Review of Distributed Ledgers: The technological Advances behind cryptocurrency

Suvarna K. Kadam[#1]

[#]*Department of Computer Engineering,*
D. Y. Patil College of Engineering Akurdi SPPU
Pune INDIA
[1]skadam@unipune.ac.in

***Abstract*—**
Blockchain and related Distributed Ledger Technologies (DLT) are proving to be the ground breaking and likely to change the role of web from centralized document sharing platform to a generic de-centralized platform that can exchanged digital currency and help autonomously manage financial and real-estate assets. Original idea of Web was a decentralized network with open access. But it slowly grew around centralised servers and demanded privileged access to ensure security while trying to keep openness. The idea of decentralised Web can be re-instantiated if web can ensure trustable, secure and accountable updates among autonomous participants without a central server. Distributed Ledgers are one of key technologies responsible for bringing the openness of web back without compromising its security. The commercial & legal transactions can now be handled completely on the web as DLTs provide more secure and accountable environment. This paper reviews advances in DLTs to demystify the current capabilities, limitations and challenges. It also reviews some of the prominent applications of DLTs including digital currency.

***Keywords*— Blockchain, Digital Ledgers, Crypto Currency, Distributed Ledger Technology(DLT)**

I. Introduction

The financial dealings often require authority and authenticity to ensure fairness. Traditionally, ledgers have been used by authority bodies such as government, banks and judiciary to record transactions of important assets such as money and property. Humanity has advanced from recording the transactions from clay tablets to paper medium to finally the digital form. Now, these advances are capable of *digitally* manage the transactions to buy/sell assets.

The advent of cryptocurrency and distributed ledgers has paved way to bring a major change to banking and payment services. The problem with traditional Internet banking and payment systems is that all transaction records are maintained in a centralized ledger that typically the banking/financial authority controls. The centralized nature of ledgers has two problems 1) Cyber attacks are easier on single target making ledgers more vulnerable to security threats, 2) The original intention of decentralised Web is not fulfilled with centralized ledgers.

Distributed Ledger Technology(DLT) are one of key technologies responsible for bringing the openness of web back without compromising its security[1,3]. The commercial and legal transactions can now be handled completely on the web as DLTs provide more secure and accountable environment for exchanging digital assets in the forms of currencies, popularly known as cryptocurrency.

The paper review the recent advances in DLTs. It organized as follows: In Section 2, distributed ledgers are reviewed; followed by detailed comparative study of state-of the art distributed ledger technologies in section 4. In Section 5, the recent cryptocurrencies along with the related distributed ledger technology (DLT) employed to realize that cryptocurrency are discussed. The review concludes with impact of DLT on the future of the Web.

II. Distributed Ledgers

Distributed Ledgers are popularly known as blockchain[5,6] ever since Bitcoin was invented by an unknown group of people under the pseudonym Satoshi Nakamoto [13]. Bitcoin was the first decentralized digital currency that can be exchanged without a central controlling authority. Bitcoin could be exchanged on peer-to-peer network that supports direct transactions between users independent of any intermediary. These decentralized transactions can be verified by network nodes and recorded in a public distributed ledger known as a blockchain. A blockchain is essentially a *list of records* called blocks, which are linked and secured using cryptography. Each block maintains a encrypted hash of the previous block and timestamp along with the transaction data. Thus a blockchain is robust against the tampering of the data. Every modification request is processed by all nodes and the data in any given block can be altered only when the networked nodes achieve *consensus* that the change is indeed valid. Blockchain thus introduced the concept of truly decentralized ledger that can be maintained securely without necessarily being controlled and administered by a central authority. Figure 1 elaborates the how centralized ledger help in maintaining records of traditional commercial and property

dealings. Governments or bank may act as clearing house with complete control on ledger.

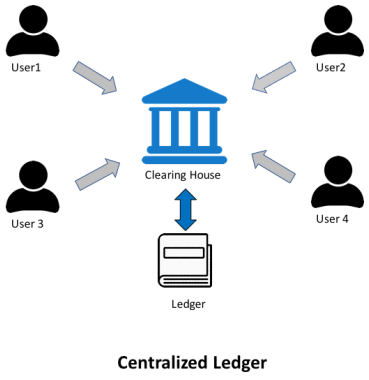

Figure 1. Transaction Handling in Conventional Centralized Ledger

.

Figure 2 illustrates transaction handling with the distributed ledger technology (DLT) such as Blockchain where a ledger is shared among the parties. Distributed ledger is maintained based on consensus of users. There is no central authority/clearing house or centralised data storage. In fact digital data is replicated, shared and may be spread across multiple physical locations or nodes.

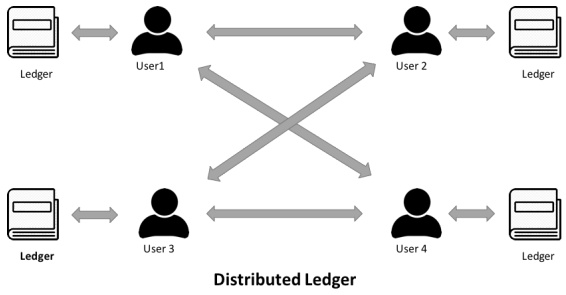

Figure 1. Transaction Handling in Distributed Ledger

A. Distributed Ledger Terminology

Distributed Ledger is a linked list of sets of transactions between the peers of a network, ordered by time, and where each peer holds a local copy.

A **record** is transaction being stored in the ledger by a peer node. It is oftened encrypted using a cryptographic key to assure integrity and non-repudiation.

Peer-to-peer (P2P) architecture partitions tasks or workloads between peers. Peers are equally privileged participant nodes in transaction record processing. Peers have processing power, disk storage or network bandwidth that can be shared with other networked participants.

Distributed Consensus

Distributed computing and multi-agent systems must acknoledge the possibility of faulty processes and find a way to make processes *agree* on some data value needed for correct computation. Distributed consensus can be taken to decide whether to commit a transaction to a database, or whether to add record to transaction.

Proof of work(PoW) is a mining protocol that helps in achieving distributed consensus in trustless environment. The protocol defines computationally *expensive* task called *mining*. Mining serves as two purposes:1) To verify the legitimacy of a transaction and avoiding double-spending, 2) To create new digital currencies by rewarding miners for performing the previous task.

Proof-of-stake (PoS) is another type of consensus algorithm. In PoS-based distributed consensus, the creator of the next block is selected through various combinations of random selection and wealth or age (i.e. the stake).

III. Comparison of Distributed Ledger Technologies

Originally DLTs and cryptocurrency were proposed for financial industry including banks. However very soon it was found that DLTs are not limited to just dealing in virtual currencies or commodities but can be instrumental in exchanging digital asseset. The fact that DLT allows information or records to be transferred and updated by network participants , and that it is done in a trustworthy, secure and efficient way, carries enormous potential for applications.

A. Distributed Ledgers Types: Permissioned & Permissionless

DLT platforms can be divided into two main categories: permissionless(public), and permissioned(private).

1. In permissionless DLT platforms, the ledger is maintained by collaborative action among nodes in the public network and is accessible to everyone. Anyone can join the network, participate in the process of block verification to create consensus. Example of permissionless blockchain is the Bitcoin and Ethereum blockchains.
2. In a permissioned DLT platform restricts the actors who can contribute to the consensus of the system state. The ledger is maintained by authorised nodes and is accessible to registered members only. Permissioned platforms enable faster validation of transaction and can offer improved privacy.

The two categories also differ in the underlying mining model – 1) permissionless DLTs use Proof of Work(PoW) mining where hashing is used to ensure trust. The network consensus can be reached as long as 51% of the nodes are not comprmised by attackers (honest nodes). Bitcoin uses PoW mining whereas Ethereum uses a Proof of Stake model (PoS) for reaching consensus. Proof of stake mining require the members to prove ownership/*stake* in a certain amount of currency. Unlike PoW that buys computing power for mining,

a PoS systems uses capital to acquire the coins/tokens that eventually allows to achieve consensus for validating transactions.

Permissioned DLTs are not required to use the computing power based mining (such as PoW) to reach a consensus since all of the members are known. Instead, Permissioned DLTs are using consensus algorithms like RAFT[18] or Paxos. Raft is a consensus algorithm for managing a replicated log of records. It is equivalent to Paxos and as efficient, but its structure is different Paxos. Raft was proposed to be more understandable and provides a better foundation to build implementable systems. There are also other PBFT algorithms that can be used to reach consensus without PoW mining.

B. Distributed Ledgers Technology (DLT) plaforms

A distributed ledger can be thought of as a consensus on replicated, shared, and synchronized digital data that is managed without any need of central administrator or centralised data storage. Data is stored in geographically spread out locations.

BitCoin Block Chain: The first distributed ledger was conceptualised in the form of BitCoin Block Chain[6,13]. It was implemented to realize the cryptocurrency bitcoin's core infrastructure that maintains a public ledger for all Bitcoin transactions on the network. Bitcoin block chain made it possible to solve the double spending problem without requiring a trusted authority and made cryptocurrencies practical.

After Bitcoin Blockchain (often refrred as BlockChain 1.0), further DLTs were proposed that were referred as Blockchain 2.0. These second-generation programmable blockchain allows members to write sophisticated *smart contracts*. In addition to keep records of transactions, Blockchain 2.0 DLT can enable exchange of *value* (in form of digital assests) without powerful intermediaries.

Bitcoin blockchain is one of the largest public blockchain networks in production today. However public blockchain has a drawback that substantial amount of computational power is required to maintain a distributed ledger at a larger scale.
Table 1 briefly reviews the existing DLT platforms and compare based on key characteristics of whether they are public (Permissionless) or private(permissioned) and consensus mechanism applied.

TABLE I
DISTRIBUTED LEDGER PLATFORMS

Technology	Mode of Participation	Consensus Mechanism	Consensus at
Bitcoin Blockchain	Permissionless	PoW[1]	Transaction Level
Ethereum	Permissionless	PoW[2], PoS[3]	Ledger Level
HyperLedger Fabric	Permissioned	PBFT[4]	Transaction Level
R3 Corda	Permissioned	Multiple	Transaction Level
Waves	Permissioned	PoS	Ledger, Transaction Level
Ripple's consensus system	Permissioned	PoS	Ledger, Transaction Level

Ethereum:
Ethereum[14] is another growing DLT platform. It is an open-source public blockchain that is programmable and supports smart contract (scripting) functionality. It supports a modified version of BitCoin's consensus mechanism that allows more efficient blocktime while mining. Cryptocurrency Ether is generated on the Ethereum platform. Ethereum implements programmable second-generation block chain The smart contracts are priece of code that is stored on a global network of nodes. Smart contracts are executed automatically are never stopped from execution. Etherium also made it possible to completely automated handling of distributed ledgers and therefor cryptocurrency. It offers the standard benefits of transparency and security of DLT as it is not possible to stop a service when it is run by computers globally. Etherium is a groundbreaking business idea that has been depoyed successfully, but it still has challenges of misuse, for ex. etherium smart contracts can be used to run investment fraud and Ponzi schemes.

HyperLedger Fabric:
Hyperledger Fabric [19] is an open-source collaborative DLT which is permissioned(private) blockchain.
Hyperledger brings blockchain-based distributed ledgers into a wide range of applications. Thus Hyperledger is an `umbrella term' for *open source* distributed ledger platforms and related components and modules. It was created to support the cross-industry domains such as finance, banking, Internet of Things, supply chain, manufacturing and technology. Hyperledger Fabric has modular architecture with plug-and-play modules for consensus mechnism and Ledger services. Hyperledger Fabric can deliver high degrees of

[1] Proof of Work(PoW) is distributed consensus protocol used in Blockchain

[2]

[3] Proof of Stake(PoS) is distributed consensus protocol used in Blockchain
3 Practical Byzantine Fault Tolerance (PBFT)
[4]

confidentiality, resiliency, flexibility and scalability as it is designed to support pluggable implementations.
Unlike the earlier DLTs such as Bitcoin and Ethereumwhich utilize completely trustless networks, HyperLedger assumes trusted netwrok that helps in reducing the computational burden. Moreover HyperLedger is developed by Consortium and hence follows systematic development of the technology by identifying common components, avoiding duplication of effort, promoting interoperability and portability.

R3 Corda
R3 is a distributed database technology company that leads a consortium of more than 70 companies and financial institutions. The consortium's joint efforts have created an open-source distributed ledger platform called Corda[11] which is especially designed for the financial world. Corda has capability to handle more complex transactions and restricts access to transaction data. The goal of Corda is to provide a platform with common services to ensure that any services built on top are compatible between the network participants. Corda's code was open-sourced oin 2016 and may be contributed to the Hyperledger project. Although Corda is inspired by blockchain databases, and is expected to have many of the benefits of blockchains, it is not a blockchain.

Waves:
Waves is another upcoming open-source blockchain platform. This DLT was founded in 2016 by Alexander Ivanov. Waves is community developed software and supports wide range of initiatives built on the platform and based in different locations around the world.
Waves is developed, marketed, and operated by Waves Platform AG that allows members to launch their own custom cryptocurrency tokens. Similar to popular cryptocurrencies such as Bitcoin and Ether can be traded on external exchanges, Waves has a unique functionality in its core software and wallet that allows the members to create, transfer and exchange blockchain tokens on a peer-to-peer basis and paying transaction fees in the native WAVES token. It uses a network consensus algorithm based on Bitcoin-NG, updated for *proof-of-stake networks*, called Waves-NG. Waves uses trusted gateways to issue blockchain tokens. According to the most recent development roadmap published by The Waves Platform, Smart Contracts are scheduled to be added to Full Node software builds during 2018.

Ripple:
DLT Platforms similar to Waves have been proposed and actively being developed. Ripple, a decentralized platform, was one of the first, a kind of distributed ledger a bit like a blockchain, It allows users to send money between each other. The company Ripple is the creator and a developer of the Ripple payment protocol and exchange network. Originally named Opencoin and renamed Ripple Labs in 2015.
Ripple can be conceptualized as a real-time gross settlement system (RTGS), currency exchange and remittance network. Ripple is built upon a distributed open source internet protocol, consensus ledger and native cryptocurrency called XRP. It claims to enable secure, instant and nearly free. Ripple also support global financial transactions of any size with no chargebacks. upports tokens representing fiat currency, cryptocurrency, commodity or any other unit of value. At its core, ripple is based around a shared, public database or ledger[6], which uses a consensus process that allows for payments, exchanges and remittance in a distributed process.

C. Alternatives to *Distributed Ledgers Technology (DLT)*

Hashgraph:
Hashgraph[20] is decentralized platform that aims to be more robust that existing DLTs. Hashgraph is a new consensus alternative to the blockchain. It uses a gossip protocol that works when every node in Hashgraph broadcastssigned information (called events) on newly-created transactions and transactions received from others, to its randomly chosen neighbors. These neighbor nodes will aggregate received events with information received from other nodes into a new event, and then send it on to other randomly chosen neighbors. This process continues until convergence when all nodes become aware of the information created or received. Due to the rapid convergence property of the gossip protocol, every piece of new information can reach each node in the network in a fast manner.
Hashgraph refers to the data structure and consensus algorithm that is much faster, fairer, and more secure than blockchain. It is speculated to be the future of distributed ledger technology(DLT). It uses two special techniques to achieve fast, fair and secure consensus.

1. Gossip about Gossip
2. Virtual Voting

Gossip about Gossip basically means attaching a small additional amount of information to this Gossip, which are two hashes containing the last two members talked to. Using this information, a Hashgraph can be built and regularly updated when more information is gossiped, on each node.
Once the Hashgraph is ready, it is easy to know what a node would vote, since we are aware of information that each node has and when they knew it. This data can thus be used as an input to the voting algorithm and to find which transactions have reached consensus quickly. The history of the gossip protocol can be illustrated by a directed graph, i.e., each node maintains a graph representing sequences of forwarders/witnesses for each transaction. In the ideal case, all the nodes have the same view of all transactions and their witnesses. Further, by performing virtual voting, each node can determine if a transaction is valid based on whether it has over two-thirds of nodes in the network as witnesses. Note that Hashgraph runs in the Byzantine setting, where the assumption is that less than a third of nodes are Byzantine (nodes that can

behave badly by forging, delaying, replaying and dropping incoming/outgoing messages).

IV. Conclusions

Blockchain and related Distributed Ledger Technologies (DLT) are backbone for the decentralized platform that can exchanged digital currency and help autonomously manage financial and real-estate assets. The idea of decentralised Web is re-instantiated as web can ensure trustable, secure and accountable updates among autonomous participants without a central server. This paper surveys the key DLTs and Blockchain variants along with the brief review and cryptocurrencies circulated on these DLTs..

References

[1] Mills, David C., et al. "Distributed ledger technology in payments, clearing, and settlement." (2016).

[2] Mohan, C. "Tutorial: blockchains and databases." *Proceedings of the VLDB Endowment* 10.12 (2017): 2000-2001.

[3] ASTRI. Whitepaper on Distributed Ledger Technology, November 2016, [ONLINE] http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technol ogy.pdf

[4] Deshpande, A, et al. "Distributed Ledger Technologies/ Blockchain: Challenges, opportunities and the prospects for standards." *Overview report The British Standards Institution (BSI)* (2017).

[5] Matthew hancock, Ed vaizey "Distributed Ledger Technology: beyond block chain,A report by the UK Government Chief Scientific Adviser" (19 January 2016). Available at : https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain

[6] Swan M 'Blockchain: Blueprint for a New Economy' O'Reilly Media Inc 2015

[7] Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2014.

[8] Eyal, Ittay, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. "Bitcoin-NG: A Scalable Blockchain Protocol." In NSDI, pp. 45-59. 2016.

[9] Chohan, Usman, Cryptocurrencies: A Brief Thematic Review (August 4, 2017). Available at SSRN: https://ssrn.com/abstract=3024330

[10] Pilkington, Marc. "11 Blockchain technology: principles and applications." Research handbook on digital transformations(2016): 225.

[11] Mike Hearn, "Corda: A distributed ledger" (2016). Available at: https://docs.corda.net/_static/corda-technical-whitepaper.pdf

[12] Julie Maupin, "Mapping the Global Legal Landscape of Blockchain and Other Distributed Ledger Technologies"(2017). Available at: https://www.cigionline.org/sites/default/files/documents/Paper%20no.149.pdf

[13] Satoshi Nakamoto (pseudonym), "Bitcoin: A Peer- to-Peer Electronic Cash System" (October 2008), online: <https://bitcoin.org/bitcoin.pdf>.

[14] Vitalik Buterin, "A Next Generation Smart Contract and Decentralized Application Platform" (2015) Ethereum White Paper, online: <https://github. com/ethereum/wiki/wiki/White-Paper>.

[15] Sergui Popov, " e Tangle" (2016) White Paper, online: <https://iota.org/IOTA_Whitepaper.pdf>.

[16] Kyle Croman et al., "On Scaling Decentralized Blockchains", Financial Cryptography & Data Security 20th International Conference, Barbados, (22–26 February 2016), online: <fc16.ifca.ai/bitcoin/ papers/CDE+16.pdf>.

[17] Iansiti, Marco; Lakhani, Karim R. "The Truth About Blockchain". (January 2017). Harvard Business Review. Harvard University. Retrieved 2017-01-17.

[18] Ongaro, D., & Ousterhout, J. K. (2014, June). In search of an understandable consensus algorithm. In USENIX Annual Technical Conference (pp. 305-319).

[19] Christian Cachin. Architecture of the Hyperledger blockchain fabric. Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL 2016), 2016.

[20] Baird, L. (2016). The Swirlds hashgraph consensus algorithm: Fair, fast, Byzantine fault tolerance. Swirlds Tech Report SWIRLDS-TR-2016-01, available online, http://www. swirlds. com/developer-resources/whitepapers. Chicago