Analecta Technica Szegedinensia

Vol. 15, No. 1 ISSN 2064-7964 2021

USING RFID TO IDENTIFY SMART PRODUCTS ON A BLOCKCHAIN ENABLED PRODUCTION NETWORK

[1]*Sándor Csikós,* [2]*György Czifra,* [1]*József Sárosi*

[1]University of Szeged Faculty of Engineering, Mars tér 7, 6724, Szeged, Hungary,
[2]University of Óbuda Doctoral School of Security Science, Bécsi út 96/b, 1034, Budapest, Hungary,
e-mail: csikos-s@mk.u-szeged.hu

Received: May 31, 2021 • Accepted: June 21, 2021

ABSTRACT

Industry 4.0 requires the cooperation of several technologies. The intersections of these technologies present us with new challenges. One of these challenges is identification, since we have to identify all the items that are on the network that do work and those that are worked upon. If we fail to identify one of these items the network is presented with an unidentified potentially malicious device or a misidentified product which can cause production to halt. Blockchains or otherwise known as Distributed Ledger Technology, DLT for short is a technology that builds upon the current bookkeeping paradigm and expands it in a decentralized direction. This however can be used in more than just banking since it is essentially a distributed database that has memory of past events not just the current state. By using a blockchain based distributed database to hold processing details and using RFID-s as keys to certain entries in the database it is possible to build a tamper proof production system that can handle the challenges of industry 4.0. It may also be possible to use blockchain technology as a form of digital paper trail that can be used to validate messages sent to the nodes of the system.

Keywords: RFID, Blockchain, smart factory, smart product, data security

1. INTRODUCTION

Industry 4.0 has been labelled with many titles, one of these is Industrial Internet of Things (IIoT) [1], which is the Internet of Things (IoT) using standardised devices and achieving greater reliability. Regardless if were talking about industrial or regular IoT the main takeaway is that devices are connected on a network where they potentially can reach any other device on the network. At first glance this is a dangerous notion, since it presents an exploit also its difficult to implement since all devices need to be uniquely identifiable. According to a projection by Watanabe and Fan [2] there were to be between 26-50 billion devices connected to the internet by 2020 with no signs that the number of devices will slow their current trend. In case of fewer devices we could use IPv4, but such high numbers require IPv6 and its derivatives.

1.1. Security threats of Industry 4.0

Khan and Salah [3] place the threats in three categories depending on what level the attack is executed on. Low level attacks encompass those threats that endanger the hardware or the communications physical and data link layers. These attacks include:

- Jamming adversaries – In case of wireless communication broadcasting signals on the same frequency as required by the protocol, but the signals don't adhere to the communication protocol. (Physical layer attack)
- Insecure initialization – For a system to work properly it needs a secure initialization and setup mechanism on its physical layer, if there is none unauthorized devices can listen in on the physical layers communication.
- Low level Sybil and spoofing attacks – Sybil attacks are those attacks when an unauthorised device disguises itself as an authorised device and tries to eat up network resources. (Physical layer attack)

DOI: https://doi.org/10.14232/analecta.2021.1.1-7

- Insecure physical interface – The proper working of a device can be interfered with on physical ports such as USB or programming ports. These can be used by attackers to get access to other devices on the network (Hardware level attack)
- Sleep deprivation attack – This attack applies to devices with limited energy stores, when they need to work longer than designed for the battery will quickly drain. (Data link layer attack)

Intermediate level attacks are the attacks that use the network, transport or session layer, a few examples of such attacks:

- Replay or duplication attacks due to fragmentation – IPv6 packets need to be fragmented for devices that work according to IEEE 802.15.4, this is due to the fact that the frame size is smaller. In the case that a device receives duplicates of these packets, reassembling these consumes more than the allocated resources. This can cause buffer overflow and the reboot of the device (network layer attack).
- Insecure neighbour discovery – devices in wireless mesh networks need to discover neighbours to be able to communicate with them. Packets from an unauthorised source can lead to a denial of service attack (network level attack).
- Buffer reservation attack – a devices buffer memory that is used to assemble packets can be filled with incomplete packets, this causes a denial of service attack since the memory holding the incomplete packets is not freed (network level attack).
- RPL routing attack – the IPv6 routing protocol for Low-Powered and lossy networks (RPL) is vulnerable to several attacks from compromised devices on the network, these can deplete network resources (network level attack).
- Sinkhole and wormhole attacks – in case of sinkhole attacks the attacker responds to the routing request thereby causing the traffic to flow through the attacker node, this can be used to perform malicious activity on the network. In the case of wormhole attacks there is an tunnel through which eavesdropping, privacy violation and denial of service attacks can be executed (network level attack).
- Sybil attacks on intermediate layers – devices on the networks with false identities can initiate spamming, spreading of malware and phishing attacks (network layer attack).
- Authentication and secure communication – devices and users need to be authenticated by authenticated by key management systems. Flaws embedded in these systems house several vulnerabilities to the network (network and transport layer attack).
- Transport level end-to-end security – the purpose of this system in the transport layer is to ensure that the senders message securely arrives to the receiver (transport and network layer attack).
- Session establishment and resumption – session hijacking with forged messages can lead to denial of service attacks, also the attacker can impersonate the victim and can receive the packets meant for the victim (transport layer attack)
- Privacy violation on cloud based IoT – there are several attacks that target identity and location privacy on cloud based IoT networks. Similarly a malicious cloud service provider can access confidential information transmitted by us.

High level security issues are those that use the application layer to execute attacks, a few of these attacks are:

- CoAP security with internet – Constrained Application Protocol (CoAP) is used by devices that have very limited resources. CoAP messages follow a format described in RFC-7252 which needs to be encrypted for secure communication.
- Insecure interfaces – we can access IoT devices through the web, mobile or cloud. These interfaces are vulnerable to several attacks that target data privacy.
- Insecure software/firmware – IoT devices using SQLi and XSS languages need to be tested carefully and updates need to be carried out in a secure manner.
- Middleware security – the middleware for the heterogeneous communication of IoT devices needs to be secure enough to provide this service.

1.2 The role of RFID in Industry 4.0

From the list of described problems we continue our exploration in the narrowed down scope to the problems within identification and secure communication, since smart products fall into this category and these are one of the innovations of Industry 4.0. Smart products are products that though directly or indirectly contain instructions for their production. By this we mean that they are identifiable and they contain information for their production either in their own memory or somewhere in a database that we can access during production. For product identification there are many solutions such as optical recognition, 1 and 2 dimensional bar codes as well as identification through RFID tags. In production systems 1 and 2 dimensional bar codes only hold information for identification all other information is stored in an external database. The advantage of this method is that a central database holds the instructions for production the product itself can't be used to inject malicious instructions also updating production instructions can be done by editing the database's corresponding entry. All foreign products can be identified if they contain an unknown bar code. However a problem arises as the identification data can be read freely since it is not encrypted, this can be circumvented as the identification data can be stored encrypted. Another problem that can arise is that products can be mislabelled with a barcode that belongs on a product with different properties that the labelled product. The advantage of barcodes is that they are cheap to produce and are not sensitive to electromagnetic noise.

RFID tags on the other hand are quite susceptible to electromagnetic noise, but carry a few advantages compared to barcodes. Firstly line of sight is not required unlike for barcodes where there is a possibility that the barcode has faded. Second RFID tags are rewritable and so can hold the instructions for production or at least part of it. The main advantage of this is that it can reduce the number of network queries but it also presents problems as well. If we believe the read data without checking that could be hazardous for it could be a destructive instruction (ex: set the temperature beyond what is required), another problem is that since the tag holds the instructions this could be read out at any time. This is bad since details of production can be stolen this way from the product itself. This brings us to the problem of mutual authentication, meaning we want to identify the device and the reader as well. Since RFID tags have limited resources any method we design has to take this into account. The problem of mutual authentication has been tackled by Sidorov et al. [4] and Mujahid et al. [5]. The proposed solutions provide protection against unauthorized reading, playback, man-in-the-middle, synchronization disrupting and tracking attacks, however the solutions proposed require 520 seconds for the communication to conclude, this area can use further improvement.

There are several case studies that present the advantages of production chains that use RFID technology [6]. These solutions require a database that houses the data required for production. In the case of a distributed database each node would have a copy of the records and the queries could be done locally. The solution we are proposing is a blockchain based system. There have been studies that explore the possibilities of using blockchains in the production system [7].

2. BLOCKCHAINS AT A GLANCE

The words blockchain and cryptocurrency propose popular new technologies, however their overabundant use might cause us to think they are nothing more than buzzwords, and cause us to miss out on this revolutionary new technology. Blockchains or Distributed Ledger Technology (DLT) is a technology that solves the problem of bookkeeping in a decentralized way, but the technology has far more uses other than bookkeeping. The currently used bookkeeping method is called double entry bookkeeping since every entry needs at least 2 pieces of data from where are we transferring and to where are we transferring to (credit and debit). This bookkeeping is done by trusted third parties such as banks or bookkeepers. However this system is not without flaws since it is human based it is prone to errors and corruption. Blockchains offer a distributed trust free alternative. It is hard to give a definitive answer when will blockchain technology become a part of everyday life, there are those that equate it to the TCP protocol which started out as a niche application and evolved to the backbone of the internet [8]. Currently there are 3 generations of blockchain technology.

2.1 First generation blockchains

The first generation of blockchain was proposed in a paper by Satoshi Nakamoto [9] it is currently unknown who he is and it may be possible that it is the work of a group rather than an individual. In the paper it is proposes a system where each entity that wants to do transactions has a public and a private key and all transactions are held in an open ledger. In each transaction the recipient is identified by their public key and we add a reference to the previous transaction, this information is hashed. Hashing is a mathematical function that produces a fixed length extract of the input called a hash. The hashing function has the following properties it is a one way function that is easy to compute. Meaning it is easy to calculate the hash of a given input but it is practically impossible to do the inverse of the operation (retrieve the input from the hash). The hash is used to make the entries tamper proof, since any change will produce a totally different hash. The final step in the transaction is that the sender signs the transaction with their private key as shown in Fig. 1.

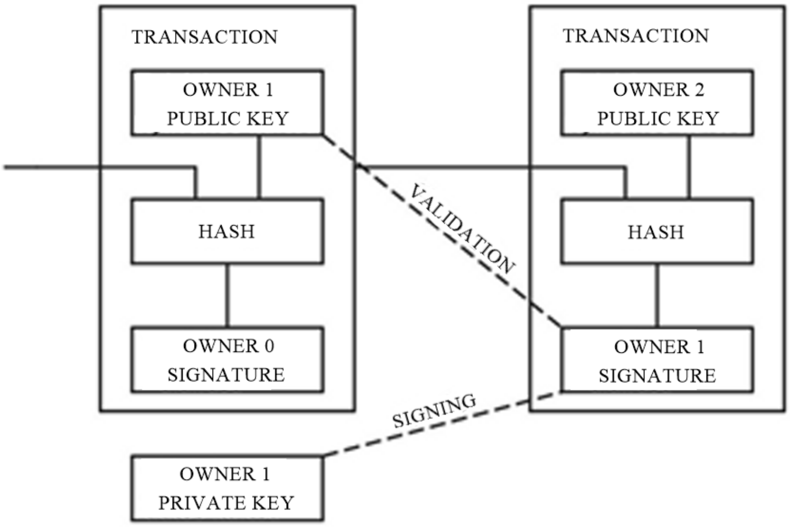

Figure 1. Transactions on a blockchain

The transactions then go to nodes called miners that place several transactions in a block, each block has the previous blocks hash and a number used only once (nonce) value as shown in Fig. 2. The miners need to figure out the value of the nonce so that the hash of the new block will start with a set number of zeroes, this is the process known as mining. Once the nonce has been calculated the node sends the newly mined block to the other nodes so they can validate the block, the process is called proof-of-work, if the block gets validated it is added to the blockchain. This proof-of-work mechanism is called a distributed systems consensus mechanism, it is a method by which the nodes can come to an agreement.

DOI: https://doi.org/10.14232/analecta.2021.1.1-7

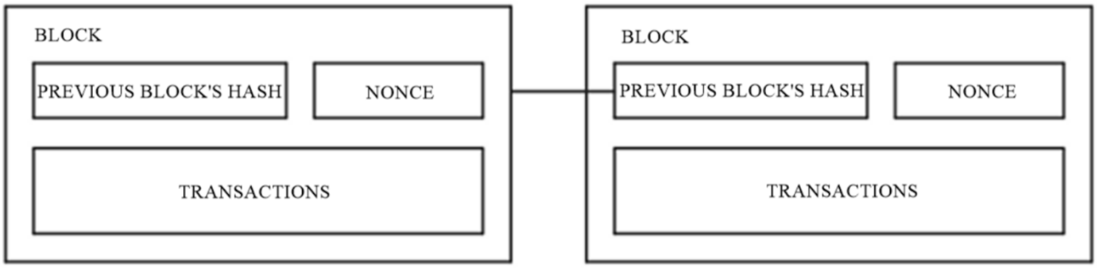

Figure 2. The structure of a blockchain

Since the only way to figure out the value of the nonce is to try all the values until there is a correct one it is computationally expensive, to reward their work the node that finds the correct nonce receives payment in cryptocurrency. The difficulty of the mining process can be adjusted up or down by adjusting the number or zeroes that are required to be in beginning of the hash, fewer zeroes easier, more zeroes increase the difficulty. Nodes follow a few simple rules on the network, they all receive all the transactions but not necessarily in the same order. Since all nodes have a copy of the blockchain they work on it can cause problems if the order of transactions is not the same for all nodes. In this case since the nonce for the blocks is correct they get attached to the blockchain and cause a fork. Since nodes always prefer the longest blockchain these forks in the blockchain die off, the transactions are logged in a different block.

Data security specifies three criteria that need to be addressed these are integrity, availability and discretion. The hashing ensures that the transactions are not altered on the blockchain. By being distributed, meaning every node has a copy of the blockchain availability is ensured. However discretion is not provided, while it is true that there is anonymity because of the public keys, the transactions cannot be denied every transaction is visible. There are so called permissioned blockchains, these unlike public blockchains don’t allow anyone to read/write on the blockchain only those who are authorized. Permissioned blockchains meet all the criteria of data security. The only way to falsify an entry in a blockchain is to recalculate every nonce of every block following the one we wish to falsify this needs to be done faster than the blockchains can produce new blocks, which is really computation intensive. Such attacks are called 51% attacks, since the blockchain is constantly growing the attacker needs to have more computational power than the rest of the network to exceed the other nodes in calculating the nonce.

2.2 Second generation blockchains

The second generation of blockchains builds on the first generation by creating smart contracts [10] these are programs that are stored and executed on the blockchain. The purpose of these smart contracts is to execute when certain predefined conditions are met. The first generation two blockchain is Etherium which creates an Etherium Virtual Machine (EVM). This can be thought of as a quasi-Turing complete computer the quasi nature comes from the fact that there’s maximum computational capacity which is a parameter called gas [11]. Another big difference between Etherium and Bitcoin is that the newer version of Etherium uses proof-of-stake instead of proof-of-work for a consensus mechanism where nodes do not compete with each other to find the nonce. According to the trends of the second generation we are heading for a global decentralized cloud based computer.

2.3 Third generation blockchains

The third generation of blockchains differs from the previous two by incorporating the notion of scalability, sustainability and interoperability which are major problems of the first two generations.

Blockchains have a problem with scalability, meaning that the performance of the system does not increase linearly with the number of nodes in the system. Transactions per second (TPS) in the case of Bitcoin has a

DOI: https://doi.org/10.14232/analecta.2021.1.1-7

theoretical maximum of 7 TPS and an average of 3-4 TPS. In comparison with some other money transferring systems VISA has a maximum of 56000 TPS and an average of 2000 TPS while PayPal is capable of 170 TPS [12]. The cause of this problem is the size of each block in the blockchain which has been set to 1 MB by Satoshi Nakamoto [13], a larger block size means more transactions can be processed at the same time and has the potential to drastically increase the TPS. Other cryptocurrencies experiment with greater block sizes but as of yet there is no quantifiable data. Generally it is true that the more nodes a system has the more resources are needed for its operation, since every node needs a copy of the blockchain it is not an easy thing to accomplish and may not be possible with nodes that have few resources and may not be necessary.

Another problem with first and second generation blockchains is sustainability. Nodes running the proof-of-work consensus mechanism collectively have a power consumption that rivals small countries [14]. To make the calculation of the nonce more feasible crypto-miners group themselves in mining pools where they pool their computational capacity and share in the rewards. Clumping together in pools detracts from the decentralized aspect of the blockchain since this way an attacker doesn't need to control the blockchain just the mining pool [15]. There are some alternatives to proof-of-work one of which is proof-of-stake [16]. In the case of proof-of-stake nodes do not compete with each other to be the first one to find the nonce, in this case nodes stake a specified amount of cryptocurrency the amount of which influences their chance to be chosen to validate the next block. In the case the validation is correct the staked amount plus the transaction fees are returned once the other nodes have checked the work, if it is detected that the node has cheated the staked amount is lost, this motivates honest behaviour.

The problem with interoperability is that transactions between different cryptocurrencies are difficult to achieve without a third party. The most prominent third generation blockchains are Cardano and IOTA.

3. DISCUSSION

According to Miloslavskaya the technology can be used for a secure information and event management systems (SIEM) database [17], but it has applications in other fields as well. The database built upon blockchain technology is much more resistant to traditional hacking attempts than conventional databases, once the scalability problem is solved it can be used as an un-falsifiable currency or a way to hold elections [18], or abstractly speaking the validation of past events such as the traceability of wood in the lumber industry, or validation of news sources. Smart contracts provide an excellent basis for e-governance [19]. Merging RFID and blockchain technologies is a novel idea and has seen some implementation in industry particularly the tracking of wood in the lumber industry [7]. The blockchain in this implementation provides a digital paper trail for the lifecycle of the wood and RFID is used to identify the items in question. The concept can be further built upon as the blockchain can hold more than just a paper trail for the product in question, it can also hold the next set of instructions in the production chain. Housing some or all of the instructions on the product presents an area that could be exploited by malicious actors and only serves as a means to lessen the amount of queries that need to take place on the network.

4. CONCLUSIONS

As we have presented a smart product requires two key components, a database to store the production information and a means to identify the product. RFID tags and barcodes can both be used to identify a product, however an RFID tag is more versatile and can be rewritten which is favourable. A blockchain can be used as a distributed database that has a record of past events and thus is difficult to tamper with. It satisfies the availability and integrity criteria of data security and a permissioned blockchain satisfies the discretion criteria as well. Naturally the adaptation of such a technology can expect pushback from people whose jobs it would automate, but a controlled integration is unavoidable. We can compare blockchains to email, since the advent of emails has not eliminated the post office, but made our lives easier.

REFERENCES

[1] A. Gilchrist, Industry 4.0. Berkeley, CA: Apress, 2016. doi: 10.1007/978-1-4842-2047-4.

[2] H. Watanabe and H. Fan, 'A Novel Chip-Level Blockchain Security Solution for the Internet of Things Networks', Technologies, vol. 7, no. 1, p. 28, Mar. 2019, doi: 10.3390/technologies7010028.

[3] M. A. Khan and K. Salah, 'IoT Security: Review, Blockchain Solutions, and Open Challenges', Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[4] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor, 'Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains', IEEE Access, vol. 7, pp. 7273–7285, 2019, doi: 10.1109/ACCESS.2018.2890389.

[5] U. Mujahid, M. Najam-ul-Islam, and M. Khalid, 'Efficient Hardware Implementation of KMAP+: An Ultralightweight Mutual Authentication Protocol', Journal of Circuits, Systems and Computers, vol. 27, no. 02, p. 1850033, Feb. 2018, doi: 10.1142/S0218126618500330.

[6] RFID in Manufacturing. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. doi: 10.1007/978-3-540-76454-0.

[7] S. Figorilli et al., 'A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood along the Whole Supply Chain', Sensors, vol. 18, no. 9, p. 3133, Sep. 2018, doi: 10.3390/s18093133.

[8] M. Iansiti and K. R. Lakhani, 'The Truth About Blockchain', p. 11.

[9] S. Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', p. 9.

[10] N. Szabo, 'Formalizing and Securing Relationships on Public Networks', First Monday, vol. 2, no. 9, Sep. 1997, doi: 10.5210/fm.v2i9.548.

[11] D. G. Wood, 'ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER', p. 32.

[12] J. Gobel and A. E. Krzesinski, 'Increased Block Size and Bitcoin Blockchain Dynamics', in 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Nov. 2017, pp. 1–6. doi: 10.1109/ATNAC.2017.8215367.

[13] 'Don't Count or Spend Payments until They Have 1 Confirmation, · Bitcoin/Bitcoin@a790fa4', GitHub, Accessed: May 24, 2019. [Online]. Available: https://github.com/bitcoin/bitcoin/commit/a790fa46f40d751307f86c37a709eb119768ce5b

[14] M. J. Krause and T. Tolaymat, 'Quantification of Energy and Carbon Costs for Mining Cryptocurrencies', Nature Sustainability, vol. 1, no. 11, pp. 711–718, Nov. 2018, doi: 10.1038/s41893-018-0152-7.

[15] 'Hashrate Distribution', Blockchain.com, Accessed: May 24, 2019. [Online]. Available: https://www.blockchain.com/pools

[16] A. Kiayias, A. Russell, B. David, and R. Oliynykov, 'Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol', in Advances in Cryptology – CRYPTO 2017, vol. 10401, J. Katz and H. Shacham, Eds. Cham: Springer International Publishing, 2017, pp. 357–388. doi: 10.1007/978-3-319-63688-7_12.

[17] N. Miloslavskaya, 'Designing Blockchain-Based SIEM 3.0 System', Information and Computer Security, vol. 26, no. 4, pp. 491–512, Oct. 2018, doi: 10.1108/ICS-10-2017-0075.

[18] B. Shahzad and J. Crowcroft, 'Trustworthy Electronic Voting Using Adjusted Blockchain Technology', IEEE Access, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

[19] H. Treiblmaier and R. Beck, Eds., Business Transformation through Blockchain. Volume 2: ... Cham, Switzerland: Palgrave Macmillan, 2019.

DOI: https://doi.org/10.14232/analecta.2021.1.1-7