A Blockchain-Based Decentralized Security Architecture for IoT

Pelin Angin[1](✉), Melih Burak Mert[1], Okan Mete[1], Azer Ramazanli[1], Kaan Sarica[1], and Bora Gungoren[2]

[1] Department of Computer Engineering, Middle East Technical University, Ankara, Turkey
pangin@ceng.metu.edu.tr, {melih.mert,okan.mete, azer.ramazanli,kaan.sarica}@metu.edu.tr
[2] Portakal Teknoloji, Ankara, Turkey
bora.gungoren@gmail.com

Abstract. Advances in the Internet of Things (IoT) computing paradigm have made it a popular solution covering many areas such as smart cities, connected vehicles, smart farming etc. to provide major economic benefits, reduced resource consumption, smarter environments and increased sharing of resources among other advantages. However, the security issues arising from the scale of connectivity and heterogeneity of resources in IoT make it a hot target for attackers, where centralized security solutions fall short. The vulnerabilities in providing proper device authentication and data integrity in IoT networks have been shown to introduce devastating effects. This calls for designing a data security architecture for IoT, which can accurately authenticate devices by anyone in the network in a decentralized manner and prevent unauthorized modification of the stored data. In this paper, we propose a blockchain-based approach for IoT systems that introduces transparency and tamper-resistance into data storage and retrieval in IoT networks. Evaluation of a developed prototype demonstrates that the proposed solution is promising to present a unified framework for IoT data security.

Keywords: Data integrity · Blockchain · IoT security · Verification

1 Introduction

The Internet of Things (IoT), enabling the connectivity of physical and virtual objects to create smart environments, has witnessed exponential growth in the past decade with the advances in networking infrastructures and smart devices. According to a Gartner study, the number of IoT units worldwide is expected to reach around 20 billion by 2020 [7], and the IoT connections even only within the EU is estimated to reach 6 billion by 2020 [3], covering a market of over one trillion euros. Among major applications of IoT are smart homes integrating various sensors for security, elderly care and smart energy consumption,

D. Georgakopoulos and L.-J. Zhang (Eds.): ICIOT 2018, LNCS 10972, pp. 3–18, 2018.
https://doi.org/10.1007/978-3-319-94370-1_1

wearables for personal health monitoring, smart manufacturing expected to be prevalent in the European logistic chain and production line, smart energy grids, smart cities utilizing data from various sensors for long term development planning, connected vehicles, smart farming improving the agri-food supply chain, earth/ocean observation systems addressing environmental issues, and surveillance/safety warning systems for emergency response. Wide adoption of IoT is expected to provide immense economic benefits, as it enables crossing over borders between different industrial sectors, creating more efficient processes, reduced consumption and increased sharing of resources. IoT technology will also address societal challenges as in the cases of:

– At-home health monitoring in Netherlands resulting in significant efficiency gains for elderly care efforts [16]
– Auto-adjusting streetlights in Barcelona providing over 30% energy savings [1]
– UK's intelligent transport system reducing travel time by 25% and accidents by 50% [19]

Given the potential of IoT to create smarter, safer, and efficient systems as "the next major economic and societal innovation wave" after Internet's evolution, development of IoT infrastructures and services are a significant task.

Despite the many economic and societal benefits of IoT, the security issues it gives rise to are a concerning aspect of the technology, hampering wider adoption. The crosslinking of various types of objects in IoT enables each object to influence the behavior of others and the exchange of vast amounts of information taking place automatically without the users' awareness leads to security problems including violations of data privacy and integrity, vital for both proper functioning of critical systems and data protection rights of individuals. IoT-enabled devices have already created a large attack surface for hackers to exploit. Among major security incidents involving IoT devices are:

– CIA tools turning Samsung SmartTVs into secret listening devices [8]
– The massive distributed denial of service attack against a major DNS provider (Dyn) launched through security cameras [5]
– Hackers remotely taking control of a Jeep Cherokee [9]
– The Stuxnet virus destroying a fifth of Iran's nuclear centrifuges by spinning out of control [12]

When we consider Industrial Internet of Things (IIoT), involving organizations in the energy, utilities, government, healthcare and finance sectors, the seriousness of the situation becomes more obvious. Vulnerabilities in such systems not only create privacy violations, but also hurt safety and availability, as in the case of disrupting power supply for communities through hacking into energy grids, making authentication and data integrity paramount.

Achieving security in IoT faces new challenges peculiar to the technology in addition to previously known vulnerabilities:

- Many of the current IoT devices lack basic security requirements.
- There is a lack of standardization for IoT standards and protocols, which creates security loopholes.
- There is a lack of clarity regarding who is responsible for security violations [17].
- There are scalability problems associated with the sizes of machine-to-machine (M2M) networks.
- The low computing power/battery life of many devices make them unfit for computation-intensive cryptographic operations.

The challenges facing a secure IoT model partly stem from the centralized architecture of the current IoT ecosystem, which requires devices to be authenticated through trusted third parties (TTP) with high processing power in the cloud. Even if seemingly sufficient for today's networks, a centralized security architecture will be unable to meet the needs of the near future's huge IoT networks, with the central security servers being a single point of failure, therefore hot targets for attackers, and leading to performance bottlenecks and high maintenance costs. In order to seamlessly integrate into existing IoT systems, the security architecture to be developed needs to be energy-efficient, easy to operate across a variety of IoT devices, scalable for huge device networks, provide real-time authentication and data integrity verification, and ensure end-to-end security of disseminated data in line with the protection rights of individuals such that they remain in control.

In this work, we propose an adaptable data security architecture for IoT, addressing the specific requirements pertaining to the nature of IoT devices such as limited processing power, battery life and storage space, and provide a security architecture truly fit for the decentralized nature of IoT applications, addressing the shortcomings of existing state-of-the-art client-server based models. The architecture is based on the application of the blockchain technology to IoT in order to provide secure device authentication and protect/verify the integrity of data collected by sensors and other devices in an IoT network.

The rest of this paper is organized as follows: Sect. 2 provides an overview of data security approaches in IoT. Section 3 introduces the proposed data security architecture for IoT. Section 4 discusses the results of preliminary experiments for the feasibility of the approach. Section 5 concludes the paper.

2 Related Work

Current security architectures for IoT are generally extensions of legacy client-server based models, which provide authentication of devices by certification authorities through strong standards like the X.509 public key infrastructure (PKI) [11], and utilize extensions of TLS such as DTLS [14] for securing network communication, which are both heavy-weight for devices lacking sufficient energy, storage and processing power and rely on a centralized architecture for tasks including management of security keys and data integrity verification [2], resulting in large delays unsuitable for the distributed nature of IoT applications. Following the immense growth of the IoT technology in the past decade, there have been several proposals for IoT security and privacy, among which are:

- A distributed capability-based access control method based on PKI using the Elliptic Curve Digital Signature Algorithm (ECDSA), which falls short of satisfying the real-time requirements of many IoT applications due to large delays [18]
- An IP-sec and TLS based protocol to provide authentication and privacy, which is computationally-intensive [10]
- A privacy management method based on the measurement of the risks of disclosing sensitive data, which strictly relies on the accuracy of the risk estimation methods [20].

One recent technique proving successful in providing decentralized, verifiable security and privacy of data is blockchain. Blockchain is a promising technology for secure IoT, providing a decentralized architecture, anonymity of users, tamperproof record of data transactions and highly trusted data verification/device authentication [4]. There are already proposals for utilizing blockchain as the underlying security model for various IoT systems [15], and companies like IBM and Samsung have started exploring the potential of blockchain for IoT. Although blockchain is seen by many as the next disruptive technology with great promise for IoT, a direct application of blockchain to IoT has major shortcomings to be addressed:

- The ever-growing nature of the public ledger of transactions in blockchain is not suitable for the limited storage space available in many IoT devices.
- The distributed consensus protocol involving all nodes for each transaction takes a long time, not meeting the real-time needs of some IoT applications.
- The cryptographic processing on the devices consumes too much energy.

Our proposed architecture differs from purely blockchain-based architectures in that it takes into consideration the resource limitations of IoT devices in the blockchain network, and imposes a hierarchical blockchain structure for providing data security in IoT.

3 Proposed Approach

In order to address the data security challenges of IoT, in this work we propose a decentralized data security framework for IoT, adaptable to the very nature and context of IoT applications and devices. The framework has the goal of enabling the creation of a secure IoT ecosystem through standardization and interoperability, paving the way for further interdisciplinary research involving fields ranging from autonomous vehicles to smart energy distribution networks, removing the security barrier from wider adoption of IoT-enabled devices and services. The objectives of the framework are as follows:

1. To build a decentralized, anonymity-preserving, non-repudiation capable authentication and data verification framework, able to integrate IoT devices with various capabilities and generating data in various forms.
2. To ensure adaptable operation of the data security framework, such that it adjusts the processes involved in data verification and dissemination based on the capabilities of participating devices and operation context.
3. To ensure optimal performance in terms of energy consumption and end-to-end data communication delay.

We begin this section by describing a typical data generation scenario in IoT along with its data security requirements, provide an overview of blockchain and describe the hierarchical blockchain architecture we propose to provide decentralized data security in IoT networks.

3.1 The Smart Energy Trading Scenario

One specific use case of IoT in the energy sector is the building of distributed energy distribution networks automated with the help of smart energy meters that measure the energy consumption at individual units in the network. Thanks to the availability of renewable energy production tools like rooftop solar panels, houses can now even generate their own energy and perform energy trading with their neighbors without the need for an intermediary. In the presence of no trusted intermediate authority, the tracking of the amount of energy produced/-consumed by each unit will need to rely on a mechanism that does not require *trust* between the network participants. This kind of IoT scenario is prone to the following security issues:

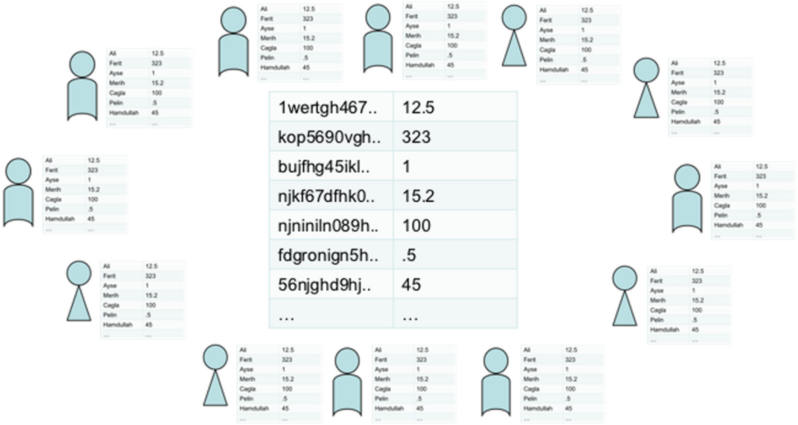
1. Especially in developing countries, fraudulent users could be involved in acts such as modifying the readings of the meters or even altering the behavior of the meters to incur negative usage costs, hence destroying the integrity of the data gathered by the IoT devices.
2. If the data gathered by all units are kept at a single site, that site becomes a single point of failure, and an attack on the site could result in the loss of all measurement data.
3. Malicious devices in the network could spoof other devices to hold them responsible for their own usage.
4. In the case of energy trading, devices buying/selling energy may not meet contractual obligations and it will be hard for the involved parties to track them down in case of using fake identities.

The last two of the above items require strong authentication mechanisms, however approaches based on trusted third parties (TTP) will not scale when the size of these networks is considered, and TTPs are still subject to the single-point-of-failure problem.

3.2 Blockchain

Blockchain, which is seen as the fifth disruptive technology in computing after mainframes, PC, the Internet and social media, is a distributed database (called *ledger*) shared and controlled by a group of networked independent parties as seen in Fig. 1. Within the context of the energy trading scenario, the ledger can be thought of as a database of all trading, production and consumption (as a result of energy consumption and production) transactions ever made by the network participants. For the sake of simplicity, the ledger in Fig. 1 shows the current energy surplus of the network participants in the database.

Blockchain provides an immutable record of data secured by a peer-to-peer (P2P) network of participants, who validate all transactions against the ever-growing database, using the cryptographic hash of each block of data in the chain that links it to its predecessor. The database updates to include new transaction records occur by broadcasting the transaction to the entire network as seen in Fig. 2 (which corresponds to sending a given amount of energy from A to B for our scenario) and running a distributed consensus algorithm typically involving the solution to a cryptographic puzzle (proof of work) by special participants of the network (miners) [13]. The whole network has a consistent copy of the ledger, which provides transaction transparency.



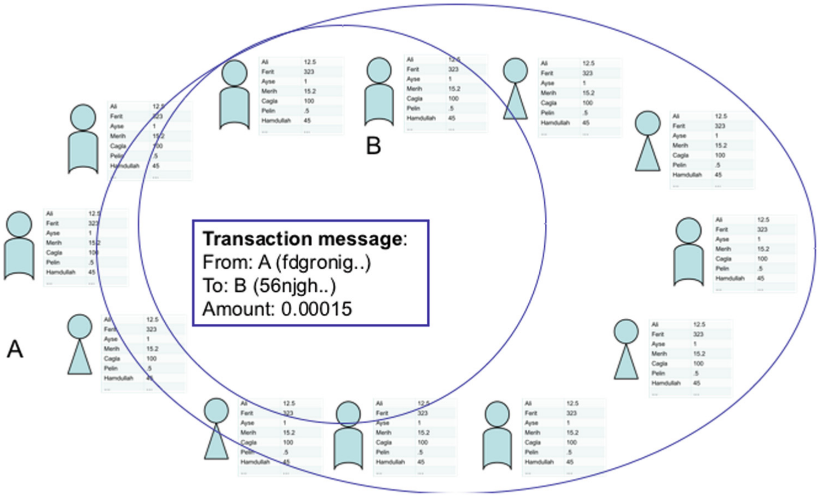
1wertgh467..	12.5
kop5690vgh..	323
bujfhg45ikl..	1
njkf67dfhk0..	15.2
njniniln089h..	100
fdgronign5h..	.5
56njghd9hj..	45
...	...

Ali	12.5
Ferit	323
Ayse	1
Melih	15.2
Cagla	100
Pelin	.5
Hamdullah	45
...	...

Fig. 1. Blockchain network and the ledger

Some important features of blockchain, which make it an important tool for distributed data security are as follows:

- It is a continuously growing list of records.
- It is protected from revision and tampering (i.e. it is immutable).
- It records all transactions that ever occurred.
- It provides non-repudiation (i.e. participants performing transactions cannot deny involvement in transactions they performed).



Transaction message:
From: A (fdgronig..)
To: B (56njgh..)
Amount: 0.00015

Ali	12.5
Ferit	323
Ayse	1
Merih	15.2
Cagla	100
Pelin	.5
Hamdullah	45
...	...

Fig. 2. Transaction in blockchain

- Upon a new transaction, the blockchain is validated across the distributed network before including the transaction as the next block in the chain (i.e. it relies on a distributed consensus mechanism).
- Blocks are made by miners (utilizing special equipment/software) coming to agreement on which transactions fit in each block, and which block will be the next in the chain.

One important feature of blockchain that makes it an effective technique for data security at scale is that it does not rely on *trust* between the participants in the network, and there is no central trusted authority involved. The security of blockchain relies purely on cryptography and distributed consensus in the network. In order to be able to write an alternative transaction history or replace any transaction in the chain, an attacker would have to invest in significant computational resources, which serves as a deterrent for adversaries. The transparency feature (i.e. everyone participating in the network has full visibility of all transactions) is a significant aspect for verifiability of all data transactions by all parties involved.

On the other hand, there are also some limitations of blockchain, which make it difficult to adapt to the problem of IoT security. Among the limitations are the following:

- The 50% + 1 rule: An attacker controlling over 50% of the network will be able to amend transactions, i.e. write an alternative history.
- Prohibitive power consumption: There are different consensus mechanisms (e.g. proof of stake, proof of work, proof of identity etc.) for blockchain, and proof of work, which requires the solving of cryptographic puzzles by the miners in the network, has been the most popular for public blockchains.

The security of this scheme relies on the complexity of the computations performed by the nodes, however this also makes it prohibitive in terms of energy consumption for resource-constrained devices to participate in the block formation process.

- Evergrowing ledger size: As the ledger keeps a record of all transactions that occurred since the formation of that blockchain, its size could become overburdening for capacity-limited IoT devices.

3.3 Hierarchical Blockchain Architecture

In order to account for the storage, processing and energy limitations of IoT devices, we propose a hierarchical blockchain architecture for data security in IoT. In the proposed architecture, the resource-limited IoT devices are connected to an upper layer of "data collectors" that are powerful devices with larger storage and less energy constraints (e.g. cloud servers). In a classical approach, these collectors would normally be connected to a central server, which stores all the collected data. However, in such an architecture, there is a chance to lose the data on some nodes, and the server is vulnerable to attacks. In the proposed architecture, we solve these problems with the benefits of blockchain. Blockchain provides a secure distributed database and eliminates the necessity of a central server. A simplified view of the hierarchical blockchain architecture is provided in Fig. 3.

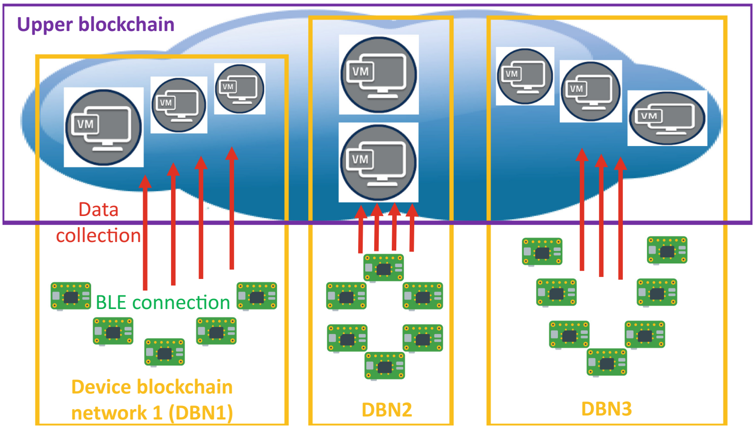


Fig. 3. High-level view of hierarchical blockchain architecture

The model ensures that the computation required for data verification is securely offloaded to nearby edge/cloud servers by resource-constrained devices in an adaptable manner considering device capacity, battery level and available storage space. This will lead to optimized resource utilization through a context-aware hybrid security architecture with computation-intensive work assigned to devices of greater capacity.

Upon issuance of a new transaction (e.g. a new energy purchase) request from a node in the IoT blockchain network, the following steps are taken:

1. The request issuer digitally signs the transaction (data update) with its own private key and broadcasts it in the device-level IoT blockchain network.
2. The transaction goes into a pool of pending transactions as seen in Fig. 4.
3. The miners in the local network verify the validity of the transaction origin by checking the digital signature on the transaction against the public key of the sender.
4. Miners pick out transactions from the pending pool, confirm the validity of the transaction logic (e.g. that the issuer has sufficient balance in his/her account to purchase the requested amount of energy) and start solving a cryptographic puzzle (using a secure hash algorithm such as SHA256 [6]). Solving the puzzle is achieved by finding a nonce value through repeatedly performing a cryptographic hash calculation involving the hash of the previous block and the current transaction until the target value is achieved.
5. The first miner able to solve the puzzle places the selected transaction in the chain, which needs to be approved by a majority of the network participants. The verification by the other participants is easy, as they are now given the correct nonce value and already have the hash of the previous block.
6. The linking of the transaction to the chain is provided by including the cryptographic hash (irreversible) of the previous block in the chain, so that any modifications to the previous data collected will not be possible (i.e. will require significant effort and computational resources).

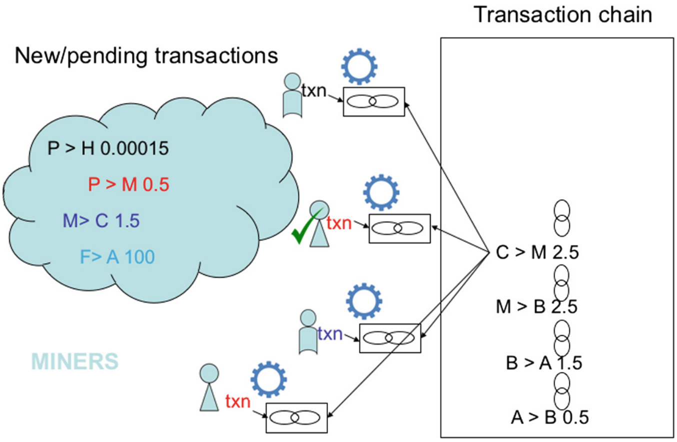


Fig. 4. Formation of blocks in blockchain

While the device-level blockchain operates as described above, the blockchain at the upper layer having powerful servers maintains the ledger of all transactions from the various blockchains at the layer below. This enables resetting of the device-level blockchains periodically to handle resource limitations, while still maintaining a transparent, data integrity-preserving complete history of transactions replicated at multiple sites.

Reconsidering the security issues with the scenario described in Sect. 3.1, we observe the proposed model mitigates them as follows:

1. Once a reading enters the blockchain, it will not be possible to change it, as the alteration would require building the whole chain from the beginning, relying on the utilization of expensive computational resources, which will outweigh the benefits of changing the meter reading/trade transaction for the adversary. Additionally, transactions that are not possible (such as negative meter readings) will not be validated by the blockchain network.
2. As the whole transaction history will be replicated at multiple sites in a transparent manner, there will be no single point of failure.
3. It will not be possible for malicious devices to spoof others, as transactions will require digital signatures, validated by all network participants.
4. Due to the transparency of transactions and the validation process, fraudulent transactions will not be possible.

4 Implementation

In a prototype implementation of the proposed architecture, we used Raspberry Pi[1] devices that collect temperature data using their sensors. These devices are connected to cloud servers that serve as data collectors through WiFi. Raspberry Pi devices connected to the same data collector create a blockchain network between themselves, and all data collectors also create a blockchain network among themselves, without using a central server. Due to the storage limitations of the Raspberry Pi devices, ledgers are formed within the network formed at the device level, and the data are pushed to the layer above periodically. This results in a blockchain of blockchains to store the entire transaction history at the upper layer involving powerful cloud servers. The blockchain was implemented using the Ethereum blockchain platform[2].

In order to evaluate the feasibility of the proposed architecture for IoT security, we performed experiments with the developed IoT blockchain. Ethereum virtual machines were installed on Raspberry Pi devices, as well as on machine instances (t2.medium and c5.large instance types) in the AWS EC2[3] and connected to the same blockchain network through WiFi. The task of mining was offloaded to the cloud servers, as the devices were observed not to be capable of successfully completing the mining process when the difficulty level of the cryptographic puzzle to solve was high, which justifies the use of edge computing and a hierarchical approach in the proposed architecture[4].

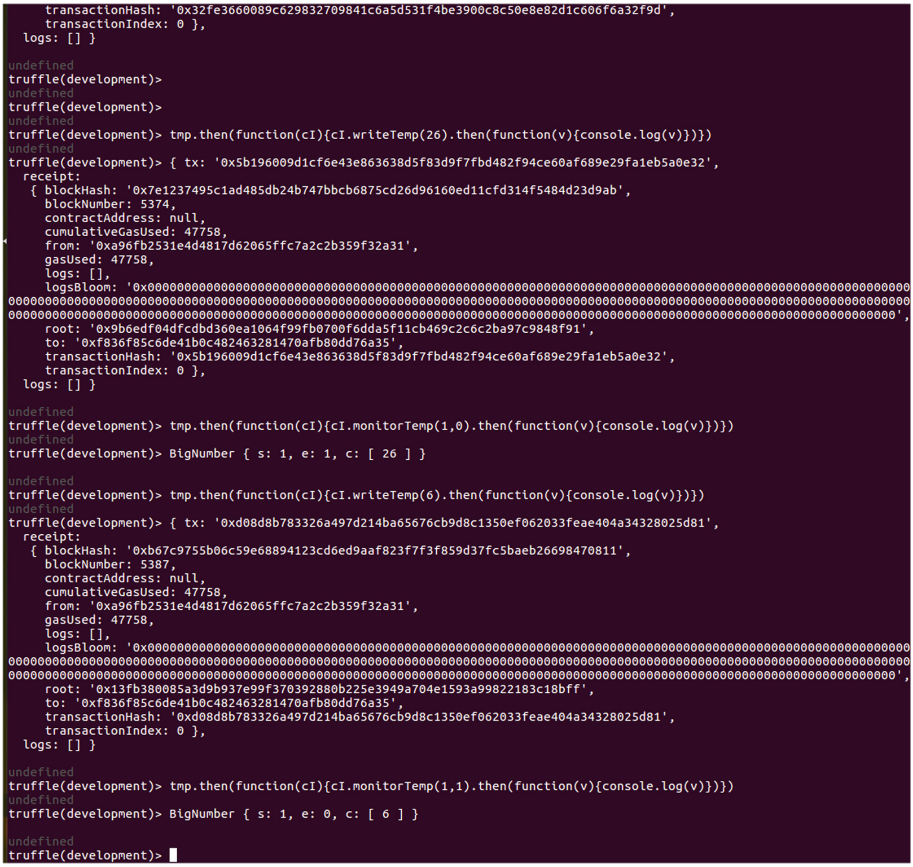
[1] https://www.raspberrypi.org/.

[2] https://www.ethereum.org/.

[3] https://aws.amazon.com/ec2/.

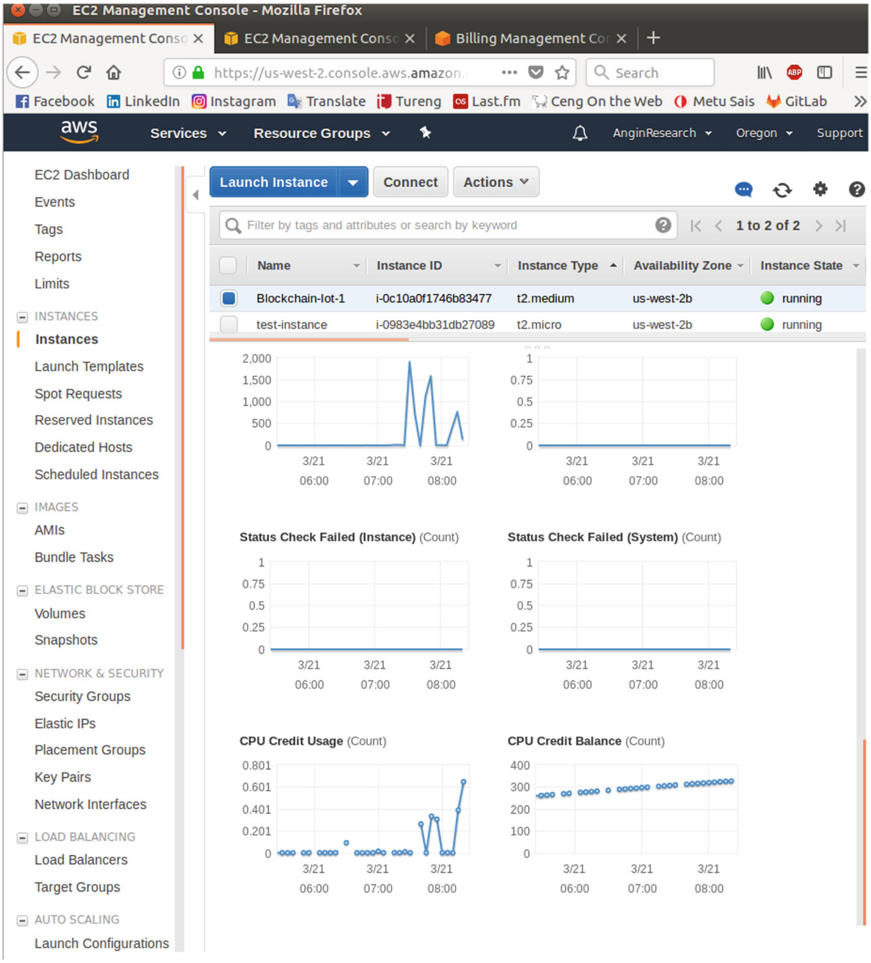
[4] Actually, even the t2.micro instance of AWS EC2 was not capable of successfully completing a mining task in the experiments.

In order to keep the transaction processing time standard (around 12–15 s), the Ethereum blockchain builds a directed acyclic graph (DAG) and automatically adjusts the difficulty of the cryptographic puzzles, which makes it difficult to evaluate performance in terms of transaction processing time. It was observed that the collected sensor data was processed and stored securely on all nodes in the formed IoT network. Figures 5, 6, 7 and 8 show excerpts from the runtime environment of the implemented blockchain.



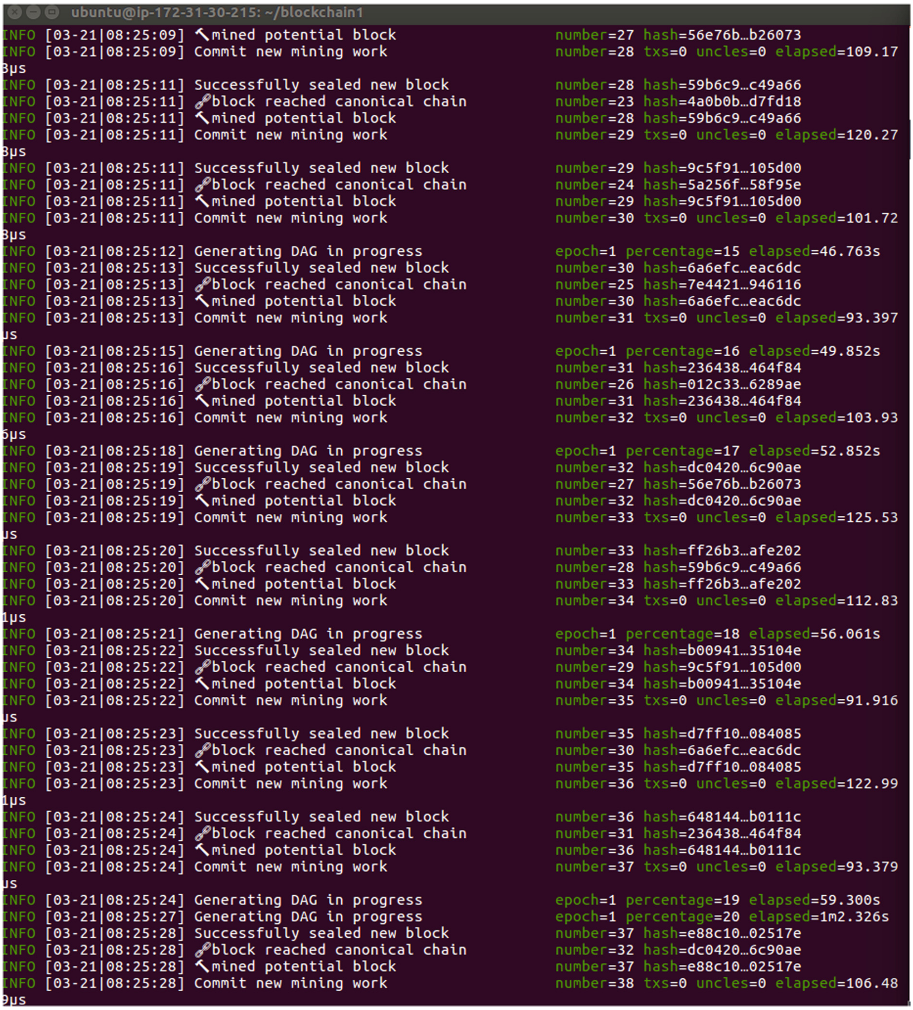
```
     transactionHash: '0x32fe3660089c629832709841c6a5d531f4be3900c8c50e8e82d1c606f6a32f9d',
     transactionIndex: 0 },
  logs: [] }

undefined
truffle(development)>
undefined
truffle(development)>
undefined
truffle(development)> tmp.then(function(cI){cI.writeTemp(26).then(function(v){console.log(v)})})
undefined
truffle(development)> { tx: '0x5b196009d1cf6e43e863638d5f83d9f7fbd482f94ce60af689e29fa1eb5a0e32',
  receipt:
   { blockHash: '0x7e1237495c1ad485db24b747bbcb6875cd26d96160ed11cfd314f5484d23d9ab',
     blockNumber: 5374,
     contractAddress: null,
     cumulativeGasUsed: 47758,
     from: '0xa96fb2531e4d4817d62065ffc7a2c2b359f32a31',
     gasUsed: 47758,
     logs: [],
     logsBloom: '0x000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000',
     root: '0x9b6edf04dfcdbd360ea1064f99fb0700f6dda5f11cb469c2c6c2ba97c9848f91',
     to: '0xf836f85c6de41b0c482463281470afb80dd76a35',
     transactionHash: '0x5b196009d1cf6e43e863638d5f83d9f7fbd482f94ce60af689e29fa1eb5a0e32',
     transactionIndex: 0 },
  logs: [] }

undefined
truffle(development)> tmp.then(function(cI){cI.monitorTemp(1,0).then(function(v){console.log(v)})})
undefined
truffle(development)> BigNumber { s: 1, e: 1, c: [ 26 ] }

undefined
truffle(development)> tmp.then(function(cI){cI.writeTemp(6).then(function(v){console.log(v)})})
undefined
truffle(development)> { tx: '0xd08d8b783326a497d214ba65676cb9d8c1350ef062033feae404a34328025d81',
  receipt:
   { blockHash: '0xb67c9755b06c59e68894123cd6ed9aaf823f7f3f859d37fc5baeb26698470811',
     blockNumber: 5387,
     contractAddress: null,
     cumulativeGasUsed: 47758,
     from: '0xa96fb2531e4d4817d62065ffc7a2c2b359f32a31',
     gasUsed: 47758,
     logs: [],
     logsBloom: '0x000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000',
     root: '0x13fb380085a3d9b937e99f370392880b225e3949a704e1593a99822183c18bff',
     to: '0xf836f85c6de41b0c482463281470afb80dd76a35',
     transactionHash: '0xd08d8b783326a497d214ba65676cb9d8c1350ef062033feae404a34328025d81',
     transactionIndex: 0 },
  logs: [] }

undefined
truffle(development)> tmp.then(function(cI){cI.monitorTemp(1,1).then(function(v){console.log(v)})})
undefined
truffle(development)> BigNumber { s: 1, e: 0, c: [ 6 ] }

undefined
truffle(development)>
```

Fig. 5. Ethereum transaction sample



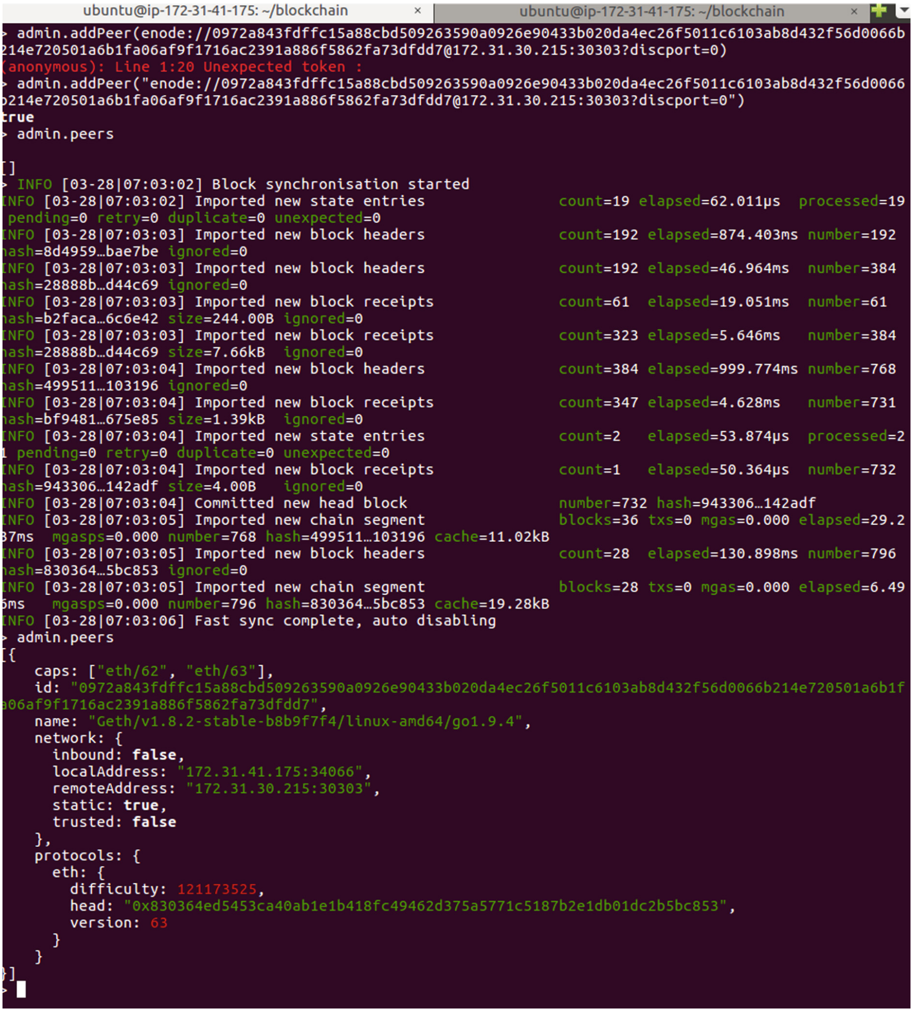
□	Name	Instance ID	Instance Type	Availability Zone	Instance State
☑	Blockchain-Iot-1	i-0c10a0f1746b83477	t2.medium	us-west-2b	● running
□	test-instance	i-0983e4bb31db27089	t2.micro	us-west-2b	● running

Fig. 6. AWS instances in Ethereum blockchain



```
INFO [03-21|08:25:09] ⛏mined potential block                   number=27 hash=56e76b…b26073
INFO [03-21|08:25:09] Commit new mining work                   number=28 txs=0 uncles=0 elapsed=109.17
3µs
INFO [03-21|08:25:11] Successfully sealed new block            number=28 hash=59b6c9…c49a66
INFO [03-21|08:25:11] 🔗block reached canonical chain           number=23 hash=4a0b0b…d7fd18
INFO [03-21|08:25:11] ⛏mined potential block                   number=28 hash=59b6c9…c49a66
INFO [03-21|08:25:11] Commit new mining work                   number=29 txs=0 uncles=0 elapsed=120.27
3µs
INFO [03-21|08:25:11] Successfully sealed new block            number=29 hash=9c5f91…105d00
INFO [03-21|08:25:11] 🔗block reached canonical chain           number=24 hash=5a256f…58f95e
INFO [03-21|08:25:11] ⛏mined potential block                   number=29 hash=9c5f91…105d00
INFO [03-21|08:25:11] Commit new mining work                   number=30 txs=0 uncles=0 elapsed=101.72
3µs
INFO [03-21|08:25:12] Generating DAG in progress               epoch=1 percentage=15 elapsed=46.763s
INFO [03-21|08:25:13] Successfully sealed new block            number=30 hash=6a6efc…eac6dc
INFO [03-21|08:25:13] 🔗block reached canonical chain           number=25 hash=7e4421…946116
INFO [03-21|08:25:13] ⛏mined potential block                   number=30 hash=6a6efc…eac6dc
INFO [03-21|08:25:13] Commit new mining work                   number=31 txs=0 uncles=0 elapsed=93.397
µs
INFO [03-21|08:25:15] Generating DAG in progress               epoch=1 percentage=16 elapsed=49.852s
INFO [03-21|08:25:16] Successfully sealed new block            number=31 hash=236438…464f84
INFO [03-21|08:25:16] 🔗block reached canonical chain           number=26 hash=012c33…6289ae
INFO [03-21|08:25:16] ⛏mined potential block                   number=31 hash=236438…464f84
INFO [03-21|08:25:16] Commit new mining work                   number=32 txs=0 uncles=0 elapsed=103.93
6µs
INFO [03-21|08:25:18] Generating DAG in progress               epoch=1 percentage=17 elapsed=52.852s
INFO [03-21|08:25:19] Successfully sealed new block            number=32 hash=dc0420…6c90ae
INFO [03-21|08:25:19] 🔗block reached canonical chain           number=27 hash=56e76b…b26073
INFO [03-21|08:25:19] ⛏mined potential block                   number=32 hash=dc0420…6c90ae
INFO [03-21|08:25:19] Commit new mining work                   number=33 txs=0 uncles=0 elapsed=125.53
µs
INFO [03-21|08:25:20] Successfully sealed new block            number=33 hash=ff26b3…afe202
INFO [03-21|08:25:20] 🔗block reached canonical chain           number=28 hash=59b6c9…c49a66
INFO [03-21|08:25:20] ⛏mined potential block                   number=33 hash=ff26b3…afe202
INFO [03-21|08:25:20] Commit new mining work                   number=34 txs=0 uncles=0 elapsed=112.83
1µs
INFO [03-21|08:25:21] Generating DAG in progress               epoch=1 percentage=18 elapsed=56.061s
INFO [03-21|08:25:22] Successfully sealed new block            number=34 hash=b00941…35104e
INFO [03-21|08:25:22] 🔗block reached canonical chain           number=29 hash=9c5f91…105d00
INFO [03-21|08:25:22] ⛏mined potential block                   number=34 hash=b00941…35104e
INFO [03-21|08:25:22] Commit new mining work                   number=35 txs=0 uncles=0 elapsed=91.916
µs
INFO [03-21|08:25:23] Successfully sealed new block            number=35 hash=d7ff10…084085
INFO [03-21|08:25:23] 🔗block reached canonical chain           number=30 hash=6a6efc…eac6dc
INFO [03-21|08:25:23] ⛏mined potential block                   number=35 hash=d7ff10…084085
INFO [03-21|08:25:23] Commit new mining work                   number=36 txs=0 uncles=0 elapsed=122.99
1µs
INFO [03-21|08:25:24] Successfully sealed new block            number=36 hash=648144…b0111c
INFO [03-21|08:25:24] 🔗block reached canonical chain           number=31 hash=236438…464f84
INFO [03-21|08:25:24] ⛏mined potential block                   number=36 hash=648144…b0111c
INFO [03-21|08:25:24] Commit new mining work                   number=37 txs=0 uncles=0 elapsed=93.379
µs
INFO [03-21|08:25:24] Generating DAG in progress               epoch=1 percentage=19 elapsed=59.300s
INFO [03-21|08:25:27] Generating DAG in progress               epoch=1 percentage=20 elapsed=1m2.326s
INFO [03-21|08:25:28] Successfully sealed new block            number=37 hash=e88c10…02517e
INFO [03-21|08:25:28] 🔗block reached canonical chain           number=32 hash=dc0420…6c90ae
INFO [03-21|08:25:28] ⛏mined potential block                   number=37 hash=e88c10…02517e
INFO [03-21|08:25:28] Commit new mining work                   number=38 txs=0 uncles=0 elapsed=106.48
9µs
```

Fig. 7. Mining in Ethereum blockchain


ubuntu@ip-172-31-41-175: ~/blockchain
ubuntu@ip-172-31-41-175: ~/blockchain

```
> admin.addPeer(enode://0972a843fdffc15a88cbd509263590a0926e90433b020da4ec26f5011c6103ab8d432f56d0066b
214e720501a6b1fa06af9f1716ac2391a886f5862fa73dfdd7@172.31.30.215:30303?discport=0)
(anonymous): Line 1:20 Unexpected token :
> admin.addPeer("enode://0972a843fdffc15a88cbd509263590a0926e90433b020da4ec26f5011c6103ab8d432f56d0066
b214e720501a6b1fa06af9f1716ac2391a886f5862fa73dfdd7@172.31.30.215:30303?discport=0")
true
> admin.peers

[]
> INFO [03-28|07:03:02] Block synchronisation started
INFO [03-28|07:03:02] Imported new state entries              count=19 elapsed=62.011µs  processed=19
 pending=0 retry=0 duplicate=0 unexpected=0
INFO [03-28|07:03:03] Imported new block headers              count=192 elapsed=874.403ms number=192
hash=8d4959…bae7be ignored=0
INFO [03-28|07:03:03] Imported new block headers              count=192 elapsed=46.964ms  number=384
hash=28888b…d44c69 ignored=0
INFO [03-28|07:03:03] Imported new block receipts             count=61  elapsed=19.051ms  number=61
hash=b2faca…6c6e42 size=244.00B ignored=0
INFO [03-28|07:03:03] Imported new block receipts             count=323 elapsed=5.646ms   number=384
hash=28888b…d44c69 size=7.66kB  ignored=0
INFO [03-28|07:03:04] Imported new block headers              count=384 elapsed=999.774ms number=768
hash=499511…103196 ignored=0
INFO [03-28|07:03:04] Imported new block receipts             count=347 elapsed=4.628ms   number=731
hash=bf9481…675e85 size=1.39kB  ignored=0
INFO [03-28|07:03:04] Imported new state entries              count=2   elapsed=53.874µs  processed=2
1 pending=0 retry=0 duplicate=0 unexpected=0
INFO [03-28|07:03:04] Imported new block receipts             count=1   elapsed=50.364µs  number=732
hash=943306…142adf size=4.00B   ignored=0
INFO [03-28|07:03:04] Committed new head block                number=732 hash=943306…142adf
INFO [03-28|07:03:05] Imported new chain segment              blocks=36 txs=0 mgas=0.000 elapsed=29.2
37ms  mgasps=0.000 number=768 hash=499511…103196 cache=11.02kB
INFO [03-28|07:03:05] Imported new block headers              count=28  elapsed=130.898ms number=796
hash=830364…5bc853 ignored=0
INFO [03-28|07:03:05] Imported new chain segment              blocks=28 txs=0 mgas=0.000 elapsed=6.49
5ms   mgasps=0.000 number=796 hash=830364…5bc853 cache=19.28kB
INFO [03-28|07:03:06] Fast sync complete, auto disabling
> admin.peers
[{
    caps: ["eth/62", "eth/63"],
    id: "0972a843fdffc15a88cbd509263590a0926e90433b020da4ec26f5011c6103ab8d432f56d0066b214e720501a6b1f
a06af9f1716ac2391a886f5862fa73dfdd7",
    name: "Geth/v1.8.2-stable-b8b9f7f4/linux-amd64/go1.9.4",
    network: {
      inbound: false,
      localAddress: "172.31.41.175:34066",
      remoteAddress: "172.31.30.215:30303",
      static: true,
      trusted: false
    },
    protocols: {
      eth: {
        difficulty: 121173525,
        head: "0x830364ed5453ca40ab1e1b418fc49462d375a5771c5187b2e1db01dc2b5bc853",
        version: 63
      }
    }
}]
> 
```

Fig. 8. Blockchain syncronization in Ethereum blockchain

5 Conclusion

In this paper we proposed a data security architecture for IoT networks. The solution is based on the application of the blockchain technology to IoT networks to provide decentralized device authentication and data security guarantees, taking into consideration the resource limitations of IoT devices and the heterogeneity of IoT networks, which enables utilization of powerful cloud servers for mining in the blockchain network. This work differs from previous work based on blockchain in that it proposes a hierarchical structure of blockchain (blockchain of blockchains) to overcome the resource problems in IoT. A prototype implementation of the proposed architecture demonstrates the feasibility and promise of the model to provide data security in IoT. Future work will include modifications to the structure of blockchain itself to utilize lightweight cryptography fit for the nature of IoT as well as amendments to the consensus protocol used, in order the achieve higher performance mining on IoT devices as well.

References

1. Barcelona: Barcelona ciutat digital. http://ajuntament.barcelona.cat/digital/ca. Accessed Mar 2018
2. Capossele, A., Cervo, V., Cicco, G.D., Petrioli, C.: Security as a CoAP resource: an optimized DTLS implementation for the iot. In: IEEE ICC, pp. 549–554 (2015)
3. European Commission: IDC and TXT solutions, smart 2013/0037 cloud and iot combination, study for the european commission. http://www.telit2market.com/wp-content/uploads/2015/02/TEL_14016_P_112-114.pdf. Accessed Mar 2018
4. Dorri, A., Kanhere, S.S., Jurdak, R.: Towards and optimized blockchain for IoT. In: 2nd ACM/IEEE IoTDI, pp. 173–178 (2017)
5. Dyn: Dyn analysis summary of friday october 21 attack. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/. Accessed Mar 2018
6. Eastlake, D., Hansen, T.: US Secure Hash Algorithms. RFC 6234, RFC Editor, May 2011
7. Gartner: Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016. https://www.gartner.com/newsroom/id/3598917. Accessed Apr 2018
8. Globe, B.: If the CIA can compromise our gadgets, can others do the same? https://www.bostonglobe.com/business/2017/03/08/wikileaks-hits-cia-secrecy-software-spying/EQdLVwseMu70HEYlZcowOO/story.html. Accessed Mar 2018
9. Greenberg, A.: Hackers remotely kill a jeep on the highway with me in it. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Accessed Mar 2018
10. Gross, H., Hölbl, M., Slamanig, D., Spreitzer, R.: Privacy-aware authentication in the internet of things. In: Reiter, M., Naccache, D. (eds.) CANS 2015. LNCS, vol. 9476, pp. 32–39. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-26823-1_3
11. NIST Network Working Group: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280, RFC Editor, May 2008
12. Kelley, M.B.: The stuxnet attack on iran's nuclear plant was 'far more dangerous' than previously thought. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11. Accessed Mar 2018
13. Laurence, T.: Blockchain for dummies. For Dummies (2017)
14. Modadugu, N., Rescorla, E.: The design and implementation of datagram TLS. In: Network and Distributed System Security Symposium (NDSS) (2004)
15. Moinet, A., Darties, B., Baril, J.L.: Blockchain based trust & authentication for decentralized sensor networks. CoRR abs/1706.01730 (2017)
16. Qorvo: Sensara senior lifestyle. http://www.qorvo.com/resources/d/qorvo-sensara-senior-lifestyle-white-paper. Accessed Mar 2018
17. Research, F.: A Mix of New and Existing Technologies Help Secure IoT Deployments. Technical report, Forrester Research (Q1 2017)

18. Skarmeta, A., et al.: A decentralized approach for security and privacy challenges in the internet of things. In: IEEE World Forum on Internet of Things (WF-IoT), pp. 67–72 (2014)
19. Road Traffic Technology: M42 active traffic management scheme, birmingham. http://www.roadtraffic-technology.com/projects/m42/. Accessed Mar 2018
20. Ukil, A., Bandyopadhyay, S., Pal, A.: Iot-privacy: to be private or not to be private. In: INFOCOM Computer Communications Workshops, pp. 123–124 (2014)