2017 International Conference on Intelligent Computing and Control (I2C2)

Blockchain: The Perfect Data Protection Tool

Arpita Nayak
IIIT University
Bhubaneswar, India
arpitanayak241@gmail.com

Kaustubh Dutta
KIIT University
Bhubaneswar, India
kdutta2511@gmail.com

***Abstract*— Blockchain is a technology that is based on Bitcoin cryptocurrency. It is a technology for decentralizing transaction and managing data. Immense research and deep thinking has gone into conceptualizing blockchain since the time it was first showcased by Satoshi Nakamoto in 2008. The growing interest among researchers and technologists is the central attribute of blockchain that provides a high level of security, anonymity and data integrity without any intervention from third party who is in control of the transactions. Here in this study we have carried out through a well-defined study with the sole aim of collecting all relevant research areas and technologies on Blockchain Technology. With Blockchain becoming future in transactions in financial sector, it also comes with its own burden of risks. But since it has the potential to revolutionize the existing technology, it feels right to take the plunge[1].**

***Index Terms*—Blockchain, Ledger, Centralized, Bitcoin, Cryptocurrency.**

I. Introduction

Blockchain is a distributed database which maintains a list of records that goes on increasing continuously known as blocks that are secured from tampering and revision. Every block contains a timestamp and is link to the previous block. The blockchains are designed in a fashion such that they are inherently resistant to the modification of data. Blockchain utilizes a peer to peer network, a distributed time-stamping server and tamper-proof records of transaction data that makes it even more secure and helps to order data in a much organized way. The technology of blockchain is an open, distributed ledger which can track and record transactions taking place between a buyer and a merchant or simply between two parties involved in an efficient approach. Algorithm now days are efficient enough to trigger transactions automatically which is almost like an evolution in the banking world. The network, design architecture and an example of a distributed computing system with high fault tolerance has almost opened the gateway of the world especially in the financial sector. Thus decentralized consensus can be achieved with blockchain making it suitable for identifying and recording events, transaction processing and documenting provenance.

Blockchain was implemented as a main component of the digital currency bitcoin that serves as the public ledger for almost all transactions [2]. The innovation of blockchain as digital currency can help to solve the double spending problem. The invention of bitcoin has a marvel as it led to the advancement of related other fields as well.

The results on current trends on research reveal that focus on Bitcoin system is approximately around 65% to 75% and less than 25% on other Blockchain applications like smart contracts and licensing. Significant studies and research has gone into the improvement of the limitations of Blockchain on the perspectives of privacy and security. Due to the lack of concrete evaluation on the effectiveness, financial organizations are reluctant to change their existing framework into blockchain methodology. With days to come researchers are proposing to solve the challenges of scalability including throughput and latency so as to bring about a change in the history of digital currency.

II. Blockchain Transactions

The significant advantage of blockchain is the method of transactions which are verified and trackable. Instead of having a trusted third-party or a central bank, the technology is based on consensus among a peer-to-peer network of computers that run on complex algorithms. Instead of storing in one database, time-stamped transactions in blocks are stored in different systems across a value chain. This helps in achieving a decentralization of trust which has helped realizing cross-border payments, trading and faster settlements in a reliable and cost efficient way. The key foundational elements of blockchain include:

- Decentralization – Distributing control among all peers in the transaction chain instead of having one central authority controlling everything within an ecosystem. Thus the technology works on the principle of a shared infrastructure.

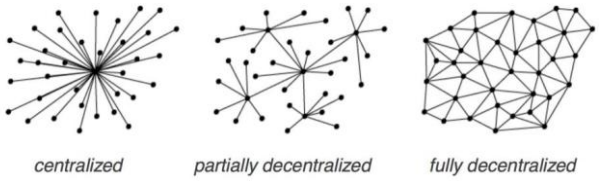

Fig. 1. Type of Ledgers

- Digital Signature- An exchange of transactional value using unique digital signatures that rely on public and private keys to create an authentic proof of ownership [3].

- Mining- After transactions are verified and completed they are stored in blocks using strict cryptographic patterns.
- Data integrity- To prevent tampering of transaction data as agreed upon, the use of complex algorithm and consensus helps in ensuring data safety.

III. Blockchain vs. Distributed Ledger Systems

Blockchain is a peer-to-peer network that is hashed to timestamp records where already a chain of hash based proof of work is going on so that a record cannot be changed without doing again the proof of work. So, a blockchain is a type of distributed ledger that comprises of data recorded digitally that is unchangeable, in packages called blocks [4].

The blocks of data are stored in linear chain. The blocks that contain data are cryptographically hashed. The hashed blocks are dependent on previous blocks so as to prevent tampering of data in blockchain.

Distributed Ledger is a peer-to-peer network prevents modification of ordered series of records that have been stamped by using a defined consensus mechanism. It is built upon a series of networks of databases where participants can create, separate and keep information in an efficient and secure manner.

Without any central party or central administrator, these networks of databases can be operated smoothly and securely. Every participant can access common information simultaneously. In a nutshell, it is a consensus of digital data that has been replicated, shared and synchronized which are spread across sites and/or countries.

In short, Blockchain is a type of distributed ledger but not all distributed ledgers employ chain transactions linearly. Some of the blockchain and distributed ledger systems are: Chain, Corda, Hyperledger, Quoram, Stellar.

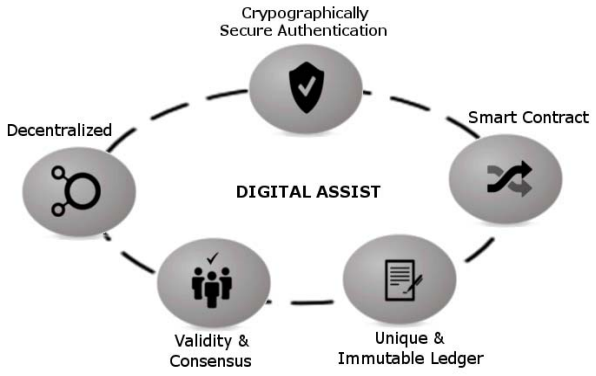

Fig. 2. Functional Components

IV. Societal Impact of Blockchain Technology

Blockchain technology's impact will continue to grow as predicted by industrial experts considering the growth in number of blockchain use cases. Blockchain's promise to change how wealth is created across the globe is one of the most significant societal impacts to note. Few implications of using blockchain technology are :

- To make people participate in digital economy, particularly for people who all are living in developing world and who don't have bank accounts.
- Protecting rights of ownership records.
- To help creating a sharing economy.
- Electronic remittance will be common that will simplify the process of sending money to family members in foreign countries.
- To help consumers monetize data.
- To reduce business costs.
- To enable smart contracts that will make the government officials accountable.
- Resistance to single points of failure or censorship.
- Self-execution of business logic with self-enforcement.
- Selective transparency and privacy.
- Rethinking roles of intermediaries.
- Bundling of services.
- Better security with digital payment as it ensures privacy too.

IT's involvement with blockchain technology has resulted in implementation in almost every other industry; with financial services being the most implemented. In addition to using blockchain technology in financial services and legal industries, it can be used in insurance, advertising, auditing, supply chain, manufacturing [5].

Particularly banks are in pressure of implementing blockchain because they have to face competition from payment softwares by private companies, telecom companies asking customers to use mobile phones as bank wallet and cryptocurrencies [6].

The decentralized characteristics of the blockchain and smart contracts mean that an agreement built on its platform does not need a separate party. When set conditions are met, it triggers automatically that indicates that contractual conditions are translated into logical functions. This is possible because the smart contracts are computer code.

V. Benefits and Risks of Blockchain

Benefits:

- Use of blockchain can aid in preservation of records, evidence and institutional memory because data that has been recorded on the blockchain is difficult to alter and not under the control of one party.

- Blockchain has the potential to reduce workload of multiple stakeholders where transactions and contracts can be kept on a shared ledger and it also has the ability to provide a consistent contract execution environment automatically [7].

- Transactions records can be placed in the Blockchain network within a very short period of time, thus reducing

delivery times and document collection. The delivery times can be dramatically reduced from days to even minutes.

Risks

- Privacy is a big concern. All data does not belong on a public ledger. While technical solutions and private blockchain may resolve this issue for some and may be booming, but the main question arises is who should have access to the data [8].

- Market disruption may result as one of the cons of blockchain. It could replace all of the current procedures where participants trade directly. The current procedures that include processing, recording, reconciling and auditing transactions may be replaced that may cause disruption.

VI. Conclusion

Blockchain is not just limited to the financial system; instead it's a great solution provider to almost any platform or product that can be thought of. Mostly the platform or product that works on sensitive data or something that requires trust like the details of financial transactions, keyless automobile entry authentication, driverless automobiles in the near future or may be the algorithm driven security instead of manned security guards. Many multi-national organizations have come up together to portray that blockchain can eventually be the backbone of the Internet of Things. Eventually when more research goes into blockchain computer networks would be more secured and with reduced malware attacks. As blockchain has the potential to come up with a decentralized marketplace it would not only be more secured but also highly efficient and faster to scale [9].

Blockchain technology offers a lot of disruptive power that has potential and companies are already in the race for different product offerings [10]. As industries continue to evolve, blockchain stands out as the best investment for future returns for at least few decades to come.

References

[1] Andrychowicz, Marcin, Stefan Dziembowski, Daniel Malinowski, and Łukasz Mazurek, "Secure Multiparty Computations on Bitcoin," paper presented at the IEEE Symposium on Security and Privacy, San Jose, Calif., May 18–21, 2014.

[2] "Zerocash: Decentralized Anonymous Payments from Bitcoin," paper presented at the 2014 IEEE Symposium on Security and Privacy, San Jose, Calif., May 18–21, 2014a.

[3] Biryukov, Alex, and Ivan Pustogarov, "Bitcoin over Tor Isn't a Good Idea," paper presented at the 2015 IEEE Symposium on Security and Privacy, San Jose, Calif., May 17–21, 2015a.

[4] "Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay," paper presented at the 19th International Conference on Financial Cryptography and Data Security 2015, San Jose, Puerto Rico, January 26–30, 2015b.

[5] Blanc, Jerome, "Thirty Years of Community and Complementary Currencies," International Journal of Community Currency Research, Vol. 16, 2012, pp. D1–4.

[6] Chaum, David, Amos Fiat, and Moni Naor, "Untraceable Electronic Cash," in Shafi Goldwasser, ed., Advances in Cryptology: Proceedings of Crypto '88: Proceedings, Berlin: Springer-Verlag, 1990, pp. 319–327.

[7] El Defrawy, Karim, and Joshua Lampkins, "Founding Digital Currency on Secure Computation," CCS '14: Proceedings of ACM SIGSAC Conference on Computer and Communications Security, March 2014, pp. 1–14.

[8] King, Sunny, and Scott Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," self-published paper, August 19, 2012. As of February 24, 2015: http://archive.org/stream/PPCoinPaper/ppcoin-paper_djvu.txt

[9] Ethereum, Writing a Contract, [online] Available: https://github.com/ethereum/gohereum/wiki/Contracts-and-Transactions.

[10] J. Bughin, An Executive's guide to the Internet of Things, McKinsey