CarChain: A Novel Public Blockchain-based Used Motor Vehicle History Reporting System

Mohammad Z.Masoud, Yousef Jaradat, Ismael Jannoud and Dema Zaidan
Electrical Engineering Department
Al-Zaytoonah University of Jordan
Amman, Jordan 11733
Email: (m.zakaria, y.jaradat, ismael.jannoud)@zuj.edu.jo

***Abstract*—Blockchain Technology has been proposed to tackle author, centrality and storage issues. It converts centralized applications into dynamic distributed ones. Many researchers have proposed protocols and applications for mapping the old central applications into blockchain based distributed application. In this work, new system framework for Public World Wide Used Motor Vehicle History Reporting System, named CarChain, is proposed and designed. The new framework has not been constructed based on any of the popular well-known public blockchain networks. The framework constructs a peer-to-peer (P2P) overlay network that broadcasts transactions as any end system multicasting system in P2P live streaming applications. The framework allows car owners, repairing companies and insurance agencies to register and add new histories for cars in a simple method. Four different smart contracts control block updates in CarChain. In addition, database technology has been leveraged to cache intermediate data. We show in this paper the challenges and research opportunities that encounter blockchain based applications, such as CarChain.**

***Index Terms*—CarChain; BlockChain; Peer-to-Peer (P2P); Overlay Network; Hashing Algorithms**

I. Introduction

Selling and buying used motor vehicle is a popular business around the world. It has been reported that 60 million cars have been purchased in USA and proximately 71.1% of these cars are used or second hand cars [1]. To purchase a used motor vehicle, customers have many concerns about the car, how it was used, is it good enough, why the owner is selling it? Without answering these questions, it is hard to trust its complex mechanical and electrical parts especially for naive customers. To tackle such an issue, in 1984 a used motor vehicle history report company has been founded [2]. The company, named CarFax, harvested data of all cars purchased in USA and Canada to launch its web-based services in 1996. In 2015, CarFax claimed that their database has more than 20 billion records of used cars. These data and information have been collected from over than 100k sources [3].

The success of used motor vehicle history report provided by CarFax in USA and Canada motivated other countries to record their own cars histories. For example, Carseer [4], is a new used motor vehicle history reporting company operates in Jordan. The UK AA history check service [5] is a similar service provides the same functionalities for UK and Europe customers.

Second hand motor vehicle services have proliferated around the world. However, these services require massive data harvesting, updating and storage capacities. In addition, the old data should have no changes after the insertion process into the databases. Moreover, these reports should be shared between different platforms over the world since used cars business is global business. In other words, USA used cars may be purchased in other countries around the world. These issues and others need to be tackled to have one history report for any car in any country around the world.

One of the new emerging distributed storage paradigms that has been proposed is blockchaining [6]. It has been proposed to tackle the issue of centrality, trust, security and authority. In this paradigm, application users construct an overlaying network. In this network, all users write their transactions and save them as blocks. Subsequently, the new blocks are added to the chain that has been generated when the overlay network is created. To guarantee that each node in the network have the same chain structure with the same transactions in each block with others, only one node is responsible of updating that chain after filling a new transactions block. Nodes compete with each others to update the chain through solving a complex mathematical problem. The first node to solve the problem updates the chain. This allows all users in the overlay to store a duplicated version of the chain in each node to enhance the storage capacity in distributed fashion. Moreover, this guarantees that no one has the ability to change any old records.

In this work, a distributed blockchain used motor vehicle history report system, named CarChain is proposed. The system constructs an overlay network that can be shared between normal customers, car sellers, car mechanics, insurance companies and governments. Different transactions belong to different users types. CarChain grants cars owners the ability to show its history to other customers and dealers without any central agencies around the word. When the ownership of the car moves from one customer to another, the history record will be updated and moves to the new owner. To reduce the complexity and the size of CarChain, hierarchical design module has been leveraged to construct different overlay networks for each country.

The rest of this paper is organized as follows. Section II introduces some of the applications that have been imple-

978-1-5386-7942-5/19/$31.00 ©2019 IEEE

mented using blockchaining. Section III shows blockchaing background. Section IV overviews the structure of CarChain and its challenges. Finally, we conclude this paper in section VI.

II. Related Works

Blockchain is not a new technology. It is a collection of existing techniques that is arranged in a new specific order to tackle different authority, security and share issues. Many applications have been proposed to be moved from ordinary or common operation to leverage blockchain. In addition, many surveys have been written to gather information of these applications [7], [8]. In the following subsection, some of field and applications of blockchain are introduced

A. Cryptocurrency

The most popular and the first application of blockchain was cryptocurrency. In 2008, the first cryptocurrency system has been proposed [9], which called bitcoin. In 2017, it has been reported that the number of cryptocurrencies around the word is approximately 5.8 million users. Most of them are bitcoin users [10]. The popularity of bitcoins motivated other developers to develop other cryptocurrency systems, such as, Ethereum [11], Ripple [12] and bitcoin cash [13]. It has been reported that the market capital of cryptocurrencies systems exceeded 360 billion dollars in 2018 [14]. Cryptocurrencies allow their subscribers to exchange money without any third party in the middle. One thing to be mentioned that, new cryptocurrencies are inserted into these systems through the mining process.

B. Security Applications

In this field, many applications have been proposed to tackle the centrality issues. First, digital identity is one of the applications that have been deployed in blockchaing in India [15]. This system was the base of other proposed systems, such as, voting systems [16], [17], digital signature [18], secure shopping [19] and privacy [20]. It would be interesting to apply blockhain technology to anti-money laundering systems that track rather physical money instead of transactions as has been recently suggested [21].

C. Economy, Marketing and Industry

As in the previous applications, blockchain has been deployed in the economy and marketing filed to eliminate the centrality and authority issues. In economy, banking systems [22] may benefit from blockchain approach to clear payment methods and enhancing credit information technology. Blockchain also found its way in logistic and supply chaining applications [23], [24].

D. Health Applications

One of the proliferated blockchain applications is the health applications [25]. In these applications, subscribers health records are stored in blocks over blockchain overlay network. Subsequently, physician may access their patients anywhere in the globe if permission is granted from the patients. This application allows users to carry their health records wherever they move around the world. In addition, no storage or database is required. Whenever arriving to the destination, the chain is downloaded into new devices and accessed with subscribers password. MedRec [26] was one of the first blockchain health applications proposed prototypes.

For the best of our knowledge we are the first to propose a blockchain based application for car history record system.

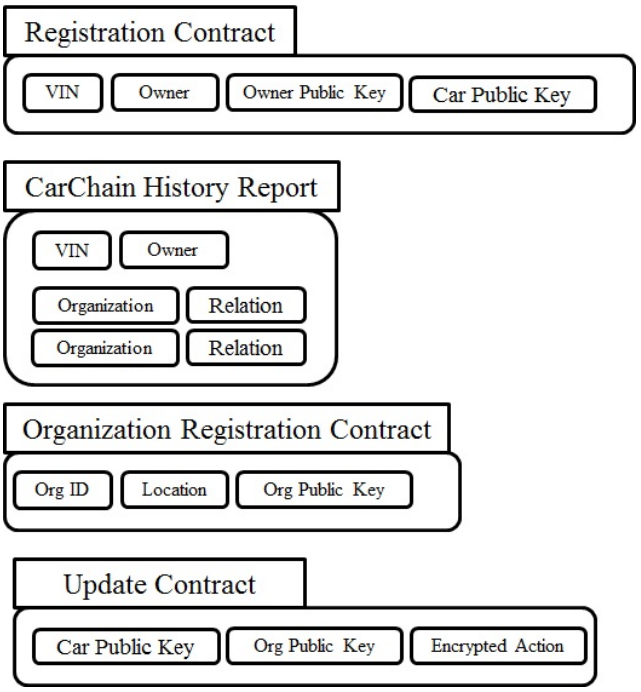

Fig. 1. Smart Contract of CarChain

III. CarChain Architecture

Blockchain has been proposed as a dynamic and decentralized ledger for crypto-currencies. However, this framework has shown flexibility for implementing any decentralized computer resources applications [11]. Carchain structure extends this property of blockchain. In CarChain, different users or subscribers can join and register; normal users or car owner, car repairing organizations and insurance agencies. CarChain leverage smart contract for block updates, registration of new owner and new organizations and agencies. Fig.1 shows these smart contracts. These contracts work as the same way as Ethereum smart contracts. Moreover, these contracts save the meta-data of the saved information. In addition to smart contract, CarChain generates transaction blocks that join the chain every period of time. To reduce computational load, only organizations are responsible of updating the chain. The following subsections introduces the architectural parts of Carchain

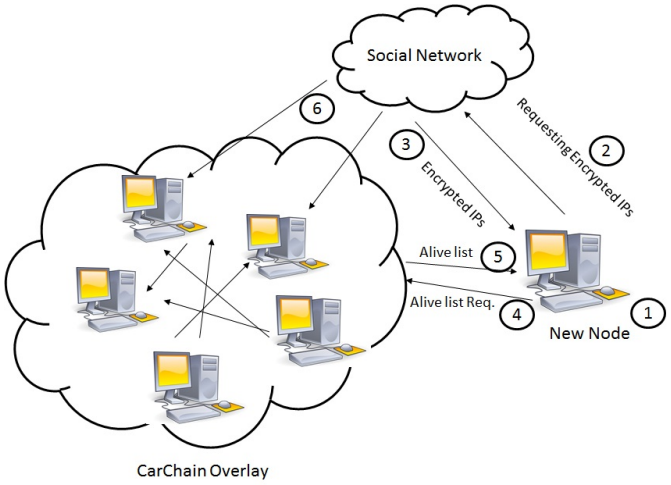

Fig. 2. CarChain Overlay Construction steps

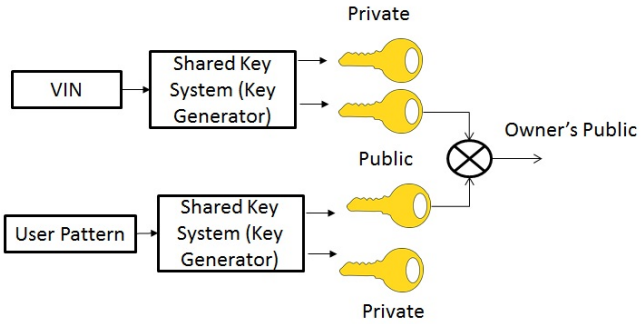

Fig. 3. CarChain Overlay Construction steps

A. CarChain Overlay Network

CarChain system framework is a distributed peer-to-peer (P2P) network application that operates as Internet protocol television (IPTV) applications, such as PPLive [27]. Nodes in overlay networks construct a direct connection between nodes. These direct connections have different network technical issues, such as, network address translation (NAT), delay, transaction propagation and searching for new and old nodes. Each new node or registered user in CarChain should find other nodes. This issue has been tackled in P2P file sharing through utilizing tracker servers. Skype network has tackled this issue through hard coded servers IP addresses in the main application. CarChain leverage social media web-sites to broadcast the IP addresses of new nodes or the new public IP addresses of the nodes if their addresses have been changed. In the first prototype, Facebook group has been created and hard-coded into the main application. Whenever the IP address of the node is changed, the new address is updated to the Facebook group. However, the node ID and address are updated in encrypted format using owners private key. Other nodes inquire the group to obtain these encrypted addresses, decrypt them and add them to node alive list. Subsequently, nodes attempt to connect with these nodes. If these nodes are alive, nodes exchange their alive list. Fig. 2 shows the steps of overlaying construction. As shown in step 1, new node is registered and inquires the social media for encrypted addresses and it updates its encrypted address. In step 3, the node starts to communicate with nodes from the overlay network to obtain their alive list and it constructs its own list. Finally, nodes inquire the social media from time to time to obtain new address lists as in step 6.

To reduce the storage and network overload, a small list is only checked for update forwarding. In other words, each node is responsible of updating a portion of the whole network.

Finally, to tackle NAT issue, NAT traversal [28] has been utilized. Unfortunately, this is a centralized part of the network and can be replaced with other public nodes in the network in the future.

B. Smart Contract

In Fig.1 four different smart contracts are shown. The following describes these contracts. One thing to be mentioned that smart contract phrase has been utilized in this work and they have no connection with smart conract in ethereum blockchain.

1) Owner Registration Contract: The first contract is the owners registration contract. In this contract, car owner generates a new pair of public and private keys for updating transactions. These keys are generated utilizing two different addresses. The first address is the car unique identification name that is printed on cars engines, which called vehicle identification number (VIN). The second address is a unique number generated from users touching pattern on touch screen or computer mouse. These two addresses generate two different pairs of public and private keys. Fig. 3 shows the steps of generating these keys.

It worth mentioning that Cars owners keep the private keys safe and publish its car and owner public key for other organizations.

2) CarChain History Report: This report shows the history of the car, the owners, accidents and repairs. Each row in the report shows the ID of an organization and its relation to the car. Moreover, it shows how the ownership of the car changed from a user to another. This contract has permission. In other words, only the owner of the car has the ability to view it. However, the owner may grant other users to view the report and revoke this permission at any time. Any update transaction is shown in this contract when generated. To reduce the generating time of this report, CarChain is stored as a database using SQL-Lite version that can be downloaded in smartphones and computers. This makes it easier to copy and download the whole chain from the overlay.

3) Organization Registration Contract: This contract is a similar to the owner registration contract. However, in this contract, only one pair of keys is generated for each organization. This key works like a digital signature for insurance and repair organizations. If the organizations are recorded in the system, the report will be trust-able.

4) Update Contract: The fourth and the most important contract is the update contract. It has three main categories. The first category is ownership replacement. In this contract, a new user requests the ownership of a used car owned by another user. To accept the request, the old own have to grant it. If it is granted, the new users public key is recorded with the VIN number of the car and a new pairs of keys are generated. In this way, the old user has no permissions to request the history report. Moreover, the old owner has no permissions for any new update contract for this car. The second category is the repair or the insurance. In this category, when an organization repairs the car or insurance agency records an accident of the car, they make a new transaction to the block. However, the owner has to accept the transaction to be recorded in the block. The final category in the update contract is permission granting and revoking updates. They are used to allow other subscribers to view the history report of the car.

C. CarChain Chain Construction

To construct the chain, nodes broadcast the update transaction to its neighbors in the alive nodes list. Before broadcasting any message, the update contract should be executed for the transaction to be granted. In other words, the updating process starts from an owner or an organization. After the update is initialized, the initializer sends the transaction to the affected node or user for accepting the transaction. If the transaction is granted from the other node, the initiator broadcast the message.

This message has a unique sequence number to stop the end systems broadcast storms. The update message consists of three fields, effector, affected and value. Both of effector and the effected are the encrypted IDs of owners and the organizations. Moreover, the effector or the affected encrypts the value or the transaction with the effectors public key. Each node in the overlay network receives the message. The three fields in the message are kept in cache memory until the construction of the new block in the chain. In other words, for any transaction to be implemented two granting processes should exist; a grant from the affected and the block creation.

To reduce the size of the chain and reduce the cache memory of the system, every one week a block is created. To generate the block, organization registered nodes starts to calculate a challenge value. This value is similar to the initial vector or the nonce value utilized in encryption chain modes in cryptography. The first node calculates the nonce value and broadcasts it to other organization nodes. They test the value for its accuracy. If more than 50% of the organization nodes find the value accurate, all nodes utilizes the value to generate the same block as the first node found the value and update the chain. Subsequently, users nodes download the new block from any organization nodes to complete their chain. If more than 50% of the node cannot prove the accuracy of the value, nodes continues digging or mining to find a new value.

To understand the updating process, Fig. 4 shows an example of a CarChain block in the cache memory of an organization node. As shown in the figure the block has four

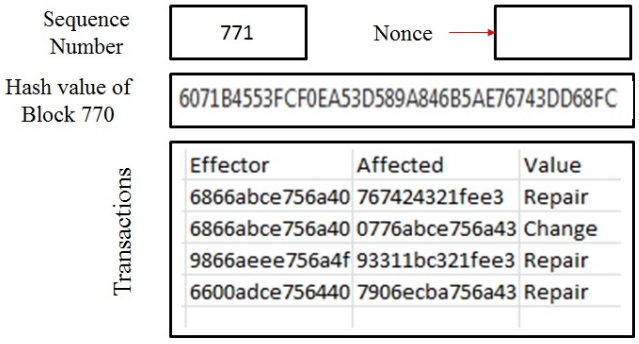

Fig. 4. Example of CarChain Block

main fields: transactions, hashed value of the older block, an empty nonce field and a sequence number. The challenge is to find a nonce value of these four fields that generates a hash value of this block starts with 1993. This number has been leveraged since it is the foundation year of our university. Two main algorithms may be used for calculating hashing, Secure Hash Algorithm (SHA) and message digests (MD) algorithms. SHA -1 has been used, which generates 160 bit output value. Trial and error is used to find nonce value. This process is called mining in blockchain applications. Eq.1 shows the hashing process. When an organization node finds this value, it broadcast it to its neighbors. The neighbor nodes try it for validation. If the value is right, they broadcast it to their neighbors. Finally, the first node adds the new block to the chain and adds its hashed value to the next block for future calculation.

$$Hash_{T+1} = SHA(nonce + Seq + Hash_T + Transactions) \quad (1)$$

where $nonce$ is the variable that nodes are required to find in each challenge and Seq is the block sequence number.

D. The Whole Picture

CarChain system framework utilizes many technical details and libraries. When deploying the CarChain framework, a database is created with a single table to cache the transactions before granting. If the node wins the challenge, the node executes a function in a new thread to convert the records in the table into a JSON structure based file. This file or structure will be added to the chain as the new block. The node has also a function that is executed every challenge to search for the nonce value. A third function is used to insert new transactions into the table.

The framework has a thread that responsible of the networking issues. This thread is responsible of generating the alive list and inserts the IP addresses in it. Moreover, it is responsible of NAT issues and transaction broadcasting. In addition, it has a main daemon to listen for broadcasted messages. This daemon generates new threads to handle new sockets. It is also responsible of checking messages sequences numbers before handling the message to the broadcasting daemon and inserting

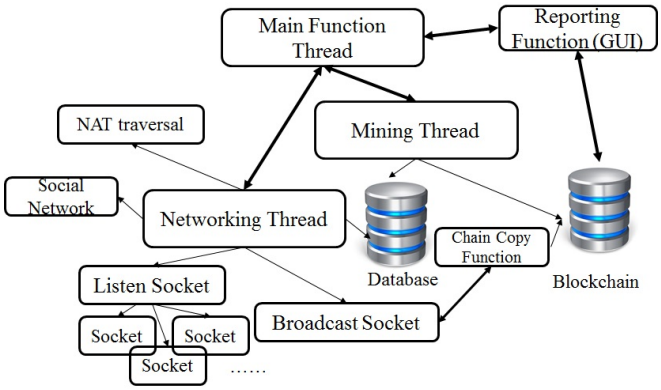

Fig. 5. CarChain Prototype

the new data into the database. If this daemon listened to a new nonce value from its neighbors, it stops the mining function and tests the new value. If it is accurate, the node broadcast the value. If not the value will be discarded and the mining function continues its process. Fig. 5 shows the technical details and functions of CarChain prototype.

IV. CarChain Challenges and Opportunities

CarChain is a blockchain based application. It is also a P2P distributed application. This heterogeneity poses challenges and many technical details in networking, security, storage and programming. In this section some of the technical challenges of CarChain will be introduced.

First, the computational power is an issue for CarChain especially with the proliferated of smartphones and tablets. The application should works correctly without any computational overhead in these systems. To reduce the computational issues, the mining function has been disabled in normal nodes and only works on organization nodes since these nodes maybe powerful servers. In the future, a computational power testing function may be added with a threshold algorithm to reduce the mining load.

Second, the storage capacity of smartphone is small. These devices have been designed for other purposes than storing a massive blockchain. However, this issue may be eliminated if the block copy function is disabled and works only in clouds or other edge computing technologies. Edge technology may tackle both the computational and storage issues of blockchain in the future.

Third, networking issues are divided into three main issues. First, public and private IP addresses. These addresses introduce a socket opening and forwarding issues especially if the nodes are located behind firewalls. NAT/PAT traversal is a helpful technique to tackle this problem. However, this method requires a standalone server or a central node in the network. This converts the dynamic overlay network into a hybrid model. These servers maybe eliminated with the help of super nodes in the system. However, more enhancements are required in this field. The final network problem is node searching and overlaying construction. This problem poses another central part of the network. Central servers are leveraged in all blockchain technology and trackers are leveraged in P2P applications for node searching. More research and algorithms are required to convert the network into a fully distributed system.

Finally, mobility of used cars reveals an issue for CarChain. A new method and function should be written to allow copying blocks between two different CarChain chains.

V. Conclusion

In this work, a new blockchain-based framework for used cars history reporting, named CarChain, has been proposed and a system prototype has been designed. CarChain has tailored the issues of centralized for used cars history reporting systems, such as, authority and repairing agencies and central storage databases. Moreover, it has the ability to allow car owners only to grant other subscribers to view the car history report without any third party. The new framework has not been tested yet since it requires different insurance agencies and users to deploy it. However, the main networking and security functions are working accurately in standalone environment.

Acknowledgment

This research paper was supported by Al-Zaytoonah University of Jordan fund by the project titled “Load Balancing Algorithm for Green Computer Networks”. “Resolution number 18/64/2016-2017”.

References

[1] “Used cars statistics,” www.statista.com/ statistics/183713 /value-of-us-passenger-cassales-and-leases-since1990, 2018.
[2] “Carfax,” https://en.wikipedia.org/wiki/Carfax(company), 2017.
[3] “Carfax statistics,” https://www.marketwatch.com/ press-release/ carfax-databasehits20billionrecords-20180425, 2017.
[4] “Carseer,” https://jo.carseer.com/, 2017.
[5] “Aa history report,” 2017. [Online]. Available: https://www.theaacarcheck.com
[6] M. Swan, *Blockchain: Blueprint for a new economy*. ” O’Reilly Media, Inc.”, 2015.
[7] M. Pilkington, “11 blockchain technology: principles and applications,” *Research handbook on digital transformations*, p. 225, 2016.
[8] Z. Zheng, S. Xie, H. Dai, and H. Wang, “Blockchain challenges and opportunities: A survey,” *Work Pap.–2016*, 2016.
[9] S. Nakamoto, “Bitcoin: A peer to peer electronic cash system,” 2008.
[10] G. Hileman and M. Rauchs, “Global cryptocurrency benchmarking study,” *Cambridge Centre for Alternative Finance*, vol. 33, 2017.
[11] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.
[12] D. Schwartz, N. Youngs, A. Britto *et al.*, “The ripple protocol consensus algorithm,” *Ripple Labs Inc White Paper*, vol. 5, 2014.
[13] S. Barber, X. Boyen, E. Shi, and E. Uzun, “Bitter to better how to make bitcoin a better currency,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2012, pp. 399–414.
[14] L. Bach, B. Mihaljevic, and M. Zagar, “Comparative analysis of blockchain consensus algorithms,” in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 2018, pp. 1545–1550.
[15] T. Khanna and A. Raina, “Aadhaar: Indias unique identification’system,” 2012.
[16] H. Agarwal and G. Pandey, “Online voting system for india based on aadhaar id,” in *ICT and Knowledge Engineering , 2013 11th International Conference on*. IEEE, 2013, pp. 1–4.
[17] R. Osgood, “The future of democracy: Blockchain voting’,” *COMP116: Information Security*, 2016.

[18] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 2015, pp. 180–184.
[19] R. M. Frey, D. Vuckovac, and A. Ilic, "A secure shopping experience based on blockchain and beacon technology." in *RecSys Posters*, 2016.
[20] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.
[21] O. H. Hamid, "Breaking through opacity: A context-aware data-driven conceptual design for a predictive anti money laundering system," in *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*. IEEE, 2017, pp. 1–9.
[22] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innovation*, vol. 2, no. 1, p. 24, 2016.
[23] N. Alzahrani and N. Bulusu, "Block-supply chain: a new anti-counterfeiting supply chain using nfc and blockchain," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. ACM, 2018, pp. 30–35.
[24] H. Wu, Z. Li, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, "A distributed ledger for supply chain physical distribution visibility," *Information*, vol. 8, no. 4, p. 137, 2017.
[25] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016.
[26] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare:medrec prototype for electronic health records and medical research data," in *Proceedings of IEEE open & big data conference*, vol. 13, 2016, p. 13.
[27] X. Hei, C. Liang, J. Liang, Y. Liu, and K. Ross, "Insight into pplive: a measurement study of a large-scale p2p iptv system," in *WWW Workshop of IPTV services over World Wide Web, May 2006*, 2006.
[28] J. Rosenberg, "Interactive connectivity establishment (ice): A protocol for network address translator (nat) traversal for offer/answer protocols," Tech. Rep., 2010.