Study of Blockchain beyond Bitcoin

Boyi Song

School of Computing and Information, Beijing Jiaotong University, Beijing, 100044, China

17722021@bjtu.edu.cn

Keywords: Blockchain; Bitcoin; IPFS; Digital Currency; Encryption currency.

Abstract: Blockchain technology has the potential for reconstituting the human society as profound as did the Internet, could applicate in numerous fields exceeding the digital cryptocurrency, as a category of decentralization mode. One of its examples is IPFS which could be concentrated as next major transformation protocol, with its advantageous transformation speed and incomparable security mechanism, stimulating the research that based on the blockchain technology and more beyond the Bitcoin.

1. Introduction

Bitcoin has attracted wide attention for its high-valued, which used to reach $19000 per Bitcoin — trading even higher than gold — $1242 per ounce, indicated by Kitco News [1]. However, the technology behind Bitcoin, named as blockchain, and its capacity is far beyond the cryptocurrency, enabling the existing technology established their applications to ameliorate vastly. A distributed database known as the integral concept of the blockchain technology, can be seen as the prototype of the Bitcoin [2]. The distributed database records every transaction done through Bitcoin and increases over time, for every ten minutes one block shall be added to the distributed database which in worldwide connected with each other like a chain. Blockchain is distributed, which also brings the decentralization feature to the Bitcoin, means the behavior of the Bitcoin is out of inspection and have the capacity in autonomous, enabling to cut out the middleman, reducing the cost of transactions and security to the cryptocurrency suggested by Underwood [3]. The common features of Bitcoin or other cryptocurrencies enabling this technology to evaluate the existing financial system and establish a new decentralized autonomous financial system, permitting people to make transactions globally easier, more inexpensive and safer. Especially, in the international remittances market, one traditional transaction fee could even reach to 30 percent, while using Bitcoin or other cryptocurrencies could reduce the credit card fee worldwide from as much as 3 percent to below one percent. Obviously, Bitcoin benefits the economy vastly and emerging the transactions, indicated by N [4]. Furthermore, the application of anonymity strategy of Bitcoin means the transaction and the property you owned is beyond the inspection, which validates the principle of “private property is sacred and inviolable” in its real sense for the first time in human history.

2. The basic fundamental of Bitcoin

2.1 Blockchain is the fundamental of the Bitcoin

Argued in the Bitcoin white paper by Nakamoto [5], the father of the Bitcoin, Bitcoin suggests that the use of a hashing peer-to-peer network to overcome the double-spending problem without the third party participate. The work or transaction record will be hashed into an ongoing chain of hash-based proof-of-work increased over time, and with the time increased, the work will be proofed with a different timestamp. It is immutable and absolutely safe for individual’s occupation and will never be disturbed by currency inflation in countries. For the reasons mentioned above, Bitcoin became popular around the world. However, the basic of cryptocurrency — blockchain is always ignored by masses.

Blockchain, enable organizations and individuals to trade without middleman participate in, can save time and money for both sides of the transaction and will be seen as the fundamental of the society in the near future, as important as the Internet in human history. The potential of this emerging technology is boundless and applications based on this technology can be used in almost every area in human society and industrialization production.

2.2 One application of the Blockchain for example

One of its applications beyond Bitcoin is the electronic medical record system (EMR). Usually, one patient may have multiple doctors in different hospitals ordering tests, diagnoses and kinds of drugs for treatment. Particularly, in the serious illness case, the patients' health care record could reach to an overwhelming number of pages. The question is that the data records do not belong to the patients or in the patients owned database, but in the hospitals' own close database system, which lead into an inefficiency question for both patients and doctors. Particularly for the emergency situation, doctors cannot give a suitable solution or handle the illness appropriately without the patient's healthcare history [6].

Blockchain can solve this problem in an elegant way by hashing the patient's electronic medical history on the chain anonymously as public key and preserve the privacy key by patients themselves. Experts thought this decentralization EMR highly, and suggest that blockchain can help people realize their personal freedom as some countries do not allow consumer to access their own genetic data, lobbied by the medical-industry[7]. Nevertheless, the privacy of the decentralization EMR has been queried by the public as the data on the chain are open for everyone.

Stated by Mertz [8], a research group at the Massachusetts Institute of Technology (MIT) chose to give a solution based on public Ethereum blockchain technology (seen as the Bitcoin's 2.0 version, enabling the developers to provide robust blockchain applications by ruling a series of protocols and provide the Ethereum virtual machine to instant platform independent.) to develop a new blockchain protocol to preserve the cybersecurity of the patients. Greenberger cited in Mertz (2018) comes from the Healthcare Information and Management System Society (HIMSS) thought highly of the group's work, predicate the improved EMR could boost the healthcare industry soon.

3. IPFS (Inter-Planet File System)

3.1 Blockchain-based Decentralized Storage Schema

Besides the EMR, another application area of the blockchain is the file system area and the name of the application is Inter-Planet File System (IPFS), seems similar to the Bit torrent technology, but the integral parts of these two technologies are far from the "synonymous". Before the implement of IPFS, Bit torrent is the most popular file system protocol over the internet. Users can download the needed source fast by simply downloading a torrent formant file first, then the computer will continue loading the source from the PC owned this source worldwide. The whole process just like sowing the torrent file as a seed and the source will grow up automatically, fast and naturally. Gradually, "seed" become the nickname of BT technology. The "seed" downloading can reach a higher speed than normal downloading protocols such as FTP protocol, as the technology divided source into pieces of small source and stored in different hosts worldwide and the protocol contain a complete computing system to judge the most convenient source node for users to download.

Although many experts recognize BT technology as a decentralization application example, the question is that each downloading needs a tracker server to provide the node address, which leads the torrent technology into a centralization diploma as the source uploading is autonomy, decentralized by users over the world, including pirates, but the downloading needs the centralized trackers to serve. When faced with the legal problem, companies or individuals who provide tracker services could possibly get into trouble. This is the root weakness of the BT protocol as it is a traditional protocol based on traditional HTTP/IP protocol stacks which is unable to implement decentralized connection to the internet. Though the users in the internet can use the service anonymously, the tracker's exact location can be found through the torrent file. The most famous pirate website [www.piratebay.com] (http://www.piratebay.com) has been banned several times due to the exposure of tracker's location.

IPFS provides its solution which is based on blockchain technology. IPFS is a thoroughly decentralized storage network announced by the protocol labs [9]. Governments have no idea how to stop or ban the source spread on the chain. Once the source has been uploaded to the chain, users of IPFS can simply download the source globally. Even on Mars, astronauts could visit the source through the IPFS protocol stacks, the origin of the name "Inter-Planet File System" is come from this feature. The technology has the potential to revolutionize the whole internet communication and aims to not only take the place of the BT but also the HTTP/IP protocol stacks.

3.2 Contents Searching

Another feature of the IPFS is contents searching. Compared with the tradition searching method, IPFS compresses the contents of the source into an identifiable hashing code while the traditional downloading such as BT using the HTTP address to identify different sources. This feature validates IPFS more robust and less counterintuitive than the letter. Compared in the searching area, IPFS has much more advantages, including security, link reliable, friendly to the IoT and mobile devices.

3.3 Problems

However, today as the BT technology has been applied for more than ten years and popular through billions of PCs, IPFS is still far from the majority. What is worse, as the emerging technology is just as familiar with the professional scientists, and seems looking too forward for the masses, frauds using the technology to fraud people or even the government, making this technology lacks of credits. IPFS aims to be a decentralized application which enabling it to avoid inspection, however, this also means strong management is lacking for the whole system. Just like other blockchain applications, for reasons mentioned above, IPFS's application is still a geek's concept.

3.4 Filecoin

To solve these questions or to encourage people using this technology, IPFS decided to add the encouragement strategy layer into the base IPFS protocol stacks. Once its users make contributions to the IPFS chain, corresponding Filecoins are supported to be paid. Filecoin is a kind of digital cryptocurrency just like the Bitcoin. Innovative applications need flux to support their environment for their continuous development, and the flux for the IPFS is active users and sources. If the application gets enormous sources, it will become irreplaceable for users, and the value of the Filecoin will also increase, which will encourage more miners to exchange their storage to store more sources. This will become a positive loop. However, the storage of the source is valued and users cannot share their storage with no payment. Compared with the IPFS, BT and other transportation protocols lack compensation for their contributor. IPFS also hopes to use this feature to beat its powerful competitors. Moreover, as a massive amount of storage sits unused in data centers and hard drives around the world, the innovation of Filecoin could solve the storage source waste problem. Filecoin can be exchanged from USD, BTD, ETH and others simultaneously. The IPFS provide a reliable store system by a hypercompetitive price compared to the big company's Cloud computing services.

4. Conclusion

The applications cases of the blockchain mentioned above indicated a serious problem of blockchain, as a revolution innovation, the blockchain is an innate decentralization technology. However, the question is that without the centralization's propaganda and inspection, the fraud with the "Blockchain" title is too much and the real application of this technology is too little. Although disadvantages of the decentralization in short terms, the blockchain has the potential to lead the next industrial revolution which would change human life and society deeply just like the industrial revolutions before it. Neutrally, the decentralization features of blockchain could possibly be complementary to tomorrow’s human society that includes both decentralization and centralization module. Participating one project voluntarily like the issues of Github and every work done shall be proved on the blockchain seems as the miner’s work in Bitcoin or other cryptocurrencies, harvesting the digital cryptocurrencies as exchange, without trust in this system. People joined the work just because the system they worked for is reliable. Just as Santoshi indicated, the contribution of Bitcoin made is to proposed a financial system without trustworthy consideration. The blockchain’s contribution is to provide a schema to every situation, which is trustworthy, to build a new system without trust on individuals, companies or countries but to trust the system itself. This system schema is the biggest gift blockchain presents to the society.

References

[1] Kitco News. “2013: Year of the Bitcoin.” Forbes, December 10, 2013\. http://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/.

[2] Swan M. Blockchain: Blueprint for a new economy [M]. “O’Reilly Media, Inc.", 2015.

[3] Underwood S. Blockchain beyond bitcoin [J]. 2016.

[4] Hajdarbegovic, N., Deloitte: Media ‘Distracting’ from Bitcoin’s Disruptive Potential.” CoinDesk, June 30, 2014\. http://www.coindesk.com/deloitte-media-distracting-bitcoins-disruptive-potential/;

[5] Nakamoto S. A peer-to-peer electronic cash system [J]. Bitcoin.–URL: https://bitcoin. Org/bitcoin. pdf, 2008.

[6] Likourezos A, Chalfin D B, Murphy D G, et al. Physician and nurse satisfaction with an electronic medical record system[J]. The Journal of emergency medicine, 2004, 27(4): 419-424.

[7] Dubovitskaya A, Xu Z, Ryu S, et al. Secure and trustable electronic medical records sharing using blockchain[C]//AMIA annual symposium proceedings. American Medical Informatics Association, 2017, 2017: 650.

[8] Mertz, L. (2018). (Block) chain reaction: A blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution. IEEE pulse, 9(3), 4-7.

[9] Benet, J., & Greco, N. (2018). Filecoin: A decentralized storage network. Protocol Labs.