An Overview of Blockchain Technology: History, Applications and Challenges

Shradha Shree

Pratt Institute

Abstract

This paper explores few published articles that report on the blockchain technology. Blockchain is a sequential chain of blocks that store information. The uniqueness of this technology lies in its three main properties: immutability, efficiently verifiable and distributed-ness. This paper presents a brief history and architecture of blockchain. The properties, applications and challenges are listed. Furthermore, the design challenges with respect to the end-user are also reviewed.

Keywords: blockchain, bitcoin, hash, cryptocurrency, design

An Overview of Blockchain Technology: History, Applications and Challenges

Introduction

Blockchain, a chain of blocks containing information, has become one of the most exciting invention after the internet [12]. In 2008, the financial meltdown led to the proposition of a decentralized digital currency – bitcoin [9]. It uses blockchain technology to carry out transactions with ledgers being managed collectively by a network of computers called nodes. There are many definitions of blockchain technology but to put it simply "it is a technology which anyone can use and is not owned by a single person" [2].

The uniqueness of this technology lies in its three main properties: immutability, efficiently verifiable and distributed-ness. The cryptographic algorithm behind the technology ensures high-level of security [13]. Since it is decentralized and distributed no single entity has full control and all information is available to everyone. This public access makes it more difficult to cheat the system [12]. To use an analogy to describe it further, it is easier to steal a cookie kept in a secluded place, than stealing it from the marketplace, being observed by people [1].

Putting the impact of blockchain in perspective - there has been over one billion dollars in the funding of the blockchain startups since the first half of 2017 [9]. There were about 15 papers published as of November 2016 in the Web of Science and 106 papers in Social Science Research Network (SSRN). The detailed numbers of papers published in both Web of Science data and SSRN are shown in Table 1 [12].

Table 1 Number of academic papers on blockchain [12].

YEAR	WEB OF SCIENCE	SSRN
BEFORE 2014	0	0
2014	0	6
2015	4	22
2016	11	79

History

The first work on a blockchain using cryptographic algorithm was described in 1991 by Stuart Haber and W. Scott Stornetta [8][3]. The idea was to implement a system where timestamps of a documents could not be tampered. Later in 1992, Bayer, Haber and Stornetta incorporated changes in the design, which improved the efficiency by collecting several document certificates into one block [8].

In 2008, an unknown person or a group of people using the name Satoshi Nakamoto published a paper entitled “Bitcoin: A Peer-To-Peer Electronic Cash System” [1]. This paper gave a description of how online payments can be sent from one person to another that would not go through a central financial institution yet be safe, secure and trustworthy. Since then bitcoin has been realized as a concept and enjoyed great success along with other digital currencies that followed. These currencies use cryptographic functions and thus are termed cryptocurrencies. Bitcoin as the first cryptocurrency has become one of the most successful application of the blockchain technology[1]. Johann Palychata from BNP Paribas wrote in the Quintessence magazine that bitcoin’s blockchain, the software that allows the digital currency to function, should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond [1][10].

Blockchain Architecture

Blockchain is a chain of block consisting of a complete list of the transactions of all the blocks. The block consists of two parts - a header and a body [13].

The header of the block consists of block version which has a set of block validation rules, hash value which functions like a fingerprint and is unique, timestamp which has the time and date and few implementation specific data called – nbits, nounce and parent block hash [13].

The body of the block is composed of a transaction counter and transactions which depend on the block size and size of the transaction [13].

What makes blockchain so secure? Its security is credited to the strong cryptographic mechanism for authentication and verification of transactions. Each person making a transaction has a set of two keys which form a pair – a private key and a public key [13]. The private key is kept confidential and it is what verifies who 'you' are; quite like a Social Security Number. The transaction is involved with two phases: signing phase and verification phase [13]. When one person is sending a message to another person then the sender signs the message with his/her private key. Signing here means modifying the message digitally using an algorithm that combines the message and the private key. This modified data is then broadcasted throughout the whole network. During the verification phase the other person who receives the message will validate the data using the sender's public key [13]. The beauty of cryptographic solution lies here. If the transaction was signed using a private key that pairs with a public key, then the program is able to validate the transaction without actually knowing the private key [13]. It only uses the signed transaction and the public key to verify the transaction.

It is worth noting that 'figuring out' a private key from the signed data and a public key that pairs with the public key is mathematically improbable. In this way the person who receives the message can check if the data is tampered or not and no one can forge a signature [13].

Properties

Blockchain has three properties which makes it unique:

Immutable

Being immutable means that once a data is stored in a block then it can never be changed [1].

It is improbable that forged block can be inserted by a bad actor since a consensus with the rest of the network will not be in agreement [1].

Efficiently Verifiable

Transactions that are made using this technology have quick and reliable authentication owing to the cryptographic algorithm used for verification [13].

Distributed

Being distributed means that everyone has a copy of the information. This ensures that no single entity has control of all data [1].

Applications

Blockchain has a huge potential owing to its properties discussed above. Businesses have started experimenting with innovative ideas and solutions to employ blockchain to solve various problems in different fields. Some of the applications are discussed below:

Cryptocurrency

One of the most obvious and successful application of blockchain is cryptocurrency. It provides a platform enabling people to directly transact with one another without having to

involve third parties or surrogates like banks [13]. Bitcoin, the most valued cryptocurrency, reached market capitalization of 10 billion dollars in 2016 [12].

Smart Contracts

These contracts automatically execute the terms. Though this is not a new application it was not used until the cryptocurrency came into existence. The mechanism behind the smart contracts is similar to how cryptocurrencies work. It is an agreement between the participating entities when a preconfigured condition is met [1].

Automobiles

Blockchain technology can be used in automobile industry. For example, by tampering with the odometer (which is an instrument to measure distance travelled) someone can make a car appear to be newer and less worn out, resulting in customers paying more than what the car is actually worth [4]. Regular odometers can be replaced with smart ones that are connected to the internet and frequently write the cars mileage to a blockchain. This would create secure and digital certificate for each car and because we use blockchain no one can tamper with the data and everyone can look up a vehicle's history [4].

Supply chain

Walmart and IBM are working together to use blockchain technology to digitize the food supply chain process. By using blockchain the process of supply chain can be made more traceable and transparent [7].

Voting

In 2015, the bitcoin foundation started a new project that developed blockchain based voting [12]. The property of immutability and verification of blockchain ensures that the voting process is more transparent.

Furthermore, many companies like IBM, Amazon, eBay have created new R&D divisions that are exploring various application of blockchain [1]. Banks like Goldman Sachs and Barclays are working together to explore its application in financial industry [1]. In 2016, Barclays used blockchain based trade which helped in clearing the transaction in 4 hours that earlier used to take 7 days [2]. According to the World Economic Forum, 80% of banks are using blockchain technology for both front-end and back-end offices [5].

Challenges

Blockchain has a lot of potential for the future but it is facing a number of technical challenges which need to be addressed:

Environment

There is a lot of wastage of electricity and resources in the proof-of work calculation which used to verify a block [13].

Scalability

As the amount of transactions are growing day by day blockchain is becoming bulkier. Every node in the network stores all the transactions as it has to validate them on the blockchain [13].

Privacy Leakage

Blockchain can preserve a certain amount of privacy through the public key and private key [13]. Users transact with their private key and public key without any real identity exposure. However, blockchain cannot guarantee the transactional privacy since the values of all transactions and balances for each public key are publicly visible [13].

Lack of Research

Academic research in the descriptive level is still lacking. It is difficult to uncover new explanations and theories underlying the blockchain technology [12].

Educating Public

People are not aware of the underlying technology used. This hinders its widespread acceptance [2].

Trust

As this technology does not have a central authority to keep a check therefore people are reluctant to trust and adapt this technology [2].

Designing for Blockchain

Blockchain is in early stage and rapidly growing with many industries exploring business opportunities. From the perspective of a designer, it has unique characteristics like understandability, trust and verification processes, transaction wait times that require innovative design solutions. In order to accomplish this, we need the design to seamlessly incorporate these properties and display what users are able to understand [6].

Data exposure

As people are trying to adjust with this technology, we can provide more exposure to the transaction steps and show the process visually [6]. Like showing that information is digitally signed or displaying a lock icon to show something that is cryptographically secured. The data and visuals should be actionable, and it should serve the purpose of building trust [6].

Avoiding Jargons

We should avoid technical jargons which general public may not be aware of [6]. The complete end-to-end process should be pleasant for the user and not exhausting.

Consistency

There should be consistency in the design for processes, colors, typography across applications [6]. This will help the users to feel at ease and lead to faster learning and adoption.

Constant Feedback

Constant feedback from the design perspective can help reduce the confusion and anxiety of the user [6]. This can be done through motion and animation and can be used to engage the user [6]. Through the visuals we need to make the users understand what is happening and what will happen next.

Readability

In cryptocurrency the crypto wallet has a unique number of about 40 characters [11]. Sending a transaction using this crypto wallet involves double-checking these 40 characters. To address this problem, we can use unique color codes to verify the address or we can use the last 4 digits of the crypto wallet to verify [11].

Conclusion

The fundamental quality of blockchain lies in the uniqueness of its ability to support trustworthy transactions via automated network systems instead of human intervention and monitoring. When this technology was first introduced it tried to solve a financial problem but today its impact can be seen burgeoning in all spheres.

I believe there are a lot of interesting challenges to solve from the perspective of end-user design. Opportunity in front-end design and can be grounds for experimenting novel ideas to facilitate widespread adoption of this technology. It is imperative for the designers to focus on making the experience for the users pleasant and easy to understand.

Moreover, this field is exciting for researchers to participate and realize the impacts of blockchain, and inevitably, we will see more business research in blockchain in the next few years.

References

[1] Crosby, M., N., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin. *Applied Innovation Review*.

[2] Fleming, K. (2017, December 22). Designing for Blockchain. Retrieved from https://medium.com/

[3] Haber, Stuart; Stornetta, W. Scott (January 1991). "How to time-stamp a digital document". *Journal of Cryptology*. 10.1.1.46.8740. doi:10.1007/bf00196791

[4] Kaltofen, T. (2018). No More Odometer Manipulation – Thanks To Block Chains. Retrieved from https://faizod.com/

[5] McWaters, R. J. (2016, August). The future of financial infrastructure an ambitious look at how blockchain can reshape financial services. Retrieved from https://www.weforum.org/

[6] Mills, S. B. (n.d.). Blockchain Design Principles. Retrieved March 21, 2017, from https://medium.com/

[7] Miller, R. (2018, September). Walmart is betting on the blockchain to improve food safety. Retrieved from https://techcrunch.com/

[8] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.

[9] Peck, M. (2017). Reinforcing The Links Of The Blockchain. *IEEE Future Directions Blockchain Initiative White Paper*.

[10] Prisco, G. (2015, July 6). The Blockchain Could Make Existing Securities Industry Players Redundant, Says BNP Paribas Analyst. *Entertainment Close-up*.

[11] Tan, T. (2018, May 18). Designing for Blockchain: Three Ways to Get Started. Retrieved from https://www.ideo.com/

[12] Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*. doi:10.1186/s40854-016-0049-2

[13] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends Zibin Zheng-Shaoan Xie-Hongning Dai-Xiangping Chen-Huaimin Wang - 2017 IEEE International Congress on Big Data (BigData Congress) - 2017. *IEEE 6th International Congress on Big Data*.