International Journal of Academic Research and Development
ISSN: 2455-4197, Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 2; Issue 4; July 2017; Page No. 304-307

BlockChain: The next generation revolution

Dr. Sandeep Aggarwal

Assistant Professor, DAV College, Abohar, Punjab, India

Abstract
Everyone is talking about blockchain, in the past few it has been evolving as an alternative digital model having vast potential beyond bitcoin or other crypto currencies. It is the technique behind that can work to automate every online transaction with a good degree of trust. The concept of blockchain has energized the financial services industry globally. The concept has already brought a disruption in the financial industry. In this paper we try to understand what the technology is, what are consensus protocol that work behind it and how it is already affecting our lives. Also we try to find out the possible implications of using this technology that can shape our future and can prove to be another milestone in this digital era like the one Internet is.

Keywords: blockchain, bitcoin, distributed databases, consensus protocol, proof of work, proof of stake, cooperative cloud storage, digital identities, online voting, data privacy

Introduction

Over the past few years (since 2008), an alternative digital model has slowly been evolving at the edges of the internet. This new paradigm is called as the blockchain. Blockchain technology has vast potential beyond bitcoin to automate every type of online transaction that requires a degree of trust. Blockchain is a new way to store and record transactions. A blockchain is a public ledger of all bitcoin transactions that have ever been executed. A block is the "current" part of a blockchain which records some or all of the recent transactions, and once completed, goes into the blockchain as permanent database. Each time a block gets completed, a new block is generated. Blocks are linked to each other (like a chain) in proper linear, chronological order with every block containing a hash of the previous block.

Block chain in layman terms is an extension to database, but technically it consists of a peer-to-peer network, a blockchain file, a consensus protocol and a blockchain parser. Blockchain technology works by creating a network of computers (called nodes) which each store a copy of the database, and a set of rules (called the consensus protocol) which define the order in which nodes may take turns adding new changes to the database. In this way, all of the nodes agree as to the state of the database at any time, and no one node has the power to falsify the data or to censor changes. Block chain is a method of storing data in a sequential chain of blocks, where each block is a package of data created within a short consecutive window of time. A block has its own "hash", based on the data it contains, which is like a fingerprint that uniquely identifies it. As time progresses, it gets computationally harder to alter the earlier blocks (they become tamper-proof) [4]. The blockchain participants use a consensus protocol to decide which data gets added next. Each block (except the first "genesis block") contains a reference to the block before it using the previous block's hash, thereby forming a chain. The earlier blocks in the chain cannot be tampered with, because changing a block changes its hash and this would break the chain of references.

Some of the devices on a peer-to-peer network regularly transmit data onto the network, to be included in the next block (the clients). Other devices (nodes, validators or miners) receive and package the data into their own proposed block and then hold a lottery (consensus system) to see which device was lucky enough to create the block to be included. They do this because there is a reward for creating the next new block (public blockchains), or because they are run by entities who value the availability of the blockchain (private blockchains) [4].

The blockchain further requires that an audit trail of all changes to the database is preserved, which allows anyone to audit that the database is correct at any time. This audit trail is composed to the individual changes to the database, which are called transactions. A group of transactions which were all added by a single node on its turn is called a block. Each block contains a reference to the block which preceded it, which establishes an ordering of the blocks. This is the origin of the term "blockchain": it is a chain of blocks, each one containing a link to the previous block and a list of new transactions since that previous block [3]. When a new node joins the network, it starts with an empty database, and downloads all of the blocks, applying the transactions within them to the database, to fast-forward this database to the same state as all the other nodes have. In essence, a blockchain establishes the order in which transactions were applied to the database so that anyone can verify that the database is accurate by rebuilding it from scratch and verifying that at no point was any improper change made.

So, A Blockchain is an audit trail for a database which is managed by a network of computers where no single computer is responsible for storing or maintaining the database, and any computer may enter or leave this network at any time without jeopardizing the integrity or

availability of the database. Any computer can rebuild the database from scratch by downloading the blockchain and processing the audit trail. With use cases in all fields from finance to identity, the stage is set for blockchain technologies to forever change the way we transfer, store, and handle data.

Blockchain Consensus Protocols

Blockchains are governed by a set of rules called the consensus protocol. These rules define which changes are allowed to be made to the database, who may make them, when they can be made, etc. One of the most important aspects of the consensus protocol is the rules governing how and when blocks are added to the chain. This is important because in order for blockchains to be useful, they must establish an unchangeable timeline of events, which must be agreed upon by all nodes, so that all nodes can agree on the current state of the database [3]. Moreover, this timeline cannot be subject to censorship, thus no single node may be entrusted with control over what enters it when. There are a number of consensus protocols:

- "proof-of-work" (used by Bitcoin, Ethereum)
- "proof-of-stake" (proposed for Ethereum)
- "practical Byzantine fault tolerance" (Hyperledger Fabric)
- "proof of elapsed time" (Hyperledger Sawtooth Lake)
- "round robin" (Multichain)

There are currently two main types of consensus protocol: Proof of Work (PoW) and Proof of Stake (PoS). Proof of Work is the original consensus protocol, and is currently used by Bitcoin, Ethereum, and many other blockchains. Proof of Work is based on puzzles which are difficult to solve, but once solved, it's easy to verify that the solution is correct. This is analogous to a jigsaw puzzle: hours of effort are required to put the puzzle together, but it takes only a momentary glance to see that one has been assembled correctly. In Proof of Work consensus, the effort required to solve a puzzle is called Work, and a solution is called a Proof of Work. In other words, the fact that I know the solution to the puzzle proves that someone did the work to find that solution. The solution is proof that someone did work. Blockchains which use Proof of Work consensus require such proof for each new block to be added to the chain, thus requiring Work to be done to create new blocks. This Work is frequently referred to as 'mining.' Proof of Work consensus protocols state that the chain containing the most blocks is the correct chain because it contains the most work. Blockchains which use Proof of Work are regarded as secure timelines because if one node attempted to rewrite history by changing an old block, its change would invalidate the work on the block it changed and all blocks after it by making the Proofs incorrect. In order to convince other nodes that the modified chain is the correct chain, that node would have to redo all of the work in all of the blocks after his change to make new, valid Proofs, and because all other nodes are still making new blocks with new Proofs and adding them to the original chain, the one node would have to redo all of the old work faster than all other nodes combined in order to catch up and surpass the original chain. This is known as a 51% attack, so named because the one node would have to have at least 51% of the computational power (ability to do Work and find Proofs) of all nodes combined. If this attack were successfully carried out, the attacking node would be able to censor transactions from the blockchain, change the order in which transactions occurred, or change transactions that node made (but the node would be unable to change any other node's transactions).

Proof of Stake is a newer consensus protocol which was developed to address some perceived weaknesses in Proof of Work and is currently utilized by Peercoin, BitShares, and several other blockchains. Some of the advantages of Proof of Stake are that no Work is required, thus it requires less energy; the 51% attack is theoretically more expensive; and PoS may encourage a more decentralized network of nodes than PoW. Proof of Stake consensus protocols have more varied rules governing which nodes may create new blocks when than Proof of Work protocols, but in general all PoS protocols specify that block production is controlled by Stake in the blockchain rather than computational power. Stake in the blockchain is balances in the currency the blockchain tracks, thus the greater the balance a node owns, the more say that node has in block production. Proponents of Proof of Stake consensus protocols argue that owners of large amounts of stake will wish to protect their investment and thus will take action to ensure block production continues smoothly and securely. Attacks on the network will damage trust in the network, thereby devaluing the stake. A 51% attack would require the attacker to buy 51% of the stake in the network, which would be extremely expensive since the more stake the attacker buys, the higher the price will rise, and using that stake to attack the network will result in a complete loss since the value of the stake would be destroyed by the attack. This is as compared with a 51% attack on a Proof of Work blockchain, which requires only computing power which typically becomes cheaper when purchased in bulk, and can be repurposed or sold when the attack is complete. It is further supposed that, whereas Proof of Work consensus incentivizes greater centralization because computing power is cheaper with centralized cooling and power, no such incentive exists with Proof of Stake since a typical smartphone has more than sufficient computational power to produce blocks for a PoS blockchain.

Benefits of BlockChain

1. As a public ledger system, blockchain records and validate each and every transaction made, which makes it secure and reliable.
2. All the transactions made are authorized by miners, which makes the transactions immutable and prevent it from the threat of hacking.
3. Blockchain technology discards the need of any third-party or central authority for peer-to-peer transactions.
4. Decentralization of the technology.

Blockchain Applications Shaping Future

i) Cooperative cloud storage

Blockchain technology is at the heart of cooperative

cloud storage, it allows distributed retention of encrypted data. As we know Current cloud storage services are centralized thus the users must place trust in a single storage provider. "They" control all of your online assets [2]. On the other hand with the Blockchain, this can become decentralized. Storj.io and factom are two start-ups exploring this idea. For instance, Storj is providing decentralized cloud storage using a Blockchain-powered network to improve security and using spare disk space allocated by a community of "farmers" who receive rent in Storj's native crypto currency. Here stored files are "shredded" and the shards encrypted and distributed across the available storage – this is where such blockchain features as a transaction ledger, public/private key encryption, and cryptographic hash functions come in. Additionally, users (you) can rent out their excess storage capacity. Anyone on the internet can store your data at a pre-agreed price [2]. Hashing and having the data in multiple locations are the keys to securing it.

For Storj Labs, blockchain elegantly solves many of the challenges around putting your files on someone else's home or office computer or NAS device. In particular, the shards are protected against intrusion, and three copies of each are stored to provide redundancy in case a remote system goes offline. The blockchain stores information such as the network locations of each shard and its cryptographic hash as proof of storage, verifying that the farmer still has that shard and that it is unmodified. After encrypting your data, it is sent out to a network with easy to track basic metadata.

ii) Digital identities

Blockchain technologies make tracking and managing digital identities secure and efficient, resulting in seamless sign-ins and reduced fraud. Be it banking, healthcare, national security, citizenship documentation, online retailing or walking into a bar, identity authentication and authorization is a process intricately woven into commerce and culture worldwide. Due to the lack of common comprehension and often-unchecked cyberspace of personal information, Identity in the context of technology is facing significant hurdles. Events such as hacked databases and breached accounts are shining light on the growing problems of a technologically advanced society, without outpaced identity-based security innovations.

Alongside biometrics, blockchain technology offers a solution to many digital identity issues, where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner. Current methods use problematic password-based systems of shared secrets exchanged and stored on insecure systems. Blockchain based authentication systems are based on irrefutable identity verification using digital signatures based on public key cryptography. In blockchain identity authentication, the only check performed is whether or not the transaction was signed by the correct private key. It is inferred that whoever has access to the private key is the owner and the exact identity of the owner is deemed irrelevant [2]. ShoCard is a digital identity that protects consumer privacy and is as easy to understand and use as showing a driver's license. It's optimized for mobile and so secure that a bank can rely on it. Blockchain technology can be applied to identity applications in various areas like as Digital Identities, Passports, E-Residency, Birth Certificates, Wedding Certificates, IDs, and Online Account Logins etc.

iii) Online Voting

Another application for blockchain technology is online voting. The greatest barrier to getting electoral processes online, according to its detractors, is security. Using the blockchain, a voter could check that her or his vote was successfully transmitted while remaining anonymous to the rest of the world. By casting votes as transactions, we can create a blockchain which keeps track of the tallies of the votes. This way, everyone can agree on the final count because they can count the votes themselves, and because of the blockchain audit trail, they can verify that no votes were changed or removed, and no illegitimate votes were added. We hope that Blockchain technologies will become the gold standard for all nations of the world shortly. It is time for our system and governments to become more transparent [2].

Weakness in the blockchain

One major limitation is that these services are no longer peer to peer, they are intermediaries piggybacking the P2P blockchain to take advantage of its security and verifiability. Likewise, those authorized ledgers are no longer truly decentralized, the network nodes verifying transactions must be authorized to do so. This could make them more vulnerable.

Another more general caveat is that as transactions occur, the blockchain lengthens and grows, yet each node needs a copy of the whole chain. At the time of writing, the bitcoin database looked likely to hit 100GB around the end of 2016. Some of other major problems felt in Block chaining are.

- Data Privacy – everyone can see exactly what you have done on the Bitcoin blockchain, provided that they know your wallet address.
- Anonymity – wallets are by definition pseudonymous, which creates challenges for KYC, AML and financial crime controls.
- Governance around core development is undefined and unregulated.
- Validating nodes (miners) are in a variety of locations globally, and of varying risk categories.
- Lack of customer protection – once an asset is stolen, there is no way to overwrite code or refund money.
- Speed of settlement – currently between 10 minutes and several hours.

Conclusion

As mentioned above, most of these applications are still underdeveloped. Given that crypto-currency bitcoin is the poster-child for blockchain technology, it's no surprise that much of the blockchain fuss and much of the actual blockchain work is focused on payment systems and related areas such as invoicing and tax reporting. The future potential of the blockchain applications is still unraveling. According to blockchain technology developers, there are roughly a thousand companies in

the world focusing on blockchain-related innovations at the moment. Only a small fraction of these companies are working on actual blockchain technology development. At this point, it is still uncertain whether the knowledge and the understanding on this technology will spread enough to attract sufficient numbers of customers, entrepreneurs and developers to reach the critical mass of a stable mainstream ecosystem. Furthermore, many other factors, such as changes in regulation and disruptive developments in competing technologies can affect the attraction in unpredictable ways. The next couples of years will be all about experimenting and applying to all aspects of society. Regardless of which application comes first on a global scale. The bottom line is, Blockchain is here to stay and is transforming how our society functions.

References

1. Blockchain and the promise of cooperative cloud storage at computerweekly.com
2. Ameer Rosaic. 5 Blockchain Applications That Are Shaping Your Future, http://www.huffingtonpost.com/ ameer-rosic-/5-blockchain-applications_b_13279010.html
3. Nathan Hourt. Blockchain Technology in Online Voting, https://followmyvote.com/online-voting-technology/blockchain-technology/
4. Kimmo Rouhiainen, Keir Finlow-Bates, L-001-intro.pdf at www.chainfrog.com
5. LTP, know more about blockchain: overview, technology, application areas and use cases, https://letstalkpayments.com/an-overview-of-blockchain-technology.