Application of Blockchain and Smart Contracts on the Internet of Things

Nicholas Lucci *nicholas.lucci@ubalt.edu*
Applied Information Technology
University of Baltimore
Baltimore, Maryland, USA

Mohammed Ketel *mketel@ubalt.edu*
Applied Information Technology
University of Baltimore
Baltimore, Maryland, USA

Abstract

With the recent peak in interest regarding the concepts of bitcoin and the associated Blockchain (BC) network, this paper seeks to examine current implementations of using peer-to-peer based transaction system and the technology behind it. Due to the inherent trustless transaction model incorporated within a BC based system, members are able to transact with other members without the use of a middleman. Additionally, this paper explores the concepts of smart contracts, scripts embedded into the BC system to execute specified external functions following a successful transaction on the network. This decentralized system appears to be the perfect fit for the growing Internet of Things (IoT), the network of devices that can facilitate a growing market between devices and services across the internet. The paper explores the various difficulties associated with setting up such a system, while also exploring the benefits solutions that a decentralized IoT BC system would provide to the current technological landscape. The findings of the paper indicate that there is a demand and a place for an IoT BC through the implementations of smart contracts and careful planning. This type of network could help to revolutionize the current industrial landscape across a variety of sectors in the near future.

Keywords: Blockchain, Bitcoin, IoT, Security, Smart Contracts.

1. INTRODUCTION

Recently, both cryptocurrency and the associated Blockchain (BC) technology have attracted a wide array of interest across a variety of fields, including finance [1, 2], healthcare [3, 4], governmental agencies [5, 6] and the technology sector [7 - 9]. The use of BC technology allows applications to be run independently of any central authority while retaining the same amount of confidence as before. This functionality is possible because of the peer-to-peer structure of the network, which allows parties on the network to communicate securely even though they do not inherently trust each other. The use of cryptography ingrained into the BC network promotes a secure environment for all transactions across the network [10].

The use of smart contracts built upon the BC network offers unique advantages for developers and researchers working with the Internet of Things (IoT). Smart contracts are self-executing scripts that contain instructions based on an input [7, 8, and 27]. This can be anything from transferring funds from one financial institution to another, or releasing the title to a car after a payment is verified on the network. Due to the trustless nature of the BC network, smart contracts create the ability to consolidate the verification process for the end user and eliminate the need for middlemen and third party services. Smart contracts create a much more streamlined process for everyone involved and provide numerous benefits to security that are simply not available to traditional contracts [13, 27].

Unfortunately, even with all the benefits that a BC based network and smart contracts bring to the table, they are not always an ideal solution. This paper will seek to expand upon the concepts of smart contracts and the associated BC network, while exploring the pros and cons of implementing a BC based network alongside the IoT. This paper will also seek to expand upon the future implementations of the IoT and show how to formulate decisions when trying to decide whether or not a blockchain based network will provide a benefit to the desired applications.

The paper will begin by expanding upon the concept of a BC, breaking down the technicalities between how the BC operates and the associated network operations involved. Next, it will detail the concept of smart contracts and how they can help to redefine how transactions on a BC-based network can be automated between the involved parties. The next part will explore how BCs and IoT can be used together while identifying current implementations and their associated pros and cons. Finally, the paper will present the conclusions found.

2. TECHNOLOGICAL OVERVIEW

2.1 Concept of a Blockchain

A BC is a digital ledger technology in which transactions made in cryptocurrency are recorded chronologically and publicly [7, 8]. It is a distributed database that is used to maintain a continuously growing list of records known as blocks and is managed using a peer-to-peer network that collectively adheres to a protocol for validating each subsequent block in the chain [7, 8]. The concept of a BC was conceptualized by Satoshi Nakamoto and first appeared in 2008 as a core component of bitcoin where it serves as a ledger for public transactions [10]. As a transaction becomes validated by the miners on the network, the transaction block will be appended to the BC creating a long standing mutually agreed upon chain of blocks which makes up the public ledger of transactions establishing who owns what [11]. Each block in the chain contains a hash to the previous block in the chain, maintaining that the chain continues to remain validated as it grows.

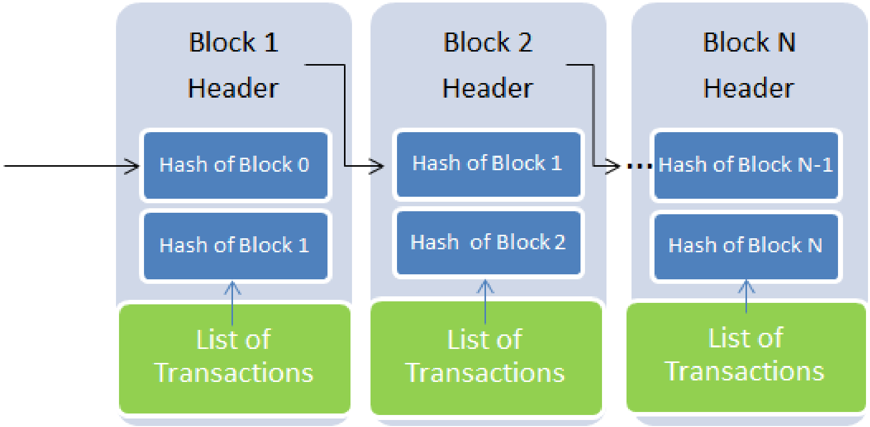

FIGURE 1: A Simplified Blockchain.

2.2 Independent Blockchains

When using a BC it is not necessary to have a connected cryptocurrency as a block is able to function solely on its own [12]. A BC is merely a link of transactions between parties which are batched together into a chain. Each header element of a block is hashed and then referenced in the next block ensuring the integrity of the chain as seen in Figure 1. Any node on the network can access this chain of blocks and figure out the current state of each transaction ID by following the chain of blocks throughout the transactions [13].

While this process describes individual blocks on the network, it is important to understand how the network functions. Each client on a network is known as a node with each node having access to the same BC as all other nodes on the network [8]. These nodes together form a peer to peer network where the users interact with each other using a series of private and public keys, essentially account numbers. When creating a node on a network, each node will have access to a public key which essentially acts as a public address for a person on the network. This is used in conjunction with the private key, which is used to sign off on transactions associated with the public key [13].

Together the combination of public and private keys is protected by asymmetric encryption, which brings authenticity and integrity to the network, while ensuring that each transaction is unique and cannot be duplicated. Following a transaction being signed with a private key, the block is relayed to the one-hop peers on the network who then also validate the authenticity of the transaction before forwarding it further on through the network [7, 13].

The transactions that have been validated for authenticity are then ordered into the candidate BC by timestamp. If the block is validated through the mining process which will be explained later, the mining node will resend the now cryptographically authenticated block back through the network. Should the block be seen as authentic by the nodes on the network, meaning that the block both contains valid transaction information as well as correct references to the hashes of the previous blocks; the block will then be accepted by the network [7, 9]. Once accepted, the block will then be added onto the current BC, where the network will see the update, and the current BC will be permanently updated and publically viewable. This process will continually repeat itself as more transactions continue to occur over the network. One of the main concerns however, is what exactly constitutes a valid transaction? Since the BC is essentially a group of untrusted nodes connected on the network, there needs to be a certain set of regulations in place to verify the legitimacy of every transaction before it is added to the BC. This commonality is known as consensus and is the basis for a peer-to-peer managed BC system [8, 13].

When creating a BC, it is important to note that each BC client can determine the rules necessary to decide whether an incoming transaction is valid and whether that transaction block should be added to the network [27]. In a simplified model where each address is mapped to a public key, a valid transaction is one that attempts to modify a value when there is a corresponding private key signature present [7, 27]. When each node follows the steps outlined by the BC client, that block then become an authenticated and timestamped record of the activity on the network [27]. This system does not require that the nodes have to trust any other nodes in particular. The effect of the system is that a trustless environment is created, with authenticity being verified by the combined efforts of all nodes on the system rather than any individual force [6].

2.3 Consensus

With any BC client, the integrity of the transaction list is based upon the idea that each transaction is stored on a single chain in the appropriate time order from the first to the most current transaction. As mentioned earlier, the idea of a BC relies on the distributed consensus that each node in the client is running off the same ledger is vital to ensuring the success of the system. Each BC network may use a slightly different consensus mechanism to establish this trust; however, the variability speaks towards the adaptability of the system for the different situations that it may be adopted for [7, 9].

In an ideal situation, each node would vote on a new block as it appeared and the block with the majority of votes cast would become the next block in the chain. However, due to the open availability of a network, some-one could potentially create multiple accounts and flood the server with votes for blocks that are not actually legitimate. With enough support, a person or group could alter the BC to mislead the network into accepting a false path in the BC filled with false transactions [7, 13].

To get around this problem, cryptocoins like bitcoin have employed rigorous validation standards that are inherently expensive to perform [14]. Bitcoin uses the SHA-256 algorithm to secure the transaction details, which is a one way cryptographic algorithm producing a single output given an input string [15]. A node on the network will attempt to input a random number into algorithm along with details from the most recent block and some transaction details such as public keys from the sender. Should this algorithm produce an output hash with the appropriate specifications, the block is added to the chain, the universal BC is updated across all nodes and the miner is credited some cryptocurrency. In the case of bitcoin, the output hash must have a certain number of trailing zeroes, which can be adjusted depending on how difficult the hash should be to solve. This proof of work creates incentive for miners on the network to use their computing power to verify transactions.

Different BC systems make use of other algorithms such as Scrypt in the case of Litecoin [16] and a combination of several algorithms in the case of Myriad [17]. This adaptability of the BC system allows for tradeoffs between speed of transactions and security without compromising the authenticity of the network.

However, when it comes to private BCs for commercial or personal purposes, these extensive proof of work concepts are not necessary. When dealing with a private network, when nodes are whitelisted accordingly there is no risk of a minority attack compromising the network. This allows other more effective methodologies to be used in order to verify the legitimacy of the BC.

One such consensus algorithm is the “Unique Node List” (UNL) system of Ripple, a cryptocurrency designed to facilitate transactions between financial institutions [18, 27]. In the UNL system, rather than having to query a majority of nodes on the network in order to come to a consensus, the UNL system creates multiple subnetworks within the larger ripple system. This means that a node needs only to query its own UNL in order to come to a consensus for the entire network, vastly improving upon the open style traditional BC systems [27]. Regardless of the type of consensus used, it should be noted that each miner in the network only has a small amount of power as compared to a traditional centralized database.

2.4 Transactions on a Blockchain

When describing a typical transaction as it would take place in a financial institution it is easy to imagine a physical account into which money can be transferred. Imagine we are looking at an informational database with fields for “Account Holder”, “Amount” and “Asset Type”. An account for person X which contains $100 USD would contain all the necessary information to indicate that X has $100 in X’s account at the bank. Now if X were to transfer $10 of that to Y who has $10 in Y’s bank account, X would write out a check with the details of X’s account and the receiver’s account written out, along with a signed signature verifying X identity. The bank would then verify the legitimacy of the details and we would then see X’s account decrease to $90 while Y’s increases to $20 in the system. Despite no physical goods being traded the digital reference to the funds was altered in the database for both parties. It is possible to get a similar result with some improvement by using a BC which will make the transaction faster and without the need of intermediaries [9, 27].

Cryptography is exceptionally good at facilitating these types of signed transactions, such as with a BC network that employs a currency model of distributed digital assets. The same process can also be used with smart contracts although they are slightly more difficult to set up and design around.

The questions around the use of a BC arise from the breakdown of a traditional model of database related financial service. In the transfer scenario from X to Y, the transaction must be legitimized and concurrency must be prevented. This type of validation and transfer serves as an integral part of the BC-based system, but how exactly bitcoins are or any other cryptocurrency generated to begin with.

2.5 How Cryptocurrency is Formed

Like many other forms of currency, cryptocurrency derives its value from the trust of the users in the system. Established by the United States Constitution, the United States Dollar (USD) was originally able to be exchanged for its equivalent worth in gold at any time. This put an inherent trust into the use of the USD as the dollar bill was backed by a tangible asset that held value. Since 1971 however, the link between gold and the USD has been severed completely [16, 20]. Nowadays, the USD solely relies upon the trust established by the US government ensuring that one dollar is worth exactly one dollar of bargaining power. Without getting into the specifics of fiat currency or the logistics of the debt the United States lends out to ensure the economy continues to grow; the of advantages of a centralized currency remain an integral part of a modern-day society [10-12, 16].

Similar to how the USD derives value from the trust the people have in the legal backings of the U.S. government, bitcoin and in fact all cryptocurrency derive their trust from the integral security features of the crypto-currency [1, 2]. Much as how one physical USD is worth exactly one $1, one bitcoin, litecoin or any other is trusted to be worth exactly one, regardless of which dollar or coin is in possession. The difference is how this currency is controlled and introduced into the system [10, 16, and 20].

When establishing a BC network, the permissions allowed determine the availability of resources to be allocated across the platform. When using a network such as MultiChain [23, 27], an open source BC platform permissions can be assigned based on based on public keys on the network. This allows for configurations of who can connect to the network, complete transactions on the network and issue resources across the network [27].

With bitcoin, new bitcoins are issued with each successful completion of a mined block. Each time a mined block is accepted by the network, a transaction is then broadcasted to the network, rewarding the successful mining node with a predetermined amount of bitcoin. The unique benefit to a network with an agreed upon source of currency is that there is no middleman or regulation involved once setup is complete [16]. As every node in the system has access to the history of all the verifiable transactions, there is no need for constant regulations to occur. Once a network is established it essentially operates in set and forget mode.

3. SMART CONTRACTS

First proposed by Nick Szabo in 1994, smart contracts are defined as “a computerized transaction protocol that executes the terms of a contract” [21]. Originally, Szabo slated the idea of a smart contract to translate a contractual clause, such as asset transfer into digital code and to link physical objects with code that will self-execute in the event that certain actions are completed [22]. This type of contract was intended to cut out the middleman needed for a transaction between parties, helping to cut down on fraudulent and accidental occurrences, while speeding up the transfer process in the meanwhile. With a smart contract in the BC setting, a smart contract would be a script embedded into the BC itself. This would give each smart contract a unique address corresponding with the block the contract is stored upon and could be executed when a transaction occurs on the associated block. Executing a smart contract associated with a block would allow the transaction to be seen across the network by every node on the network, allowing the BC network to act as a distributed record of the transaction [7, 8, and 16].

Smart contracts are useful in that they allow general purpose computations to occur in tandem with the BC. However, these smart contracts excel when they are implemented into managing data-driven interactions between entities on the network. Additionally, the contract is visible publically to the network [7]. As the code resides on the BC, the contract can be inspected by every node associated with the BC as well. This bodes well with the cryptographic basis behind the BC system as all network participants can view a secure and traceable path of each transaction that occurs on the contract, much like how each block on the BC can be easily verified.

A BC that supports a digital transaction is especially important as it allows transactions to occur between parties that do not trust each other. A BC supporting smart contracts takes this notion even further by allowing multiple interactions to occur between the mistrusted parties [27]. The transacting parties can identify the code and terms associated with the contract and have verifiable proof that the contract is legitimately hosted due to the constraints of the network. Additionally, the need for each signature to be digitally signed by the correct parties promotes the verifiability between the correct transacting parties [7, 9]. This eliminates any doubt about the legitimacy of the terms discussed in any particular contract and proves that each party willingly accepted the terms and conditions laid out by a smart contract before engaging with it. A smart contract operates anonymously from any single source with the behavior and terms of the contract being clearly viewable from the start. This proves especially important in multi-party and multi-contract deals. With full authoritative trust being based on a single autonomous and easily verifiable set of constraints, smart contracts can be trusted to carry out the limited scope of each individual contract or pass along instructions to a chain of contracts as an autonomous and trusted middleman that is not influenced by any involved party [16, 27].

Finally, another strength of the smart contract model relies on the concept of “decentralized autonomous organizations” (DAOs) whose behavior can be modified based upon the constraints of the contract being met [27, 29, and 32]. Such an example would be would be a series of contracts linked together that point at a primary address with which to include in the chain of contracts. If several financial institutions offered contracts with variable rates, a rule can be included to point a currency exchange contract towards the address of the financial institution offering the best rate at the given time. This contract may wind up pointing at a different address several times in a day or even within a few seconds [10, 13].

4. BLOCKCHAIN CATEGORIZATION

A BC network’s main benefit relies on the ability of the network to be optimized for a task according to several categories regarding the network’s usage. The most important of note is [7, 9, 23, 27, 29, and 34]:

- Who can access the network? While a public network may be suitable for applications such as bitcoin, where the currency’s strength is in its availability. The problem arises with the security concerns and inflationary procedures that must be accounted for. Events such as the Sybil attack [14] in the early days of bitcoin have proven that a consensus in public networks is costly and that incentive must be given to the miners on the system for the raw computing power they donate [27, 29]. On the flipside, private networks offer much more control than their public counterparts. Private networks can be whitelisted to allow on authorized parties access to the network, ensuring a more regulated environment with a more manageable throughput that is ideal for stakeholders of the tech.
- Who can transact on a network? While a party may be able to join a network, the power to transact, deploy smart contracts and mine blocks on the network can be whitelisted only to verified parties [23]. This is much more practical on a private network where only certain individuals are recognized and assigned permissions accordingly.
- Transaction style model vs contract based model? BCs that support a transaction based model are ideal for the tracking and transfer of digital assets while BCs supporting the contract based model provide a means to run multistage processes including logical constraints and data manipulation right on the chain. Unfortunately the main drawback behind a contract based model becomes the speed cost at which the network operates. A transaction style model easily identifies its inputs and outputs before execution leading to quicker speeds and the ability to process noncompeting blocks all at once. On the other side, having to declare the clauses of a contract and identify the affected linked contract clauses in any associated chains, the contract based model loses the ability to run contract blocks concurrently. Regardless of the model style used, the BC network still provides some key benefits over the traditional system from the start [34].

- A peer to peer system that is distributed and resilient to failure at a single source.
- A network that identifies conflicts and automatically routes the chain of blocks to converge into a single designated and easily viewable path.
- Trust in the verification and security afforded by the easily viewable system by which verification is performed [32].
- Eliminates the possibility of disputes as each transaction has a public record of proof.
- Trustless communications through a secure source in a predictable fashion.

5. THE INTERNET OF THINGS

5.1 Overview of IoT

The Internet of Things (IoT) has had a variety of definitions over the years. They all have one theme in common, the idea of connectivity. Broadly, IoT consists of all devices that are able to collect data, interact with its environment, can be uniquely identifiable. All of these data collecting devices are connected to the internet in order to share their data and interact with the user [35]. There are many components when it comes to IoT devices. Because of the lack of their computing power and storage space, these devices need to rely more on advanced software. Some of these components include, but are not limited to, sensor, actuator, computing software, and network and connectivity software. All of these devices need to communicate/help each other through a set of connectivity protocols such as HTTP/REST, MQTT, CoAP, AMQP and XMPP [36]. These protocols all have certain standards they need to meet in order to communicate efficiently.

Manufactures are shipping these devices to customers knowing they impose a security threat, and software patches have shown to be cumbersome and ineffective [36]. Problematically, IoT devices are often designed with security as an afterthought instead of as a core feature. Many cheap devices are being sold with no security features at all. Consequentially, malicious actors are taking advantage of these vulnerabilities to attack devices, causing damage to individuals and companies. Other common problems arise through the negligence and quality of the devices. The purchaser usually leaves login credentials for their devices at factory settings. This lowers the privacy of the device as the username and password used wouldn't be strong enough. Most company has their fixed login credentials which cannot be modified by the consumer [36].

5.2 IoT Architecture

There is an assortment of opinions on the number of layer in the architecture of IoT. However most agree that are three primary layers which are defined by their function and the device that they are used. A typical IoT system has three layers perception, network, and application [37]. Figure 2 illustrates three-layer IoT architecture. The perception layer gathers information from the environment using sensors and carries out node collaboration. This layer also includes actuators and controllers that can make actions on the environment. After the information is obtained the perception layer transfers it to the network layer. The network layer serves in the filtering and data transmission from different sensors. Data routing and transmission to the hub and devices are conducted at the network layer. Switching and device routing is also a part of its function. Technologies such as 4G, 5G, RFID, Zigbee, and Wi-Fi are employed at this layer. The application layer is basically the finished product. It assures confidentiality, integrity and authenticity by making sure that it’s specific to the user. Data storage and other IoT services belong to this layer [37].Even though it may seem like a fairy simple task to achieve; there are still obstacles to overcome. Each layer is vulnerable to threats and attacks. Some threats in the perception layer consist of wireless signal strengths, which can be compromised by disturbing waves. Another threat is physical attacks since IoT nodes are located in the environment they can be tampered with. Traffic analysis and the diversity of network components/protocols have been security concerns within the network layer. The diversity of components allows devices to become vulnerable to DoS attacks and it also allows for manipulation of the devices [36, 37]. The application layer lacks policies and standards regarding the interaction and development of applications [37].

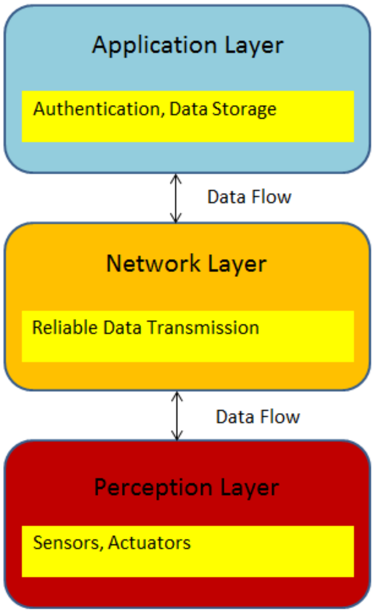

FIGURE 2: Three-Layer IoT Architecture.

6. BLOCKCHAIN AND INTERNET OF THINGS INTEGRATION

The case for a shift towards the decentralized architecture of the IoT provides some striking similarities with the evolution of BC technology [27]. The current model of IoT technology relies on a centralized source for all updates and communications that proves to be difficult to both scale and maintain accordingly. The trust between the users and their IoT devices is not overly transparent leading to issues of trust between the consumer and manufacturer as to the status of updates and data distribution [27]. One approach to the problem has been the proposed use of a BC system which smartly solves many of the problems with the current system [27]. When we think about the implementations of an IoT BC network, the idea of a decentralized contractual network comes to mind. A manufacturer would create a smart contract that allows them to store a link to the latest firmware update on their network. The device would then connect to the BC network either by being preprogrammed or discovering the network and would query the contract for the latest firmware update. The link could lead to a distributed peer to peer file sharing network, which would allow the device to then download and apply the update. The original nodes would have to originate directly from the manufacturer; however, after a certain amount of propagation, the manufacturer would no longer need to host the contract from their own node. This would also ensure that older devices connecting to the network are still able to download the updates even if the manufacturer is no longer broadcasting them [24, 25].

Taking this one step further, a payment layer could be added onto the process of distributing the update. Some BC networks such as Filecoin [26] and EtherAPI [27] make it possible to rent file space and accept a token of cryptocurrency in exchange for completing an information request. Every device on the network is capable hosting their own file link's creating a marketplace for the associated usage fees and promoting the storage and availability of niche, outdated or custom software.

A prime example of the marketplace for micro transactions is the facilitation and sharing of services and property through Slock.it [28]. Slocks are electronic locks that connect to the Ethereum BC [27, 29] through the use of smart contracts. When a person wishes to rent out their home or other property, token can be exchanged on the Ether network that unlocks the Slock for a certain agreed upon rental amount of time. This whole process is made simple through the use of the Ether network as each transaction is signed and communicating on the same BC [30].

There are many cases of IoT-BC applications including smart home, smart grid, health care energy, management systems, and supply chains.

6.1 Smart Home Case

The main motives for using IoT devices in the home are to improve safety, power efficiency and comfort, convenience, health, and assist seniors and the disabled [36]. As IoT devices become more prevalent in smart homes and being a trustworthy source for the people and a container for their important data and information, it is imperative to emphasis on the security and privacy aspects. The authors of article [38] outlined three types of threats identified by BC that affect smart home IoT. The first threat prevents the user from accessing services. The second threat involves the hackers attempting to identify themselves as the user. In the third threat the hacker uses public records and transactions to become familiar with the user and his lifestyle with the intention of impersonating the user. Weighing these risks allows us to acknowledge that principles of cybersecurity must be in place. A proposed solution is to use BC and smart contract technologies to counter these issues [39].

The BC approach is the decentralization of service for IoT in the smart home. BC controls and secures the operation of smart homes. BC has three main components; transparency, security, and privacy [39]. Cryptography is used greatly, which plays a role in authoritativeness behind any interactions within a network [39]. If this can be included and added to IoT devices, especially those of smart homes, then personal and sensitive data can be secured and protected [39].BC uses several types of transactions between nodes/devices to link transactions between two devices or customers BC uses the IL (immutable ledger) [38]. The main player in BC IoT smart home is the miner, a resourceful stand-alone or built in device connected to control and support the incoming and outgoing transactions and can be used to integrate the homes internet gateway. The miner authenticates, authorizes, and provides auditability of the transactions [38]. A shared key, under the control of the miner, takes permission from the owner and secures communication between home devices.

IoT is incompatible with the original BC due to high bandwidth, overhead, and excessive delays [38]. To deal with that, a lightweight BC for IoT eliminating the classic BC overhead while keeping most of the security measures and privacy. Users can share the service their devices offer with other houses after verification with a public and private key [39]. The authorized homes can then share data through a public BC [39]. Also with the use of a smart contract, the home devices can carry out commands without any other authoritarian requirements. The smart contract can be appropriate for user behaviors with low computation costs [39].

7. DISADVANTAGES

Although the idea of a completely decentralized network seems promising, several considerations must be taken into effect regarding the implementation of IoT technology in tandem with a BC network [13, 27].

Compared to a traditionally configured database, a decentralized peer-to-peer BC model will generally underperform in regard to transactions processed. This decrease in performance is especially prevalent in publically BC networks which must employ a proof-of-work concept in order to maintain security and promote transaction volume across the network. Although new BC solutions which seek to solve this problem are popping up such as in the Ethereum project, the proof-of-work mechanism is a necessary step to ensure the resilience and trustless decentralization of the network as a whole [30, 31].

Maintaining privacy on a network also remains a complicated issue overall. As each device is linked to a public key, each participant does not need to know the identity of every other key on the network, only the keys of the parties with which they are interacting [27]. A user on a public network can create a large number of public keys for each separate transaction. Since all public keys are linked to a private key, the outward facing address can be changed with each transaction processed in order to protect the identity behind a transaction on an account. Unfortunately, since a new address needs to be created for each separate transaction, this workaround may prove to be more time-consuming and resource intensive when utilized on IoT devices [27, 38, and 39].

A main concern with the transition towards the use of smart contracts is the concept of legal enforceability [32, 33]. While the technology exists in the digital world to verify the transactions in real time, the legal system may be slow.

Another concern is the matter of incorrectly or poorly written smart contracts that do not perform as expected. A smart contract set up to receive fund and distribute funds may act accordingly until an odd amount or invalid input is received and not managed for. This may result in an incorrect amount of funds being stored and distributed by the contract forcing an incorrect transaction that could cost unforeseen amounts in damages [34].

Also another concern is the real-world value of the cryptocurrency market as a whole. While fluctuations in currency prices certainly affect transactions daily, apart from depression level swings, the fluctuations are manageable to deal with daily. In the world of cryptocurrency, the smaller market cap value of an asset means that the real-world value of a cryptocurrency can change quickly. This can greatly impact affected contracts [11, 16].

Finally, with the rise of IoT products comes an entire new entrance way for attackers to get to information by using the devices to their advantage. Given the fact that these products are in a new industry, they lack the basic framework to make them secure. These devices are susceptible to a variety of attacks from hackers [36, 37]. An attacker can easily scan these devices, locate open ports and take control of a device due to lack of authentication verification and framework. An attacker can use this to steal personal information such access accounts or credit cards, or they can even take control of the device [35, 36].

8. CONCLUSION

IoT products were made to make people's lives easy and more comfortable, but they have had their negative effects on security and privacy. The applications of IoT and BC as separate technologies are broad; however, combining these technologies can prove to be very powerful. BCs allow for resilient, truly distributed peer-to-peer networks. The distributed/decentralized nature of a BC appears to be the perfect fit for the growing IoT. Smart contracts are useful in that they allow general purpose computations and automation to occur in tandem with the BC. This paper explored how BCs, smart contracts, and IoT can be used together while identifying current implementations (smart home case) and their associated pros and cons.

9. REFERENCES

[1] P. Treleaven, R. Brown, and D. Yang, ‘‘Blockchain technology in finance,’’ Computer, no. 9, pp. 1 4–17, 2017.

[2] Michael Casey, “The Impact of Blockchain Technology on Finance: A Catalyst for Change,” International Center for Monetary and Banking Studies, 2018.

[3] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, “Blockchain technology in healthcare: A comprehensive review and directions for future research,” MDPI, Applied Sciences, vol. 9, no. 9, p. 1736, 2019.

[4] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016.

[5] S Ølnes, J Ubacht, M Janssen, “Blockchain in government: Benefits and implications of distributed ledger technology for information sharing,” Government Information Quarterly, An

International Journal of Information Technology Management, Policies, and Practices, Elsevier, 2017.

[6] S. Ølnes and A. Jansen, "Blockchain technology as infrastructure in public sector: an analytical framework", in Proc. of the 19th ACM Ann. Int. Conf. on Digital Government Research.: Governance in the Data Age, Article no. 77, pp. 1-10, 2018.

[7] Z Zheng, S Xie, H Dai, X Chen, H Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," 2017 IEEE international congress on big data (Big Data congress), pp. 557-564, 2017.

[8] T. Ahram et al, "Blockchain technology innovations," 2017 IEEE Technology & Engineering Management Conference (TEMSCON), 2017.

[9] P. Tasca, C. Tessone, "Taxonomy of Blockchain Technologies. Principles of Identification and Classification," arXiv preprint arXiv:1708.04872, 2017.

[10] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[11] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc., 2014.

[12] G. Greenspan. (2015). Ending the Bitcoin vs Blockchain Debate. [Online]. Available: https://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/.

[13] X. Wang, et al, "Survey on blockchain for Internet of Things," Elsevier, Computer Communications 136, pp. 10-29, 2019.

[14] J. R. Douceur, ''The Sybil attack,'' in Peer-to-Peer Systems (Lecture Notes in Computer Science). Berlin, Germany: Springer, Mar. 2002, pp. 251–260. [Online]. Available: http://link.springer.com/ chapter/10.1007/3-540-45748-8_24.

[15] National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)," 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

[16] U. Mukhopadhyay, et al, "A brief survey of Cryptocurrency systems," IEEE 14th Annual Conference on Privacy, Security and Trust (PST), 2016.

[17] Myriad, "A Coin for Everyone, " [Online]. Available: https://www.myriadcoin.org/.

[18] Ripple, accessed on Mar. 15, 2016. [Online]. Available: https://ripple.com/.

[19] D. Schwartz, N. Youngs, and A. Britto, ''The ripple protocol consensus algorithm,'' Ripple Labs, Inc., San Francisco, CA, USA, Tech. Rep., 2014. [Online]. Available: https://ripple.com/files/ ripple_consensus_whitepaper.pdf.

[20] A. Hossein and N. Krichene, (2016). 100 PERCENT RESERVE BANKING AND THE PATH TO A SINGLE-COUNTRY GOLD STANDARD. Quarterly Journal of Austrian Economics 19, no. 1: 29-64. Business Source Premier.

[21] N. Szabo. (1994). Smart Contracts. [Online]. Available: http://szabo.best.vwh.net/smart.contracts.html.

[22] N. Szabo. (1997). The Idea of Smart Contracts. [Online]. Available: http://szabo.best.vwh.net/smart_contracts_idea.html.

[23] L. Kan et al, "A Multiple Blockchains Architecture on Inter-Blockchain Communication," IEEE

International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2018.

[24] A. Yohan, N. Lo, S. Achawapong, “Blockchain-based Firmware Update Framework for Internet-of-Things Environment,” Int'l Conf. Information and Knowledge Engineering , IKE'18, pp 151-155, 2018.

[25] X. He, S. Alqahtani, R. Gamble, M. Papa, “Securing Over–The–Air IoT Firmware Updates using Blockchain” ACM, Int'l Conf. on Omni-Layer Intelligent Systems (COINS), 2019.

[26] Protocol Labs, “Filecoin: A Decentralized Storage Network,” whitepaper, 2017 [Online]. Available: https://filecoin.io/filecoin.pdf.

[27] K. Christidis, M. Devetsikiotis , “Blockchains and smart contracts for the internet of things,” IEEE Access, Vol. 4, pp. 2292 – 2303, 2016.

[28] Slock.it—Blockchain + IoT, [Online]. Available: https://slock.it/faq.md.

[29] N. Atzei, M. Bartoletti, T. Cimoli, “A Survey of Attacks on Ethereum Smart Contracts (SoK),” International Conference on Principles of Security and Trust, Lecture Notes in Computer Science, vol 10204. Springer, pp. 164-186, 2017.

[30] Ethereum Frontier, [Online]. Available: https://www.ethereum.org/.

[31] Z. Li et al,“Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things,” IEEE Transactions on Industrial Informatics, Volume: 14 , Issue: 8 , pp. 3690 – 3700, 2018.

[32] Kevin Werbach, “Trust, but verify: Why the blockchain needs the law,” Berkeley Tech. LJ, Volume 33, Pages 487-550, 2018.

[33] Kevin Werbach, “The blockchain and the new architecture of trust,” MIT Press, 2018.

[34] Introduction to Smart Contracts—Solidity 0.6.5 Documentation, [Online]. Available: https://solidity.readthedocs.io/en/v0.6.5/introduction-to-smart-contracts.html.

[35] F. Restuccia, S. D’Oro, , and T. Melodia “Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking,“ IEEE Internet of Things Journal, Vol. 1, No. 1, pp. 1-14, 2018.

[36] D. Bastos, M. Shackleton, and F. El-Moussa, “Internet of things: A survey of technologies and security risks in smart home and city environments,” in Proc. Living in the IoT: Cybersecurity . IoT-2018, pp. 1–7, 2018.

[37] T. Yousuf, R. Mahmoud, F.Aloul, and I. Zualkernan “Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures,” International Journal for Information Security Research (IJISR), Volume 5, Issue 4, pp. 608-616, 2015.

[38] M. AbuNaser and A. Alkhatib “Advanced survey of Blockchain for the Internet of Things Smart Home,” 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 58-62, 2019.

[39] Y. Zhou et al, “Improving IoT Services in Smart-Home Using Blockchain Smart Contract,” 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, pp. 81-87, 2018.