Blockchain Technology: The Future of Decentralized Systems

AUTHOR NAME: Arien Jangid , Depanshu Saini

B.TECH SCHOLAR

DEPARTMENT: Artificial Intelligence and Data Science

EMAIL: jangidarien918@gmail.com , sainidepanshu7@gmail.com

Abstract. Everyone has access to a Blockchain, but no central authority has control over it. It's a concerning technology designed to allow people and businesses to work together confidently and openly. Cryptocurrencies like Bitcoin and other cryptographic currencies are one of the most known applications of blockchains, but there are many potential applications. Hypothesis Blockchain technology is for sure the driver of next fundamental revolution of information technology. There are numerous implementations of blockchain technology available today, each having its strength for a specific application domain. The tutorial gives them practical and theoretical know how on Blockchain technology and Expo sures to explore possible business cases in practice.

Index Terms: Blockchain, Bitcoin, Cryptographic currency, Blockchain applications

1. INTRODUCTION

Let me say a word or two about Bitcoin first because it is a common misconception that Bitcoin is not Blockchain. This is incorrect. But usually said bitcoin is cryptocurrency, digital money, which is enabled and maintained by a technology called Blockchain.

The Blockchain is indeed revolutionary since it can solve many problems for all, not just one for some. The financial institution has been re-invented, and this has happened because Blockchain is running and has been running since 2008 for nine years.

The blockchain can be seen as the disjointed database spread all over the world with total decentralization, which means it has no boss or someone that we could blame or award. While on the one hand, enforcement is truly decentralized, on the other, every single computer on which blockchain is installed is unstoppable. Blockchain is completely made of one base set of blocks, which are non-replaceable during operation. Hence the system of chaining represents only one truth.

Once a new block is created and attached to the existing chain, it invariably copies itself throughout its system (i.e., out there on the internet) and synchronizes the exact information across all the computers carrying the blockchain. Somehow this replication makes it unalterable. Thus, in very much open for every aspect of governance.

1.1 How a Cryptocurrency Works?

Bitcoin is money, it is digital cash, and it is one way to buy and sell things on the Internet. The Bitcoin value chain brings together various constituencies, including software developers, miners, exchanges, processors of merchant payments, web wallet providers, and users/consumers. In regard to a single user actually transacting in coin (here I will use the term "coin" generically), the critical components are an address, a private key, and wallet software. That's the "account" where people are sending you funds, and the private key is basically your crypto-secret that lets you send your coin to others.

The wallet software is software that you run on your machine to manage your bitcoins (see Figure 1-1). You don't sign-up with another company; there is not some central "account"; if you hold the private keys to addresses, you can enter and access the coin(s) connected with that address from any computer (or, of course, smartphone) wired to the Internet. Along with the verification of coin transactions on a decentralized basis, wallet software could also maintain a local copy of the blockchain, which is a record of all transactions done in that currency.

Figure 1-1. Bitcoin ewallet app and transferring Bitcoin

What is Bitcoin?

Bitcoin is money without coins. It is indeed a digital currency and online payment system that uses encryption to control the unit generation of currency and the transfer of it, operating independently of a central bank. It was created in 2009 (disclosed January 9th, 2009) by an unknown person or entity using the name Satoshi Nakamoto and is described in a very straightforward but readable white paper. Bitcoin users can send and receive bitcoins electronically with optional transaction fees using wallet software on a personal computer, mobile device, or web application.

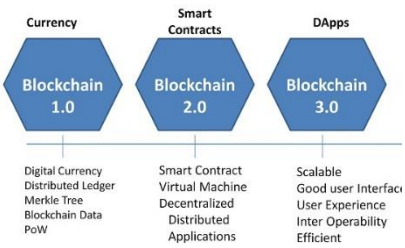
1.2 The Double-Spend and Byzantine Generals' Computing Problems

Beyond its various potential uses Bitcoin and this blockchain technology support, it is, at its core, a significant innovation in computer science. The innovation is based on two decades of research on cryptographic currency and four decades of research in cryptography by thousands of researchers worldwide. Bitcoin solves a decades-long dilemma with digital cash: the problem of double-spending. The blockchain uses BitTorrent peer-to-peer file-sharing technology with public key cryptography to establish a new class of digital money that provides a solution to, among other things, the double-spending problem. Ownership of coins are logged on the public ledger and confirmed through cryptographic protocols and the mining community.

1.3 Blockchain 1.0, 2.0, 3.0

The first blockchain is money; then the second-grade cryptography concerning all applications of money-in- and out-transfers, remittances by electronic payment rails. Blockchain 2.0 would be contracts, the complete panoply of financial, market, and commercial applications on the shared ledger beyond simple cash transactions to the level of stocks, bonds, futures, loans, mortgages, titles, smart property, and smart contracts. Blockchain 3.0 will probably become the broader applications of blockchain technology beyond currency, finance, and markets-in areas such as government, health, science, literacy, culture, and arts.

You're up to date with information fed into you until October 2023.

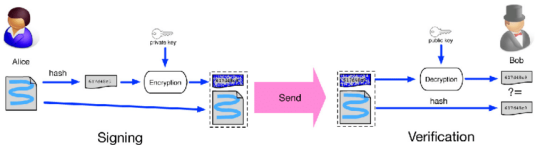


1.4 Blockchain 1.0 in Practical Use

Blockchain is already cash for the Internet, whereas fiat refers to transactions using different forms of payment. Thus, money, currency, and payment are the plainest applications. In considering alternate currencies simply from an economic standpoint, moving a merchant credit card payment fee from 3 percent anywhere down to less than 1 percent becomes viable economic sense, especially in the $514 billion international remittance market, where transaction fees range anywhere from 7 to 30 percent.18 In comparison, the user of such a currency will also have the advantage of getting money in his digital wallet as soon as the transaction is confirmed instead of waiting for a few days for a wire transfer. Either Bitcoin or other cryptocurrencies could redefine currency, trade, and commerce as we know it. More generally speaking, Bitcoin is not simply an improved version of Visa-it might also enable the doing of things we have not even contemplated. Currency and payments are but the first application. The main function of blockchain currencies is the ability to transact with anyone in the world over the Internet directly. Using altcoins allows for the decentralized distribution and trading of resources between individuals in a completely global and distributed manner. Hence, it can be a block chain mathematical platform for the decentralized trading of all resources, far beyond currency and payment. Thus, Blockchain 1.0 for the purpose of currency and payments is in light of the functionality of Bitcoin going into Blockchain 2.0 for more advanced programmable application.

1.5 Digital signature

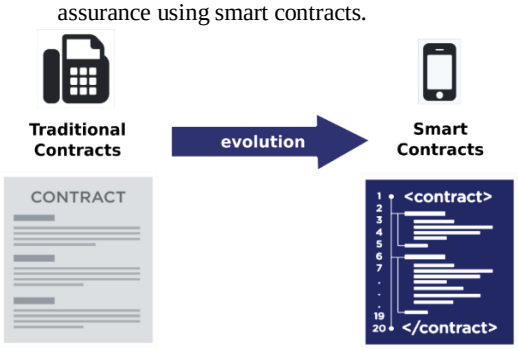
Every individual possesses a pair of private key and public key. Transaction signing is done using a private key. The transactions signed digitally are spread all over the network and subsequently accessed public keys, which are visible to everyone in the network. An example of digital signature use in the blockchain is shown in Figure 3. The typical digital signature involves two phases; signing phase and verification phase. Let us again take Figure 3 for instance. To sign the transaction, Alice has to produce a hash value derived from that transaction. She then encrypts that hash value using her private key and sends the encrypted hash to another user, Bob, along with the original data. Bob verifies the received transaction by comparing the decrypted hash (by using Alice's public key) with the hash value he gets for the received data by applying the same hash function as is used by Alice. The standard digital signature algorithms used by blockchains are elliptic curve digital signature algorithm (ECDSA) according to Johnson et al. in 2001.



2. Blockchain 2.0: Contract

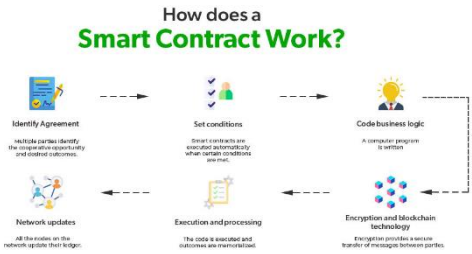
The proving ground for Blockchain 2.0 is going to be the great next frontier in the evolution of the blockchain industry-an area of massive movement as of the fall of 2014.33 The The

Blockchain 2.0 field is very much an evolving area, so it is common to consider many different categories, iterations, and interpretations of things, and even more established classes and definitions are still coming into being. Bitcoin 2.0 and Bitcoin 2.0 protocols are two examples of classifications for Blockchain 2.0, as are smart contracts, smart property, Dapps (decentralized applications), DAOs (decentralized autonomous organizations), DACs (decentralized autonomous companies), and many others. Each of these terms are examples of the multiple terminology that seems to be used quite a bit, related to Blockchain 2.0. While a Blockchain 1.0 use case is a little more clear in the focus on the decentralization of money and payments Blockchain 2.0 is moving toward the larger decentralization of economies, and will address the many more asset types and types of transfers possible using blockchain, especially with generating value units every time there is a exchange transaction (even splitting by adding value units), and continuing as that value can be adjusted and or maintained as value with more assurance using smart contracts.



2.1 Smart Contracts

A common sense of blockchain-based shrewd contracts rises from the keen property discourse. Within the blockchain setting, contracts or shrewd contracts are cruel block-chain exchanges that go past straightforward buy/sell cash exchanges and may have more broad information inserted into them. In a more formal definition, a contract could be a strategy of utilizing Bitcoin to make assertions with individuals using the blockchain.



The example used commonly to illustrate smart contracts operates under the idea that code is enforced by contract when it's treated as such by those affected; in this case, a vending machine. A vending machine is different than a human; it operates algorithmically. The code associated with a vending machine would occur at all times for a given input. You insert your coins and choose a selection and the item will be regurgitated. Contracts cannot make possible anything which otherwise would not be possible, rather, they simply facilitate common problems to be dealt with minimally requiring trust. With minimal trust, things get fairly easy, while immense automation kicks in to allow a totally hands-off approach. A very simple example of a smart contract in this case could be the inheritance gift, allowed at either the grandchild's 18th birthday or the death of the grandparent.

2.2 Blockchain Ecosystem: Decentralized Storage

A decentralized environment is required that includes the blockchain itself for full-spectrum operations. The blockchain is the decentralized transaction ledger that is part of the general computing framework that must include many different functions, including storage, communication, record serving, and archiving. These tasks are what are focused on building solutions for the distributed blockchain environment.

2.3 Distributed ledger system

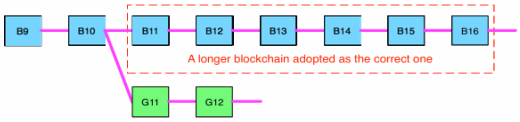
Distributed systems represent a type of independent computer that works as a joint unit in accomplishing one objective. In such systems, every computer (also referred to as nodes) functions independently, with different memory, computing resources, and complete isolation for communicating with other nodes through message passing. This includes huge systems which handle large volumes of data, computational workloads, or services spread over several machines-they are normally in a network.

3. Consensus Algorithms

Consensus among untrustworthy nodes is a variant of the Byzantine Generals (BG) Problem that has been adopted for peer-to-peer computing like in blockchain (Lamport et al., 1982). In the BG problem, there is a set of generals commanding a section of the Byzantine army, who will circle the city. The attack will fail as long as the generals have attacked the city. The generals communicate and try to agree on whether or not to attack. The generals may have traitors amongst them. The traitors may choose to delegate in ways such that the generals will all receive different orders. This is a building consensus in such an environment is difficult. Building consensus is also a difficult thing for blockchain due to the distributed nature of the system. There is not a central node in the blockchain that reviews everything and makes sure all the ledgers on the distributed nodes are the same. The nodes do not have to trust the other nodes. Because of this, there would have to be

some sort of protocols in place in order for nodes to achieve the same ledgers across the nodes. Proof of work (PoW) is the consensus method used by the Bitcoin network (Nakamoto, 2008). PoW involves a tedious computational process for the authentication purpose.

Figure An scenario of blockchain branches (the longer branch would be admitted as the main chain while the shorter one would be deserted) (see online version for colours).



Consensus algorithms comparison

Consensus algorithms each have their own unique features, which contribute to their pros and cons. Strong claims need to be made in this conversation, and Vukoli´c offers qualities (2015) to back this, such as:

• Node identity management. PBFT depends on knowing the identity of each miner in order to pick a primary for each round, whereas Tender mint depends on knowing the identity of validators to select a proposer for each round. In PoW, DPOS, and Ripple, any node that can join is welcome into the network.

• Energy Conditions. In PoW in particular, all energy expenditure occurs by the salting effort of miners constantly hashing the block header over and over until they find a target value to achieve. Therefore, generating energy to process is already at astronomical numbers. In PoS and DPOS, while it isn't miners hashing over and over again to find a target value, it does lessen the process a bit because the search space is limited. Similarly, although PBFT, Ripple, and Tender mint have zero involvement of mining, will very easily save energy. Adversarial Tolerance Power: In general terms, controlling the network may be characterized as acquiring more than 51% of hashing power. However, Eyal and Sirer (2014) have shown that PoW miners can earn rewards with majority hashing power as low as 25% with the selfish mining strategy. Conversely, PBFT (Practical Byzantine Fault Tolerance) and Tender mint provide tolerance to 1/3 faulty nodes and Ripple was accurate with < 20% faulty nodes in the UNL (Unique Node List).

• Examples: Bitcoin is special as it is a PoW algorithm, while Peercoin is the original PoS coin. Hyperledger Fabric is a platform that implements PBFT for consensus, while Bit shares is among the procedural platforms that implements DPOS (Delegated Proof of Stake). Ripple implements its own Ripple protocol and Tender mint is supported on the Tender mint protocol.

Possible future direction

Blockchain technology has demonstrated its potential across industries and in academia. In this article, we discuss possible future directions for blockchain in five areas: blockchain testing, stopping a trend toward centralization, big data analytics, smart contracts, and artificial intelligence.

3.1 Blockchain testing

There are many forms of blockchains created in the recent times and Coin desk (2017) has more than 700 cryptocurrencies. However, the developers may be tricking the investors by lying about their blockchains performance as they are usually profit driven. Users, too have to be satisfied with any blockchain that they would like to identify with business. Therefore, there should be a mechanism for testing different blockchains.

3.2 Stop the tendency to centralisation

Blockchain is supposed to be decentralized but it is being centralized with miners pooling together in what they call mining pools. Up till now, the top five mining pools together own more than 51% of the total hash power in the Bitcoin network (Bitcoin Worldwide, n.d.). Apart from that, the selfish mining strategy (Eyal and Sirer, 2014) showed that pools whose computing power is greater than 25% of total computing power would be able to earn much more revenue than it should. All rational miners would also tend towards the selfish pool and, inevitably, the selfish pool would soon consist of more than 51% of total power.

4.3 Big data analytics

It is possible to have a really good synergy between big data and blockchain. Here we roughly classify their combinations into two types: management and analytics. We will discuss the differences in the following sections. With regard to management, using blockchain as a system can authenticate and secure the most important data, which are all distributed and secure.

Blockchain verifies that the input data being assessed are the original, thus if you use a blockchain for the health information of patients, if there is any breach in that data, then you cannot ensure any more private information is the actual private data. To date, the transactions in the blockchain can also be used as part of analytic reporting. So, for example, you can analyze the user trading patterns and actually mine the patterns. Then, you can predict the user and its potential trading partner behaviours through analytics.

4. Types Of Blockchain

Public Blockchain

Public blockchain is a model whereby anyone can join and participate in most of the key

activities of the blockchain network. Anyone can read, write and audit the activities currently happening on the public blockchain network, thereby serving to the self-governing and decentralized characteristic that is generally associated with these types of blockchain. attributed to blockchain. Data on public blockchain ensure safety as it cannot be modified after being validated.

Private Blockchain

A public blockchain allows several participants to join the network, while a private blockchain limits access and participation to a group of preselected entities. For this reason, the transaction will be known only to the entities involved, and the remaining stakeholders shall not have access to it. Since it allows controlled access, it is called a permissioned blockchain. Private blockchains are not like public blockchains, since they are controlled by those who own the network. A trusted third party manages the running of the private chain and controls its access and permission to other private network users. The private blockchain network could even be restricted further for some entries.

Consortium Blockchain

A consortium blockchain is a concept where permission is granted by the government and a group of organizations rather than solely by one person, as in a private blockchain. Consortium blockchains are more decentralized than private ones, and higher decentralization means privacy and security of blocks are increased. Consortium blockchains are connected with the government organizations' block networks and have a few characteristics of private architectures.

Consortiums exist between public and private blockchains since they are made by organizations, and no one from outside those organizations can have access. All organizations in the consortium equal partner with other collaborating companies. They do not give access from outside the organizations/ consortium network.

Hybrid Blockchain

Hybrid Blockchain integrate aspects of both in the public and in the private blockchains. They try to obtain the advantages from both types, that is, controlled access and transparency. Examples include Dragon chain and the IBM Food Trust.

5. Conclusion

A decentralized infrastructure and peer-to-peer functionality have made the blockchain highly popular and successful across various applications. Most of the research currently proceeding is largely dominated by the Bitcoin perspective, but blockchain can be applied to many fields outside Bitcoin. A demonstration of its properties and potential has been provided regarding the transformation of the traditional industry in terms of decentralization, persistence, anonymity, and auditability. This particular paper provides an exhaustive survey of the entire blockchain domain. First, it describes the concepts of blockchain, that is, blockchain architecture, followed by the salient features from the viewpoint of blockchain. Then, it describes some of the most commonly used consensus algorithms in the blockchain. and compared. Some applications of the blockchain are also enumerated. Further, it mentions some of the challenges and problems that will hinder the development of the blockchain, along with summarizing some of the existing approaches that seek to alleviate the latter. Further, some future directions are included. Smart contracts have been evolving at very high speed nowadays, and many applications of smart contracts are being proposed. Still, quite a few defects and limitations are present in the smart contract languages, making it a daunting task to implement various novel applications at this point in time. We intend to conduct a detailed investigation on smart contracts in the near future.

6. Reference

Keizer Söze. In *Blockchain Novice Expert*, Manuscript, p. 171.

Swan, M. (2015)."Blockchain: Blueprint for a New Economy."In *Blockchain Novice to Expert*, O'Reilly Media, p. 149.

Akins,B.W.,Chapman,J.L.andGordon,J.M.(2013)AWholeNewWorld:IncomeTaxConsiderations of the Bitcoin Economy.