aspect. The analysis of more use cases would also be helpful. However, not many application scenarios are properly documented at this stage.

REFERENCES

Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc.

Asharaf, S. and Adarsh, S. (2017). *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities: Emerging Research and Opportunities*. IGI Global.

Baliga, A. (2017). Understanding blockchain consensus models. Technical report, Tech. rep., Persistent Systems Ltd, Tech. Rep.

Bartoletti, M. and Pompianu, L. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns. *arXiv preprint arXiv:1703.06322*.

Bashir, I. (2017). *Mastering Blockchain*. Packt.

bitinfocharts (2017). http://bit.ly/2xQ1PZQ. Accessed: 2017-09-17.

Bitnodes (2017). http://bit.ly/2fQjaul. Accessed: 2017-09-17.

Blum, M., Feldman, P., and Micali, S. (1988). Non-interactive zero-knowledge and its applications. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 103–112. ACM.

Cachin, C. (2016). Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*.

Coindesk (2017). http://bit.ly/2ye4sUf. Accessed: 2017-09-17.

Conoscenti, M., Vetrò, A., and De Martin, J. C. (2016). Blockchain for the internet of things: a systematic literature review.

Ethernodes (2017). http://bit.ly/2xY58wG. Accessed: 2017-09-17.

Gennaro, R., Goldfeder, S., and Narayanan, A. (2016). Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security. In *International Conference on Applied Cryptography and Network Security*, pages 156–174. Springer.

Greengard, S. (2015). *The Internet of Things (The MIT Press Essential Knowledge series)*. The MIT Press.

Greenspan, G. (2015). Multichain private blockchain-white paper.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660.

Macdonald, M., Liu-Thorrold, L., and Julien, R. (2017). The blockchain: A comparison of platforms and their uses beyond bitcoin.

Multichain (2017). http://bit.ly/2yIstAn. Accessed: 2017-09-17.

Thompson, C. (2015). The difference between a private, public consortium blockchain. http://bit.ly/2xZJ4Cf, Accessed in July 2017.

Wüst, K. and Gervais, A. (2017). Do you need a blockchain? *IACR Cryptology ePrint Archive*, 2017:375.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., and Chen, S. (2016). The blockchain as a software connector. In *Software Architecture (WICSA), 2016 13th Working IEEE/IFIP Conference on*, pages 182–191. IEEE.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., and Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. In *Software Architecture (ICSA), 2017 IEEE International Conference on*, pages 243–252. IEEE.