Future of the Internet of Things Emerging with Blockchain and Smart Contracts

Mir Hassan[1], Chen Jincai[2]
Wuhan National Laboratory for Optoelectronics
Huazhong University of Science and Technology
Wuhan, China

Adnan Iftekhar[3], Xiaohui Cui[4]
Key Laboratory of Aerospace Information Security
and Trusted Computing, Ministry of Education
School of Cyber Science and Engineering
Wuhan University, Wuhan, China

***Abstract*—The Internet of Things (IoT) has the potential to change the way the world works from home automation to smart cities, from improved healthcare to an efficient management system in supply chains to industry 4.0 revolution. IoT is increasingly becoming an essential part of the homes and industrial automation; nevertheless, there are still many challenges that need to fix. IoT solutions are costly and complicated, while issues regarding security and privacy must be addressed with a sustainable plan. Support the growing number of connected devices; the IoT is in dire need of a reboot. Blockchain technology might be the answer. Starting as a decentralized financial solution in the form of Bitcoin, Blockchain technology has expanded to diverse areas and Information Technology applications. Blockchain technology and Smart Contracts can address the outstanding security and privacy issues that impede further development of the IoT. Blockchain is a decentralized system with no central governance, facilitates interactions, promotes new and improved transaction models, and allows autonomous coordination of the devices using enhanced encryption techniques. The primary reason for this paper is to showcase the challenges and problems we are facing with the current internet of things solutions and analyze how the use of Blockchain and Smart Contracts can help achieve a new, more robust internet of things system. Finally, we examine some of the many projects using the Internet of Things together with Blockchain and Smart Contracts, to create new solutions that are only possible by integrating these technologies.**

***Keywords*—Internet of Things (IoT); blockchain; smart contracts; peer-to-peer security**

I. Introduction

The Internet of Things is a development of portable, home, and installed applications that are being associated with the web incorporating the more prominent computational abilities and information investigation to scramble important data on the internet. Numerous gadgets are presently associated with the web and, later on, several billions of gadgets. As related gadgets associate, they can turn into a canny arrangement of frameworks; When these keen gadgets and techniques for frameworks share and examine information over the cloud, they can fundamentally change our organizations, our lives, and our reality in interminable ways. They enhance therapeutic results, make better items quicker with lower advancement expenses, and make shopping progressively agreeable, or by upgrading vitality age and utilization [1]. Smart devices are monitored from every aspect of usage as they perform their work efficiently. Imagine a brilliant device, for example, a shrewd traffic camera; this camera can screen the road for an obstruct, mishaps, and climate conditions and imparts that status to a portal that joins it with information from different cameras, making a wise citywide transportation framework. [1]

Envision that this smart traffic framework is associated with other citywide traffic frameworks. That whole astute traffic framework is related to another citywide transportation framework that gets information from their very own keen gadgets, making a much progressively extensive system of frameworks. On the off chance that a city's astute traffic framework recognizes huge clog because of a mishap, at that point, that understanding can be sent to the citywide transportation framework, that can examine the effect of the disaster on other city frameworks. Perceiving that the disaster is close to the airplane terminal and two city schools, the framework could tell those different frameworks so they can change flight and school plans. Such a keen city framework additionally breaks down and determines ideal courses around the mishap and sends directions to the computerized signage frameworks to control drivers around the disaster. That is only one case of the potential advantages that can happen when canny gadgets share bits of knowledge with different frameworks, shaping consistent extending systems of frameworks.

In the IoT, different devices independently trade relevant data, focusing on data streams to enhance our life, further obscuring the limits between the digital and the physical universes [2]. Unfortunately, the Internet of Things faces challenges to perform with performance efficiency.

In the following section, an existing Blockchain and Smart Contract technology are introduced with which we can overcome these challenges mentioned in Section 1. Then, in Section 3, we take a look on how the blockchain and smart contract technology can help take IoT forward and analyze the already existing projects and experiments that are using these two technologies side by side to make the IoT world more safe, secure, affordable and more accessible.

II. Challenges for the Future of the Internet Of Things

The development of this captivating innovation has additionally made difficulties that can't be unraveled by utilizing advances intended for the conventional web. Beating these difficulties, in any case, is a determining factor that may decide if the IoT will result in the long run win and to what degree. Some prominent challenges for the Internet of Things present

[1]hassanmir@hust.edu.cn

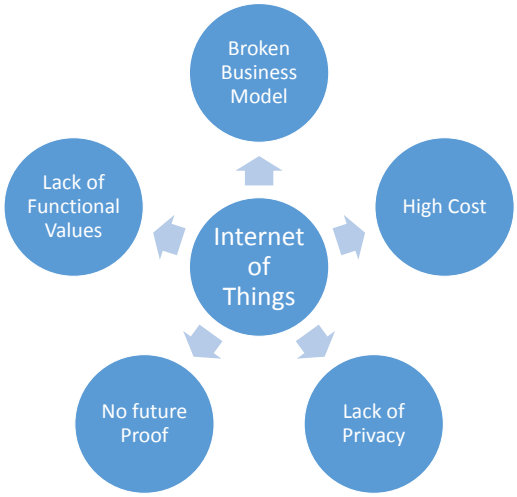

Fig. 1. Challenges for Internet of Things

in Fig. 1. IoT solutions require a high cost in the deployment of infrastructure to enhance the privacy and security of data. Unfortunately, they have no future proof of protected data due to public authorities' functional values in their business model.

A. The Cost of Connectivity

The high cost of extensive infrastructure and maintenance associated with large server farms and centralized clouds result in prohibitively expensive IoT solutions. It is unlikely that companies will have the right profit margin because of several years of support and maintenance required for even the cheap IoT devices. This cost of serving and supporting billions of smart devices - even something as simple as maintaining servers and releasing software updates [3]. According to the survey report IoT application cost high in the U.S. [4] for developing in a different field.

B. The Security and Privacy Challenges

Most IoT solutions these days are provided by centralized authorities, whether it is government, manufacturers, or service providers. It can allow these authorities to gain unauthorized access to collect and analyze user's data. Closed source (often described as security through obscurity) approaches are being built in the current system. However, these solutions are obsolete, and the newer path of open-source (security through transparency) is required to scale IoT to the next level. Although the open-source systems may be susceptible to exploitation and accidents, it is unlikely for governments or other targeted institutions to collect unauthorized users' data.

C. The Sustainability Challenge

Among information communication technologies involved in the Smart Cities movement, IoT is believed to be an essential method, especially in the field of sustainable development. Since the application of IoT is deeply integrated into Smart Cities, which serves as a paradigm for the development of IoT technology, planners should be able to link smart Cities to the concept of sustainability. The APA Smart Cities and sustainability Initiative views Smart Cities as an extension of sustainability in that Smart Cities aims to maximize the benefits for most people with minimal costs and impacts, which reflects the very goal of sustainability.

III. Blockchain and Smart Contract

A decentralized way to deal with IoT systems administration can explain the inquiries brought up in the last segment. The appropriation of an institutionalized shared correspondence model to process the several billions of exchanges between devices will altogether lessen the expenses related to the establishment and upkeep of vast concentrated server farms and conveyed calculation and capacity needs to disseminate more than billions of devices that frame IoT systems. It keeps the disappointment of any single hub in a network from backing off the whole system. The blockchain technology is a potential candidate to organize and control it in a decentralized manner as ilustrated in Fig. 2.

A. The Blockchain Technology

Blockchain, an underlying technology powers bitcoin. It was the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. Blockchain technology has created the backbone of a new type of internet by allowing digital information to be distributed but not copied. The tech community is now finding other potential uses for this technology, such as connecting systems in the IoT world [5].

The network of untrusted nodes maintains the transactions of distributed ledger is called a blockchain. Every block of the blockchain contains a rundown of transactions sorted out in a Merkle tree; new blocks are added to the blockchain. Blockchains are frequently called a majority rule approach to keep transactions as they depend on accord to confirm transactions and do not require a central authority. We recognize two types of blockchains: public blockchain and private blockchain [6].

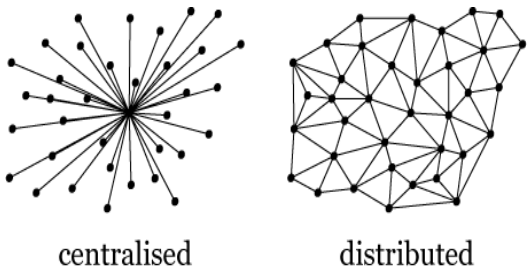

Fig. 2. Centralized and Distributed Network

B. Public and Private Blockchain

A public blockchain network is entirely open, and anyone can join and participate in the system. The network typically has an incentivizing mechanism to encourage more participants to join the network. One of the drawbacks of a public blockchain is the substantial amount of computational power that is necessary to maintain a distributed ledger on a large scale. More specifically, to achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of work to ensure all

are in sync. Two well-known implementations of this kind of blockchains are Bitcoin and Ethereum. [7]

A private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter. Businesses who set up a private blockchain will generally set up a permission network. It places restrictions on who is allowed to participate in the network, and only in certain transactions. Participants need to obtain an invitation or permission to join. A well-known implementation of this type of blockchain is IBM's Hyperledger.

C. Blocks in the Blockchain

Every block is a structure of a header and a body. The header incorporates the hash values of the previous, current, and nonce block. The block information is locked into the database utilizing the index method illustrated in Fig. 3). Since the hash values stored in each peer in the block are influenced by the benefits of the previous blocks, it is challenging to falsify and alter the registered data. In spite of data, alteration is possible if 51 percent of peers are hacked at the same time, the assault situation is convoluted.

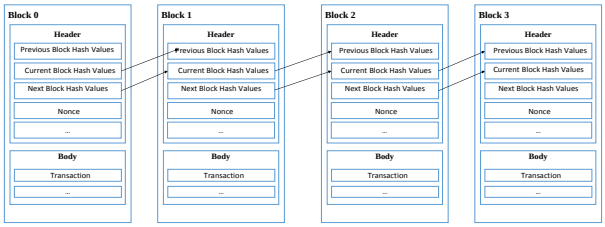

Fig. 3. Blockchain Connection Structure

D. Block Mining

Block Mining is the system that permits the blockchain to decentralize security. It anchors the bitcoin framework and empowers a system without a central authority. Miners will approve new transactions and record them on the worldwide ledger also known as Blockchain. In Bitcoin Blockchain, a block (the structure containing transactions) is mined every 10 minutes interval. Miners compete to resolve a problematic mathematical problem based on a cryptographic hash algorithm. The solution found is called the Proof-Of-Work. This proof indicates that a miner spent a lot of time and resources to solve the problem. As an incentive, Miners who tackle a cryptographic riddle are compensated with bitcoins or transaction fees [8].

E. Transaction Processing Lifecycle

The Fig. 4 is explaining the transaction processing lifecycle. It is a set of multiple processes. In the blockchain, someone initiates an operation. The transaction is then broadcast to all nodes of the blockchain. The miners validate and verify the transaction; 51 percent of the miners in the blockchain have to approve the transaction for the transaction to be added on the block. Once the new block is mined by miners, the blockchain is added to the existing Blockchain, thus making the transaction complete and permanent.

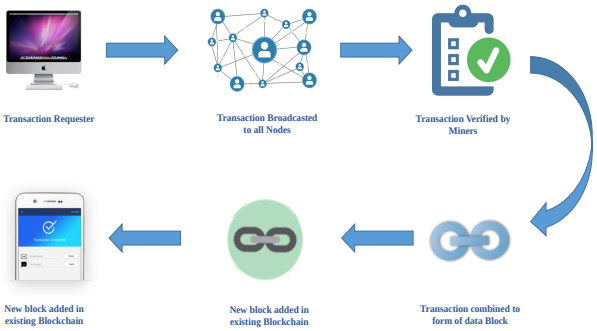

Fig. 4. Transaction Processing Lifecycle

F. Smart Contracts Structure

The initial release of smart contracts in Ethereum was intended to give parties who do not trust each other away to conclude an agreement, where they can be confident that the transaction will take place as they intend, and where they can verify the status of the contract or transaction at any time illustrate in Fig. 5. The initial strategy to achieve these design goals smart contract implementation did not follow the typical pattern for the development of the application. In particular, it included the logic, properties, and data in one package, substantially disintegrate the layers of business and data logic layers into a single layer, Then they were written to the blockchain. That provided immutable, deterministic execution, and the transparency required in untrusted environments.

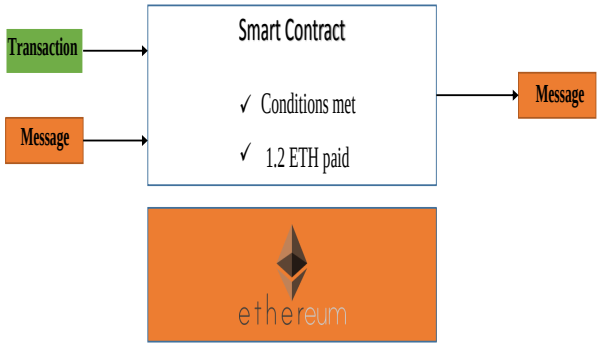

Fig. 5. Smart Contract Structure of Ethereum

G. Blockchain Benefits

Blockchain can revolutionize many industries including banking, education, voting healthcare, and supply chains. Blockchain's key benefits can be defined as:

1) Decentralization: Lack of a central data hub is one of the main reasons why blockchain is so exciting. Individual transactions in the blockchain have validity. Nodes are authorized to enforce constraints. The information in the blockchain is distributed throughout the world on different nodes so that

it is near to impossible for an attacker to corrupt the stored data.

2) Efficiency: There is no involvement of intermediaries to carry out the transactions in a blockchain; it is done directly between the two parties. The digitized information allows the prompt process time of a transaction. Adding in the Smart Contracts functionality means that an action is automatically triggered when the established criteria of the contract are satisfied. This reduces the time and the cost of processing transactions.

3) Auditability: Every transaction of the blockchain is recorded in a permanent sequence. This inerasable record of transactions provides the complete audit trail for the life of an asset. This is essential especially in the cases where there is a need to verify the authenticity of an asset.

4) Traceability: With blockchain, it is possible to track the lifecycle of a product, from the manufacturer to the consumer. It is very advantageous to track goods and find out whether the products are counterfeit or real. With blockchain, it is also possible to transfer the ownership of certain goods or products from one person to another. There is no need for a paper trail. For example, a transfer of ownership of car, land, house and many more, can be done within the blockchain without the need for paperwork and intermediaries involved.

5) Transparency: Lack of transparency in a commercial organization or other business entities can sometimes lead to distrust, work delays, and loss for the company as well as consumers. By providing complete transparency regarding transaction details of the commercial relationship, further trust and stability can be developed among the parties based on openness rather than negotiation.

6) Security: The authenticity of the information stored in the blockchain can be assured because multiple nodes of the network verify the transaction using cryptography. Most significant keys to unlock the benefits of the Internet of Things is the assured information, in an autonomous process that links actions to assets.

IV. Emerging IoT with Blockchain Technology

Emerging blockchain technology can be used to improve the security of IoT applications in health care, smart cities, energy grids, public safety, education, supply chain management, education, and other application areas. Some of them use cases, where blockchain technology can benefit IoT, are discussed below:

A. Public Health – Counterfeit Drugs

The distribution and production of counterfeit drugs is a vital and pressing worldwide issue. According to the WHO, currently, in developing countries, the delivery of counterfeit drugs is may be up to 30 percent whereas 10 per cent of all drugs in the world are counterfeit. By using blockchain and IoT elements, the spread of counterfeit drugs can be controlled. Legal drug can be stamped physically at the location of production and an identifier to the stamp can be recorded into the blockchain ledger. Forged drugs can be identified, traced, and eliminated easily because they will not have any record in the blockchain system [9]

B. Smart City – Smart Homes

In today's world, a home can be a powerful computer, with a plethora of household devices related to home security systems (alarms, surveillance cameras, door locks etc.), environmental control (Air conditioner, sensors), home entertainment (audio/video equipment), and household electronics (electronic lights, refrigerators, dishwashers, washing machine, etc.) are present. All these smart home devices allow homeowners to observe and control their home from a remote site. The information coming from the network of devices is first sent to a central server and only then presented to the homeowner on their cell phones, tablets or computers. It is vital to secure this information so attackers cannot use this information. The central server or gateway is not as secure as the blockchain. Privacy and security of smart home systems can be achieved by using blockchain. The communications between devices and control information of the devices can be recorded in the distributed ledger as transactions. Cryptography and hashing functions can protect the confidentiality, integrity, and authenticity of the network of the network of IoT as well as with the addition of time-stamp and proper encapsulation, robust security is ensured.

C. Software Updating of IoT Edge Nodes

Edge devices in an IoT network have low, medium, and high levels of computing power. Due to the increase of system-on-a-chip capabilities, edge devices are becoming smarter. Some large appliances like a refrigerator can be equipped with a powerful computing system whereas a small sensor might have a little chip having adequate computing power. Thus, if all the devices in the network have some form of computing power, the functionality of the devices can be reconfigured easily. Such devices can form peer-to-peer networks and can directly communicate with each other to share IoT service functions. Device parameters are related to functionality, and device management can be downloaded and updated periodically.

D. Supply Chain Management – Smart Supply Contracts

The manufacturers create goods and services and deliver it to the retailer under the rules written in the contract. Such interactions begin with inquiries from the buyer, which leads to contract negotiation between a seller and a buyer. The shipping process begins once the contract is signed. This may involve the use of a local shipping agency, local port of exit, customs officials, a distant port of entry, carriers, customs services, a remote delivery agent, and finally the customers.

At every stage, a sequence of messages and acknowledgments is activated culminating in the customer acknowledging receipt of the shipment. Currently, trading policies on national and international trade provide payment detail process to the supplier. This adapted chain of events is well suited for using blockchain technology for smooth, verifiable, and secure supply chain management. It is possible to record and verify all documents and activities at each stage by entering transactions into or querying the appropriately distributed ledger.

Adoption of blockchain in the IoT space can change the way IoT edge devices exchange data in a trustworthy mechanizing environment and encoding transactions while

safeguarding data exchanges and ensuring the security of all devices involved.

V. Case Studies of Blockchian IoT Platforms

We will explore some of the projects that are already combining Blockchain Technology and Internet of Things to develop new and viable solutions to existing problems:

A. Slock.it

Slock is where blockchain meets IoT. It is a decentralized platform for renting/selling your physical goods. Airbnb apartments become fully automated; parking spots can be sublet on demand, vehicles can be sold or rented without the involvement of any intermediaries. Slock.it bridges the physical world and the blockchain by making smart contracts enforceable: Slock.it has the potential to be the future infrastructure of a sharing economy [10].

B. Filament

Filament builds blockchain hardware, IoT and software solution. The distributed blockchain capabilities of Filament leverage open protocols so that devices can process and record transactions independently ensuring digital trust. The filament built a Blocklet Chip and new trusted application software, currently in beta, designed to communicate with multiple blockchain technologies natively. A secure distributed ledger solution is achieved through its software, and the block chip will allow corporations and enterprises to streamline the process of extracting the value of recording, monetizing data assets on the sensors themselves [11].

C. Skuchain

Skuchain is a blockchain technology company catered to the B2B trade =and supply chain finance market. The company aims to solve problems in the USD 18 trillion global finance market, an industry that still relies mostly on paper for many processes [12].

D. Blockchain of Things

Blockchain of Things created Catenis Enterprise to facilitate developers and organizations who wish to integrate Bitcoin blockchain capabilities into their devices quickly, be systems, software, machines, sensors, and other enterprise scale applications. The Catenis provides a layer that removes technological difficulties and delivers ease of use enhancements via standard web services for systems messaging and end node security. The Catenis allows organizations to rapidly leverage the bitcoin blockchain for enhanced security and reduced cost for global messaging and device communications. Clients can quickly generate a vast number of Catenis virtual devices. These virtual devices correspond to software applications and real-world physical systems in use [13].

VI. Conclusion

The Internet of Things integrated with blockchain will allow you to live in a smart home, drive smart cars and practice smart medicine. In this emerging world with technology, users connect with smart devices using secure identification and authentication, potentially public/private keys, and they define the rules of engagement, such as privacy, with other devices, rather than going along with the laws of a centralized node or intermediary. Manufacturers can transfer ownership, maintenance, access, and responsibility to a community of self-maintaining devices, future-proofing the IoT and saving infrastructure costs, replacing each equipment exactly when it hits obsolescence. Blockchain and IoT are twin technologies that can benefit from each other. They represent the most significant technological disruption since the usage of processing transaction systems in computing. The significant delipment of devices and software, it is conceivable to convey transaction processing and intelligence to all devices. Although there is some critical adaptability, challenges with the distributed systems, many researchers, institutions, individuals are working tirelessly to solve these issues and build an open source foundation for the development of this technology.

Acknowledgments

The Authors would like to acknowledge the support provided by the National Key R&D Program of China (No.2018YFC1604000).

References

[1] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[2] K. Ashton *et al.*, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[4] H. Singh, "Hemendra singh," Jul 2019. [Online]. Available: https://customerthink.com/how-much-does-it-cost-to-develop-an-iot-application/

[5] M. Walport *et al.*, "Distributed ledger technology: Beyond blockchain," *UK Government Office for Science*, vol. 1, 2016.

[6] M. Swan, *Blockchain*. O'Reilly Media, 2015.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," pp. 557–564, June 2017.

[8] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 254–269.

[9] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proceedings of the 2016 ACM Conference on Economics and Computation*. ACM, 2016, pp. 365–382.

[10] "Slock.it, "enabling the economy of things" 1 january 2015. [online]. available: https://slock.it/. [accessed 2 december 2018]."

[11] "Filament, "launching your blockchain project has never been easier" 10 january 2015. [online]. available: https://filament.com/. [accessed 2 2018]."

[12] "Empower my supply chain," 10 january 2015. [online]. available: htts://skuchain.com. [accessed 2 december 2018]."

[13] "Blockchain of things, "the ultimate blockchain technology," 10 january 2015. [online]. available: https://blockchainofthings.com. [accessed december 2018]."