A Collection of Articles and Essays by

Pooyan Ghamari

Blockchain & Technology Visionary

A Collection of Articles and Essays by Pooyan Ghamari

Compiled in 2022

Table of Contents

1

An Introduction to Blockchain

Blockchain is a database with the feature of simultaneous access in many computers. This database steadily develops and gets larger by adding different blocks and data to it. Blocks are the data sets or unregistered information which are recorded in the Blockchain database and system.

It can be claimed that currently there is not any technology which is attempting to dominate the world market to the extent that Blockchain technology is. You might haven't noticed it and feel that this term is one of the common terms in the world of technology with which you will not have anything to do. However, the fact is that in the coming years, or it is better to say, in the near future, a large volume of the world's financial burden will be on the shoulders of Blockchain. In a short time, you will witness the effects of using Blockchain in various industries in the fields of medication, financial affairs, communications, teaching, and the food industry. However, what is this important and novel phenomenon exactly? How does it work and what benefits does it have?

Blockchain Definition in Layman's Terms

Blockchain is a database with the feature of simultaneous access in many computers. This database steadily develops and gets larger by adding different blocks and data to it. Blocks are the data sets or unregistered information which are recorded in the Blockchain database and system.

The registration time for each block in the network is definite, and each block is linked to the previous one or the data sets previous to it. As a result, together, blocks form a chain. No organization or individual undertakes the responsibility or duty of managing these blocks and data. However, whoever is present in this set, will have a copy of all network data.

Old blocks remain in the network forever, and new blocks are added to the system, and there will not be the possibility of canceling them after being registered in the Blockchain network. So, manipulating existing data in this network through fake documents is not possible at all and all information and transactions done in it will be registered in the system forever; in other words, no one can remove the data or cancel the process of data registration after registering them.

Blockchain Data Encryption

All the existing data in Blockchain are encrypted in a particular way. All can have access to all information present in the network, but just the user who holds specific network encryption key can add new data. As long as this user is the only person who knows about the mentioned key, no one is able to impinge on his transactions. Blockchain is an independent and safe network which has a transparent performance.

Growth and Performance of Blockchain in the Field of Cryptocurrencies

In 2008, an individual or a group named “Satoshi Nakamoto” employed Blockchain system as an infrastructure to apply digital currencies. Bitcoin was the first digital currency which came to be for peer-to-peer trades. The transactions and trades conducted via Blockchain infrastructure and wherein Bitcoin is exchanged as a digital currency are very secure, and no foundation or organization will be able to control these trades. In fact, transactions in Blockchain infrastructure remove middlemen from different transactions.

Blockchain applications are not limited to cryptocurrencies. This system can be employed in different cases. For example, using Blockchain network in tracking factory products in the value chain is among remarkable applications of Blockchain. With the help of this network, the route of each product can be tracked from the moment it is manufactured up to reaching the final customer. These are just some examples of Blockchain applications. The benefits of this novel technology can be seen in medical sciences, education, and communications.

2

Privacy in Blockchain Technology

Anonymity and privacy are not just an advantage for Blockchain users. In case the users' digital asset is lost due to cyber accidents, tracking the attacker and retrieving the asset will get very problematic. However, there is no doubt that Blockchain has improved the issue of the users' privacy to a new level. The level wherein preserving the users' private information is more important than any other principle.

Privacy is one of the most important issues related to the world of technology today. Even the most pertinacious analysts have not predicted the issue of preserving privacy in the digital space to find such importance. In fact, it can be alleged that currently preserving privacy has turned into the most vital demand for the majority of the users in the atmosphere of digital communications and trades. The reason is absolutely clear. Each year billions of people make their personal, occupational and familial information available in the digital world. The news of selling Facebook users' information has unveiled a new aspect of privacy. This event was so effective that the value of the Facebook stock has dropped more than 10 billion dollars after the news of the users' information being sold was confirmed. Privacy has actually become an issue related to people's personal rights and a moral or even economic subject as well.

Developing Blockchain technology gives the hope of a better space to preserve privacy in the digital world. Having a decentralized and transparent ecosystem and also an encrypted communication, Blockchain prevents the relationship between the third party and the sent messages and transactions. These features cause making censorship, manipulation, and surveillance of digital information difficult in the large scale.

One of the significant elements in preserving privacy in Blockchain is using private and public keys. The mechanism of using public and private keys plays a significant role through providing anonymity in preserving Blockchain users' privacy. The user should generate a set of public and private keys to use Blockchain services. The public key will be available for the other network users while the private key is only in the hand of the user him/herself. Although public and private keys are mathematically related, finding the private key through having the public key is indeed impossible. The message which is encrypted by one of the keys will just be decrypted by the other key. After generating pairs of public and private keys in the Blockchain network, an address is allocated to each user; this address is the user's public key hash.

The address is used to transfer assets in Blockchain, and the transactions' history can be tracked using the addresses. Each user is diagnosed with his/her address. Similar addresses are like random IDs which keep the user's main identity hidden from the others. Moreover, the user can alter his/her pair keys in time in order to make his/her activity tracking impossible. Private keys are used to authenticate the user's identity for getting access to his/her assets. No information is stored from the user's identity such as the name, contact information, address and the like; each user is present in the network at least with one address as it was mentioned.

Each block of Blockchain provides transactions' transparency through giving the sender's address, the receiver's address, and transfer volume. Although the users' real identity remains hidden with private and public keys, from the viewpoint of many, its transparency is in contradiction with preserving privacy, and they are unwilling to clarify such information in the network. Hence, in recent years, through employing encryption science developments, new versions of Blockchain have been offered which were able to provide a higher level of preserving privacy for the users. Monero and Zcash are two examples of such structures.

Monero has entered this field through offering Ring Signature-based structure in preserving privacy beyond its rivals. Ring Signature was first introduced in 2001 in Asiacrypt conference in the field of encryption. In this encryption method, each group member can sign a message without making clear the person who has signed. In Monero network, the sender, receiver and the amount of transactions are not specified for the other people; moreover, there will not be the possibility of calculating users' asset. Even two transactions with the same origin and destination cannot be specified.

Zcash keeps hidden the sender and receiver's address and the amount of transactions through a protocol called ZKP (Zero-knowledge proof). Via this protocol, the person can prove being informed about message X without publishing it for the other. A version of ZKP used by Zcash is named zk-SNARKs.

Preserving privacy in Blockchain technology is so high that it even has drawn the attention of Dark web users. Currently, most of the financial transactions of the black trade are conducted using different cryptocurrencies in this network. Using cryptocurrencies in illegal trades like drug and money laundering has always been among the states' worries in developing this technology. From the one hand, hiding the identities will cause difficulty for them in tax collecting from the people who buy and sell cryptocurrencies. Japan has forbidden giving services to the crypto-exchanges without knowing the main identity to combat this challenges.

Anonymity and privacy are not just an advantage for Blockchain users. In case the users' digital asset is lost due to cyber accidents, tracking the attacker and retrieving the asset will get very problematic.

However, there is no doubt that Blockchain has improved the issue of the users' privacy to a new level. The level wherein preserving the users' private information is more important than any other principle.

3

Blockchain, the Beginning of the Financial and Security Revolution

Since the launch of the new banking system in the 19th century, the centralized financial system and the lack of possibility of carefully analyzing financial transactions and the possibility for tampering with bank data have been considered a serious problem. It cannot be denied that traditional banking and financial transfers, although having many advantages, have always had the possibility for financial corruption and money laundering due to the centralization of financial power in a main managing center. It seems that with the advent of Blockchain technology, banking systems are changing at high speed. Of course, it should be taken into account that although the advent of Blockchain technology was aimed at developing financial systems, its application has grown so much so today that no specific limitation can be regarded for it.

Blockchain technology is only ten years old; in fact, it was only ten years ago that this revolutionary technology was born! However, in this short amount of time, its impact has been equivalent to the impact of some of the most important innovations of the 20th century. However, before anything perhaps we need to know what Blockchain is and how it works so that we can discuss its advantages, how it should be used and its future.

Blockchain and How It Works

Blockchain is made up of the two words block and chain. In fact, this technology is a chain of blocks. Generally, Blockchain is a type of data registration and reporting system. Its difference with other systems is that the data stored on this type of system is shared among all members of the network and with the use of encryption the possibility of removing and manipulating the registered data is almost impossible.

Bitcoin was the first application of this technology and used Blockchain to store the information of users' assets. If Blockchain were an operating system, Bitcoin would be the first software on this operating system. Any information can be stored on any block; from the crimes of a person to the account info of assets such as Bitcoin. In this technology, data are stored on blocks and are related to each other through chains. Next hash blocks include previous hash blocks, and in fact, data are constantly being confirmed. Hash is reached on each Blockchain with a special mathematical function that is specified by the developers. The smallest change in the information of a block will change its hash completely.

For example, if a character is added to the information of Swiss towns, hash block changes and thus other blocks will no longer be valid, and this is why this technology is called Blockchain or the chain of blocks.

If someone changes the content of a block and updates the hash of the next blocks, what will happen? This is possible, but the distribution in the Blockchain network needs to be considered. Blockchain data are not stored on a computer or a certain server. Any computer or system that gets connected to the network will receive a version of the Blockchain.

In fact, Blockchain technology is not a fundamental technology on its own, but it is the combination of hashing processes, collective distribution, and a number of other different technologies that have led to the formation of the idea of Blockchain. With the coming together of different technologies the concept of Blockchain technology is completely made up of three foundational and main technologies. None of these three technologies are new. However, their collaboration with each other forms a new technology.

The three principles of Blockchain technology are:

1. Encryption and the private key.
2. Distributed network and public ledger.
3. Rules and an incentive (usually financial) to persuade users to collaborate in confirming transactions, keeping their records and maintaining the security of the network.

The existence of a unique electronic signature for each transaction in Blockchain guarantees ownership for users, but only controlling ownership is not enough to maintaining the security of digital communications. Even though the problem of identity is solved with public and private keys and digital signature, the activity in Blockchain should be as free as it is safe and anyone should be allowed to make and confirm transactions. This is realized with a distributed network.

How Blockchain works exactly is very complex which requires an analysis on its own. As a simple user, to use the Blockchain technology, you do not need to know how it works. Just like using the internet you do not need to know how it works.

The Importance of Blockchain and Its Applications

Blockchain as a new solution has many applications and usually in any field a special and custom type of Blockchain is used. For example, the block of cryptocurrencies and the Blockchain used for tracing foodstuff are completely different in terms of how they work, but the main principle in them is the same. However, to understand better the importance of Blockchain, its relative advantage must be analyzed with respect to any similar system.

The advantage and the need for a distributed network is understood with a better example (if a tree falls). If a tree falls in a forest and we had recorded the moment of falling with thousands of cameras, we are certain and have visual proof that the tree has fallen, even if its details (how or why it happened) are not clear. Most of Blockchain's value is that it has a large network. In this network, people who are technically called the validators are like people who have cameras, and record evidence and come to an agreement regarding them. However, in here, instead of a camera, the confirmation of evidence is based upon mathematics. In simple terms, the size of the network in a Blockchain is important for its security.

One of the most interesting features of Blockchain is processing power. In fact, the processing power in a Blockchain network can compete with the combined transaction power of hundreds of banks, and with the combination of encryption (private and public keys) with a distributed network, a very functional form of digital interactions becomes possible.

By elaborating the way Blockchain works and defining it, we can also enter the discussions about its future and capabilities. In fact, by understanding function, the importance of Blockchain becomes more clear. Blockchain is a very important technology that can increase security and proof of work in any financial, economic, social or even political ecosystem in an unbelievable way.

The issue of security and reliability is so important that even large food companies in the world such as Nestle use it to trace foodstuff, production date or the way source materials are mined. Sierra Leone is the first country in the world that has held an election with the help of Blockchain technology, and it can be said that the possibility of manipulation and fraud in the votes can lean toward zero with the help of Blockchain technology.

Blockchain and Banking

Bank and banking are among the most important markets in the world. Many of the financial, political and even cultural affairs in the world are tied to these very banking affairs and its varied services. However, on the one hand, the Blockchain technology has made a lot of traditional banking systems frightened.

Payment systems and banking services with the help of the virtual world and a variety of different software have experienced much growth. However, the launch of the decentralized system of Blockchain, through which there is no need for middlemen in financial trades, is making a huge revolution in the world. What does the elimination middlemen from transactions and trades mean? Are banks and financial services institutes afraid for no reason? Is the fear of Blockchain swallowing all the opportunities and statuses of todays' banks an illusion?

This surely is not the case. The fear of traditional banks of the advent of a Blockchain that can without wasting any time and money turn into a connecting bridge between people is seemingly very logical. The truth is that banks are not fast enough in performing banking activities. This leads to different international markets not having enough speed for interactions and trades. Also, the middlemen and the need for decentralized systems that connect the sides of trade with each other with the help of a third party require a very high cost for trades. Therefore, the need for a decentralized system seems to be ideal.

Blockchain is one of the most important infrastructures that can organize economic activities. All the activities that take place between two people or companies in this platform are registered in detail and precisely. Therefore, the possibility of tracing each transaction is very simple. In such a network, there is no sign of central organizations and institutes to organize this whole thing. Therefore, each company and person should oversee his own activities. It seems that in this condition. The financial system of companies will also be revised, and a sort of self-regulation will take place in them. The activity of Blockchain should not be mistaken for cryptocurrency trades.

Transactions that take place using cryptocurrencies are a part of possible activities with the Blockchain platform. This infrastructure can be used in education, communication, politics, voting, and other different matters. In fact, anywhere that there is the talk of a free communication system, Blockchain can be used.

We cannot talk about the future of banking or Blockchain with details and offer predictions regarding them. However, it is obvious that both of them in order to survive and grow in the future will require the collaboration of one another. Many financial and Fintech companies are developing their services based on Blockchain, and this indicates the possibility of a collaboration taking place between banking and new decentralized technologies. Though we should pay attention to the fact that many of the world’s reputable banks are currently using or developing Blockchain technology to increase their security and the speed and capacity of transactions and processes. Bank of America is one of the largest U.S. banks developing an exclusive Blockchain system for financial transactions. From the other hand, this bank currently used this technology to increase the efficiency of its ATMs.

Blockchain and User Security

If we want to address the issue of security, Blockchain can connect millions of users across the world without the need for a middleman, and this means communications will have security without the need for overseeing from central organizations and institutes. It seems that Blockchain can prevent scams and frauds from taking place in different transactions and trades of users and prevent the data from being stolen on the internet.

Blockchain network is developed and designed in a way that there is no central overseeing involved in it. Any user present in the network can have a role in creating and storing the data. All users have a role in creating and confirming the data. Therefore, eliminating or tampering with the data will be impossible.

To destruct the Blockchain network and doing scams in it, hackers should destruct the data that is registered in the computer of each user. There are millions of computers and users, and this makes the possibility of fraud and scam lean toward zero. As a result, even if a huge number of computers are hacked, there will still be numerous other computers known as nodes in the network that hold the previous data. So, hacking the data in the Blockchain network is mostly impossible.

This complex structure leads to an increase in the possibility of protecting data in the virtual world considerably. Such an infrastructure is not only limited to financial matters. This communication structure can be used to register and preserve various data. Registering and preserving data on the Blockchain reduce the possibility of fraud from any data to be minimized.

Presence and living in the virtual world get more widespread by the day. Different aspects of technology are being developed, and their entrance to the lives of even ordinary people will create the need for a new form of data protection. On Blockchain, we are faced with a very wide network that is very difficult to steal or tamper with its data. Up to now, some companies have attempted moving their data centers to the Blockchain infrastructure, and this shows that other companies will soon join this network. In fact, the capacity of Blockchain for turning into the number one choice of companies and institutions is very high.

Such a system helps the chaotic world that is being exploited by superpowers in many different ways and provides the possibility of free space for everyone. With the help of Blockchain, many of the economic transactions that are under different sanctions are put aside. Free communications are a right that Blockchain will offer to anybody in any corner of the world, and it will provide further financial, political, and even cultural and social matters in an unlimited and borderless way.

Blockchain and Developing the Food Market

It was earlier mentioned that the food market is one of the largest industries in the world and is one of the most important concerns in the field of global health. Food, hygiene, and health industries are also looking to use Blockchain.

Due to the weakness in the health care system and the lack of proper planning in the field of hygiene and health, the speed of its growth and efficiency is not all that great. Though when we say it is not that great, we do mean the production of medicine and medical tools. However, we have an integrated network in mind through which using different services and amenities on a wide scale is possible for everyone.

By using Blockchain, we can create a network of data that are tamper-proof and have enough transparency. One of the main problems in the health care systems is the problem of transferring medical data and patients' information from one part to another.

Given the existence of Blockchain, all parts of a medical system have access to a network where patients' information and medical data have been registered in fully and completely without any change. Patients' data and cases will be kept easily with the help of the Blockchain system, and access to them will be easier and faster.

In addition to organizations and hospitals, patients can also have access to the process of their cases being completed and follow up on them via Blockchain. As a result, many of the extra and bureaucratic organizational costs will no longer exist with this technology.

Yet, some Blockchain critics believe that this system lacks the needed efficiency in the field of hygiene and health, though most of these critiques are merely for trial versions. However, even the most pessimistic critics admit that with the development of Blockchain the increase in the efficiency of the hygiene and health management systems can be expected.

Blockchain and Change in the Social Infrastructures

Social networks are also moving towards Blockchain. Not much time has passed from the great enthusiasm that different social networks were met with. The world is completely interested in the capabilities that colorful networks such as Facebook and Instagram offer. The capacities of these networks is really high and interesting. Given the existence of such networks and in general the virtual network, communications have had unbelievable growth and infrastructures such as Google have impacted the entire world with their varied services. However, the story of colorful technologies does not end here. With the advent of Blockchain technology, communications are taking an entirely different form. We no longer need to be worried about users' data being leaked from different social networks. There will no longer be the possibility of exploiting communication platforms and using users' data for advertising and political purposes. However, how?

Ghost Talk is one of the modern technologies based on Blockchain that has entered the market and uses a decentralized payment platform for giving rewards and gifts to users. In fact, users that enjoy the services of this platform's social messaging system will have access to some features and will be able to receive scores.

Unlike other social networks, Ghost Talk considers some rewards and scores for content creation, sharing and in general users' activities on the network. These rewards and scores include token rewards and cryptocurrencies that are able to be stored on the Ghost Talk electronic wallet.

Ghost Talk gives much importance to content creation, and in the network that it has developed, improvement and advertisement are possible. It means that people, companies and especially small businesses can use this infrastructure for their advertisement and create content in it. Any content creation in this network will have benefits and rewards that can later be turned into token and cryptocurrency. What makes the future of Ghost Talk very bright in the mind of the very skilled experts and makes them look at Ghost Talk with optimism, is the precise strategy that it employs in its outlook. Among the suitable strategies of this service is the possibility of advertisement and content creation that offers a win-win scenario for all the beneficiaries and users.

Among the advantages of the advent of the development of different social networks such as Ghost Talk is preparing the basis for further growth and collaboration between cryptocurrencies. The acceptance of different cryptocurrencies as a tool for making transactions in these new infrastructures can make their market even hotter than before and give legitimacy to these cryptocurrencies. Currently, the capacity of cryptocurrencies and a network such Blockchain is no secret to anyone. Everybody knows that sooner or later we will see the ever more growth of these new technologies. However, what can facilitate the growth of these new technologies like a catalyzer, is more relationships among cryptocurrencies and different platforms. If the possibility of making transactions and doing activities with different cryptocurrencies in various platforms and networks is provided, we will see a heavier and hotter competition market from them.

The Importance of Blockchain

It should be expected that sooner or later many of the most important world's industries will look at the Blockchain technology as a modern solution for financial, security, and information issues. The importance of Blockchain's financial potential is so much so that the global economic forum expected in 2015 that until 2025 more than 10 percent of the global GDP will be stored based on Blockchain technology. On the other hand, it is expected that until ten years later more than one-third of the global health and hygiene industries will use the Blockchain network to protect their users and customers' information. This growth will not only include companies in the field of manufacturing medicine, but it will also include information management systems of hospitals and medical centers. So it can be expected that in the third decade of the twenty-first century, Blockchain technology will become an inseparable part of different industries in the world.

All of these are directly related to large industries or even macro-economic or social policies. However, what are the direct advantages of Blockchain technology for mankind? Perhaps this question can be answered better by analyzing the advent of Blockchain in important social and economic fields.

Registering Property

Blockchain considerably increases the efficiency of registering any kind of data, and at the same time, the registered data are completely transparent and are subject to view by everyone. Since properties are among the things that the possibility of fraud is high in them and their registration process is very costly, this technology can be used to increase the efficiency of its function. So far a number of countries such as Russia, Honduras (2015), and Georgia (2017) have turned to Blockchain in registering properties.

Poll

Blockchain can be used to deploy a polling system. However, the most important and main difference in Blockchain poll with common polls is in the "validity of its data." Since in Blockchain changing and tampering with data is not possible and if for example, 70 percent of people say that option one is better than option two, no one can change this 70 percent into 69 percent. While there is the possibility for fraud usual polling systems! Validating and avoiding fraud in electronic elections that are held using Blockchain are really interesting on their own.

Supply Chain Management

Currently, some startups have been created that work in the field of the supply chain. In order to manage the supply chain, Blockchain technology has traceability and efficiency advantages. Blockchain can be used to track the movement of goods, their source, and quality specifications. Therefore, they bring a new level of transparency with themselves. Also, simplifying processes such as transferring ownership, insurance, production process, and payment are among other advantages of using Blockchain.

Food Industry

Food fraud has turned into a prevalent problem in the global food industry. It is true that there is not a shared, global definition for food fraud, but it can generally be said that "any attempt to manipulate food, offering false advertisement through tags and adding unhealthy food supplements for financial gains, are within the definition of food fraud."

Blockchain helps increase the transparency of the food supply chain. When a food item is transported, its related data are added on the Blockchain. This is repeated for the process of changing or adding new material to that food item, and as such, when the final item is exhibited on the store shelves, all the existing spots in the food chain related to that item are updated and completed. Data will be available evenly for the regulator and for consumers, and this provides a high level of transparency.

Education

Educational institutes, universities, and schools can use Blockchain to store the data related to evaluation tests, registering and offering educational documents and licenses, confirming student exchange, and also science and technology transfer.

Cryptocurrencies

The sudden growth of Bitcoin and crypto markets was not for no reason and without merit. These currencies allow for fast, secure, and cheap money transfer all across the world. While there are financial service providers such as PayPal that perform international transactions, but they ask for much fee per each transaction. Other peer-to-peer payment methods usually have certain limitations. For example, spatial limitations and limitations in the least amount of money that can transferred. It is for this reason that businesses, much like regular users, are turning into using cryptocurrencies, not just because they are more secure, but also for providing freedom and the lack of central power in charge of accounts.

Smart Contracts

Smart contracts were first suggested by Ethereum. A smart contract is actually a programmable contract which is placed on Blockchain until the parties perform the considerations written in it. As soon as the considerations are performed, the aimed program will automatically run. For instance, a contract can be defined to send a specific amount of Bitcoin to a specific wallet in a specific day in the month (e.g., for paying a home rent). Smart contracts, too, like other existing transactions on the Blockchain, cannot be removed.

Using smart contracts, you can perform your considerations and transactions without the need for a middleman or a third party. This contract is, in fact, some computer codes which are stored in the Blockchain platform. Smart contracts include all information related to the contract terms and performing all the clauses of the contract is carried out automatically. By using these contracts, both parties of the contract are comfortable with the thought that they will get what they want.

Accounting

In fact, the nature of Blockchain has been inspired from accounting, and one of the best applications of Blockchain is in this area too. Registered transactions via Blockchain effectively omit human errors and protect information from accidental manipulations. All the records should be confirmed each time it is transferred from a Blockchain node to the next one. In addition to accuracy, guaranteeing your records will be traceable like a high-level ongoing audit process.

Of course, the whole process of basic-level accounting becomes more efficient. Instead of keeping records separately, the businesses can have a shared unit registry. Financial information integrity of the company will be guaranteed.

Energy Distribution Network

In a similar way, today energy generation networks are directed by the centers, the centers which take control on energy distribution and manage it. However, the dramatic development of renewable energies like solar energy or even batteries improvement causes small local distribution networks coming about. Therefore, if you generate energy at your home or work, you can store it in the batteries and consume it whenever you need it. You can even sell it to your neighbors.

Such events can lead to maintaining energy and avoiding its loss. Since the more distance the energy goes, the more loss and charges it will bear. Through this method, there is no intermediary anymore, and the people can trade themselves. Presently, energy production companies are the trustable link between the user and his/her need (energy). Because they control the infrastructure, so they take their share.

Journalism

Tapscott says that Blockchain can make a revolution in journalism too. For instance, for each story, news or article which is read, the reader can pay one-tenth of a penny (a hundredth of a dollar). As a result, the reader decides which text is more importance or valuable enough to be invested in and pays for it. From Tapscott's point of view, it might be a way to cope with fake news against real and valuable news the journalists create. Of course in a more professional perspective, such a measure might be more in favor of popular authors, and it leads to disregarding important but less popular news.

Medical Industry

In the medical industry where sometimes you notice the patients' records manipulated, the physicians and hospital heads can store a file of the patients' records with high security and offer it to the hospitals, therapy centers and even jurisdictions in case of necessity. It can cause lowering the risks and costs of data management besides increasing security of storing and transferring data.

The electronic medical records stored in the Blockchain will be made accessible and updated through biometry. Besides, it can provide the possibility of free access to the data related to the patients' records and decreasing the burden of transferring records between various suppliers.

Data Storage

Currently, you use Dropbox or Gdrive to store files. The main problem in using these service providers is that you should trust them. The states can urge them to disclose your information. However, by using Blockchain technology, your information will be stored in the network with unique encryption. This very issue leads to lowering the charges. Even if you have extra space in your computer, you can rent it. Storj is a good case in point.

Manufacturing and Controlling Products

In the process of about 8% of the world exchanges, fake goods are sold to the customers; hence manufacturing and delivering goods and services have always been intermingled with the issues of quality and control and the manufacturers are frequently faced with careful verification and regulations-adaptation activities. This quality guarantee in manufacture industry imposes high and growing charges on the final consumer. Blockchain provides an opportunity to decrease cumulative charges resulting from controls in the supply chain. Through applying this surveillance technology in the supply chain, protecting the intellectual property of information and designs, supervising manufacture in accordance with designs, making sure about on-time payment, decreasing relying on third persons like banks, inspectors, attorneys, and even internal audits and decreasing middle managers are imaginable. So blockchain can revive manufacture and industry.

Registering Documents

Now, most of your ownership records are stored in paper form, and it is possible to manipulate them. Since this technology uses computers, human errors will decrease. If a person manipulates the blocks' information and alter the information, the hash will change, and this change causes breaking blocks' sequence. Considering all these issues, no one can alter these blocks. Each alteration will not be hidden from everyone. Blockchain, as an extended public ledger, can do any registration better. Property registration can be a good example in this regard. Currently and through the traditional method, the procedure of property registration is very expensive, needs great human resources and is highly vulnerable to fraud.

Currently, some countries do property registration based on Blockchain. Honduras was the first government to start this innovation in 2015, though its current status is not clear. In this year, Georgia made a contract with Bitfury group in order to develop a Blockchain system to register property. According to an official report, Hernando Desoto, famous economist and ownership rights defender will be one of the consultants in this project. Lately, Sweden has also announced that it will use this system tentatively to register properties.

Internet of Things

According to Cisco, 50 billion devices will be connected to the internet till 2020. Given this number of devices which all create sending, receiving, and processing commands such as turning on, dialing and moving, the data accuracy in this route might cause unpredictable charges. Blockchain can be used to trace billions of connected devices, process trades and enable coordination between devices. This decentralized approach will remove the probability of network breaking down and create a more resistant ecosystem for the devices. Moreover, the applied encryption algorithm by Blockchain makes the customers' data more private.

Raising Capital

It is the very best application of Blockchain! Blockchain has proposed in the new concept and made a revolution in raising capital. ICO is a new way to raise capital;

everyone can invest by it, wherever they are. When someone invests at your company, you should give him a receipt. ICO suggests digital assets, and you can give your receipt to the investor with created tokens. The tokens are stored in your Blockchain network. These tokens can be applied to use offered services from your company or even are exchanged with other tokens. In fact, tokens are a new generation of stocks of the companies which are offered in the safe Blockchain infrastructure.

Digital Identity

What is your idea about a decentralized and encrypted registry? Alternatively, a digital identity? Blockchain technology gives solution to many authentication problems and can offer a unique, undeniable and safe identity. The methods which are being used today are based on registering information on an unsafe database. Using Blockchain technology, authentication is undeniable and is carried out based on digital signatures and according to the private key.

Criticism of Blockchain

Taking important and clear features of Blockchain technology, it always has faced some criticisms. It includes a wide variety of experts' opinions; however, it can be said that one of the most important criticisms of Blockchain is its application in financial fields. Wei Kai, chairman of Blockchain research section in China Information and Communication Technology Academy believes that the companies haven't succeeded in solving three major financial problems of this technology technically although he has acknowledged Blockchain ability to make an evolution in different industries. This Chinese researcher thinks that Blockchain society should still work on cases such as information privacy, applicability and also Blockchain ability to be integrated with the current economic system. One of the other problems is to make surveillance approaches coordination between various judicial fields across the world.

Today Blockchain faces with a bigger problem called scalability. The fastest property-dependent Blockchain systems cannot manage more than a few thousand financial transactions in a second. This capacity of transactions will maximally reach 25,000 transactions a second (this figure is somehow similar to the current capacity of VISA). Depository Trust and Clearing Corporation, in its 2018 report, points that each new technology should have the capacity to develop to two or three times more than its current maximum capacity and also it should be able to do 50,000 transactions a second. In order to make predictable the future physical limitations ahead of transfer speed for an extensive volume of information, there is no way for the financial system to be able to use it to evade relying on centralized transparency and settlement systems.

The Future Soon to Come

We can hope that the future of Blockchain is bright and predictable. There is almost no doubt that this technology will be active in all areas of the global industry until the next decade. It is because of its decentralized and reliable and of course controllable Blockchain ecosystem more than any other thing. However, this point should be taken into account that the development of Blockchain technology in financial and banking fields follow judicial rules of different countries and predicting it is very difficult. In fact, financial rules of the countries are continuously changing and given being young Blockchain technology we cannot be sure about the countries around the world to come to terms about financial transfers.

Considering all these issues, Blockchain will make important changes in our society, the changes many of which are not even predictable, but we can be hopeful that this technology can reduce the problems the societies are engaged with.

4

What Is the Blockchain Ecosystem?

Blockchain is a decentralized system that is not controlled by a third part. It has different types and each is designed for a specific purpose. Blockchain Ecosystem means a group of people that indirect with each other to create a special environment.

Blockchain technology will soon create a big revolution in the financial field and social and political transparency. Blockchain is a decentralized system that is not controlled or overseen by any country or government. This has led to its having some amazing capacities. These vast capacities can be used in transferring foreign bills to providing health care. However, when we say the Blockchain ecosystem, what do we really mean?

Blockchain Ecosystems

Blockchains are like roads. Just as roads have different types, Blockchains have different types as well and are not limited to one specific type. Each Blockchain network is designed for a specific purpose and in addition to that includes independent elements that form a special ecosystem next to one another. When we say Blockchain ecosystem, we mean a group of elements that interact with each other and the world around them to create an environment with special features.

For example, the cryptocurrency ecosystem based on Blockchain has four parts or elements: the users that use cryptocurrencies to receive and send currency, cryptocurrency miners that produce the cryptocurrency, investors that buy cryptocurrency, and the developers that write programs related to this system and network and develop it. No part of this system can continue working without the other.

In the following parts, the elements of the cryptocurrency ecosystem will be addressed. This ecosystem offers a complete example of the Blockchain ecosystems:

1. Users in the Blockchain Ecosystem

Users are normal people that use Blockchain and cryptocurrencies such as Bitcoin for their different purposes. For example, these people like to engage in a sort of micro-investing by buying and holding on to cryptocurrencies. Buying and selling cryptocurrencies can also be another reason as to why people use Blockchain. Among the well-known cryptocurrencies that users buy them for many purposes are Bitcoin, Ethereum or Litecoin.

2. Investors in the Blockchain Ecosystem

Investors form a large part of the Blockchain ecosystem. This part of the Blockchain environment looks for small and large scale planning for the future. In getting counsel with skilled experts in this field, they have figured out that in the future the investment capacity of Blockchain will be much more than today. These people want to invest their money in different projects for the booming of the Blockchain and in order to gain huge profits.

3. Miners in the Blockchain Ecosystem

In order for the Blockchain system to work properly and for its integrity to be preserved, there is a need for a large network of independent users across the world that are active in this system consistently. In public Blockchains, any user can be in the

Blockchain network and appear as a Bitcoin or other cryptocurrency's miner. In the mining process, miners confirm the transactions that have taken place on the Blockchain infrastructure and add new data of a transaction to the Blockchain network infrastructure. Miners should identify the encryption used in transaction data. They compete with other miners to decrypt the codes of each transaction. Any miner that can decrypt the transaction faster will gain a part of the transaction as a reward.

4. Developers in the Blockchain Ecosystem

As it was mentioned earlier, Blockchain has different types. Developers are those that work on the already existing programs on the Blockchain infrastructure. Some of them develop applications based on Blockchain and write programs that have different purposes and offer different services in various fields via Blockchain to users all across the world. In short, developers work toward making the Blockchain system more practical and improve this network regarding structure and function.

Blockchain Ecosystem in the Future

World Economic Forum has predicted that only until five years later more than 10 percent of the global GDP will be stored on Blockchain infrastructure. Different projects that revolve around cryptocurrency and Blockchain are being developed all across the world. In the near future, these projects will be operationalized, and financial technologies will enter a new era of huge capabilities.

5

The Magic of Gold and Digital Money

Imagine a world where you only make digital purchases; buying, selling or trading money or gold. A new system - an evolution of the fiat system and financial systems we know today. The reality can be experienced by the most financially literate or illiterate in many parts of the world, shared by everyone from a businessman in Dubai to a mother in San Francisco. The magic happens online.

As the journey of cryptocurrency market adoption marks ten years, the issues still remain: how do we make cryptocurrency accessible to billions of people, safely and legally? And what types of purchases are possible? How secure and fast are these transactions? These questions mark an era of immense transition, exciting times for learning, business and social impact.

First, an internet connection, broadband or Wi-Fi, is needed to access the many products and services available in this industry. Next questions arise about risks of recording information digitally, especially when purchasing cryptocurrencies on digital exchanges. All passwords must be stored safely in a digital wallet, flash drive, an encrypted note or even a bank vault.

Wondering why the prices of cryptocurrencies keep fluctuating and how to minimize this? One way to reduce price fluctuation and uncertainty is through stable coins. This type of cryptocurrency supplies digital exchanges with a price to one of the world's major legal tenders such as the U.S. dollar or Euro or to a precious metal such as gold or silver. Benefits include the ability to transfer digital assets without high, international transaction fees.

At Counos we developed our own Stablecoin. Counos Coin is a Cryptocoin based on the Litecoin source code and has a completely independent network. Its encryption algorithm is similar to that of Litecoin and uses SCRYPT algorithm, a type of Blockchain which supports the operational capacity of cryptocurrencies. The Counos platform, although released with a fixed price Coin (Counos E, Counos U, Counos CAD), can be increased like any other cryptocurrency when demand increases. One unique aspect of Counos cryptocurrency is that you can even buy gold with it.

Looking ahead another decade, we can say that cryptocurrencies are here to stay, where everything that you ever designed, gold or not can be purchased safely online knowing that the price of gold and our stable coin is the same for the businessman in Dubai as it is for the mother in San Francisco.

6

Comparing Conventional Databases and Blockchain

Database

A database is a group of organized data that are stored and can be accessed anytime. Databases usually have a client/server structure. With this structure, the database is usually set on a central system, and a group of clients use its services. Accessing database is possible via using a module software called a database management system (DBMS). Implementing database is in a way that prior to getting access to it, the process of authentication takes place.

If the identity of the client is authenticated, according to the access control list, permission will be issued for the request of the client, or it will be rejected. The requests are divided into four parts of adding a new record, deleting a record, updating a record or calling up a record. Any defect in the access control process prepares the basis for conducting cyber-attacks and tampering with the database.

Database management is done in a centralized way, and users do not play a role in it. In general, databases are divided into two main categories of relational and non-relational. Relational databases are made up of tables, and the columns of each table are called fields. Data are put in the rows of the table, and each row is called a record. Records connect with each other via the relations between tables. In non-relational databases, the data are usually stored with the key/value structure, and there is no need for defining tables with specific columns.

Blockchain

As it is clear from the name of the Blockchain, this structure is made up of a chain of blocks. Each block is made up of two parts of header and body. The body includes the stored data in the block and header is made up of a group of fields. For instance, Bitcoin header fields and the purpose of each one is explained in the following parts.

- Version: this fields specifies the version of the Blockchain.
- Previous block header’s hash: this field is the hash value of the previous block header.
- Merkle Root: this field of the result of the implementing Merkle root algorithm on all the stores data in the block body. These data in Bitcoin are transactions. By using the Merkle root, the integrity of the stored data in the block can be evaluated.
- Timestamp: this field specifies the time the block was generated.
- Difficulty target: this field specifies the difficulty target of each block. The difficulty target is a parameter that makes it possible to adjust the problem difficulty in the PoW algorithm.
- Nonce: this field specifies the number of attempts made by miners to solve the PoW problem.
- Hash Block: each block has a hash value. This hash is generated via the Merkle root and the hash value of the previous block in addition to the other number of header fields. The use of the previous block’s hash value in generating the new hack block makes possible for blocks to connect with each other. In fact, in this method of calculation, hash indicates the same concept of the chain in Blockchain.

Other common Blockchains use a similar structure to that of Bitcoin that was just introduced. The common aspect among all these Blockchain structures is the storing of data in body and connecting blocks using the hash value of the previous block in generating the hash of the new block. Unlike the common method of implementing conventional databases, the Blockchain data are not kept in a central system and are not managed centrally.

Their management and maintenance are done in a distributed way with a collaboration of a group of nodes, and this is why it is called distributed. The adding of a new block to the Blockchain requires consensus, and when a new block is added to the chain, tampering with it and deleting it will become impossible. Coming to the consensus to add the new block is done in different ways that are called consensus protocols. The PoW and PoS protocols are two well-known consensus protocols in the Blockchain structure.

Making sure of not tampering with blocks is done using the hash algorithm. Any tampering with the data of a block is done via recalculating the Merkle root. The difference in the new Merkle root with the previous Merkle root specifies the tampering with the data of that block. From the other hand, deletion of a block will change the hash of all the blocks after it. Not keeping the chain of blocks in a centralized way in a trustless space between users makes the deletion or tampering with a block to be easily noticed.

Any of the two methods of a conventional database storing and Blockchain have features that gain importance depending on their application. In the following parts, we will compare conventional databases with Blockchain from different perspectives.

Central Control

Blockchain makes possible the sharing of data between users who do not trust each other, but in the conventional database, users need to trust the entity who manages and controls it. In the conventional databases, there is always the risk of data being tampered with by the person who has the necessary permissions, but in Blockchain, there is no central control and adding of new data takes place through consensus protocols. Central control can be considered a disadvantage for a system.

In case this center comes under attack for any reason, or a problem occurs to it, the entire system will have a problem and this, in turn, will affect all the users. However, in Blockchain, the problem that is created for a node will not affect the other nodes in the network.

Immutability

The data stored on the conventional database may be deleted or updated. While in Blockchain, the stored data are kept from the beginning and are immutable and cannot be deleted.

Performance

The process of creating a new block in the Blockchain has some limitations that reduces the speed of data being stored compared to conventional databases. The limited volume of the block and the fixed rate of new block generation are among the limitations that reduce the performance of Blockchain with respect to its speed. For instance, the block generation rate in Bitcoin is one block in each ten minutes.

From the other hand, the size of each Bitcoin block is at most 1MB. Given the average size of Bitcoin transactions, each block holds about two to three thousand transactions in itself. Given these numbers, the speed of Bitcoin transactions is a onedigit number, while existing non-Blockchain solutions process much much more rate of transactions and store them.

Confidentiality

Controlling access to records in the conventional database is easily implemented. In the database, implementing access permission for each user is easily possible, and on the other hand, the database does not allow any user to access the information of the database without confirmation, but in Blockchain all users have access to information from the beginning. As such, in applications that have a high degree of confidentiality and secrecy, Blockchain will probably not be a good solution.

However, currently, there are ideas implemented in the Blockchain to provide confidentiality and are being used. Among the most well-known Blockchains that have been able to provide the confidentiality of data against illegal users is Monero. In the Blockchain of Monero, the amount, receiver, and sender of a transaction are kept hidden from others. The availability of information to all the Blockchain users can also be analyzed from another point of view. All users having access to Blockchain can provide transparency in the system, and this can be considered an advantage in some applications.

7

Public, Private, and Federated Blockchains

Bitcoin introduced the Blockchain technology to the world and today with the explosive fame of cryptocurrencies; the Blockchain technology gains more extensive aspects and more various applications each day. Yet, this technology has different kinds. Generally, there are three types of Blockchain:

Private Blockchain

Public Blockchain

Federated Blockchain

However, there are also other types of Blockchain such as public-permissioned Blockchain and private-permissioned Blockchain, which we will not talk about here.

What Is Public Blockchain?

As it is obvious from the name, public Blockchain is for the use of public and anyone can read it or write on it. This type of Blockchain has a high level of transparency since everyone can have access to it anytime. However, a question that comes to mind here is that given the nature of this Blockchain, how are its decisions made? To answer this question, we need to be familiar with Blockchain protocols such as PoS and PoW.

For example, in the Bitcoin and Litecoin Blockchain networks, anyone can mine or make transactions.

What Is Private Blockchain?

Companies can create a private Blockchain for themselves in order to provide the security and confidentiality of their data. Those who participate in a private Blockchain need to have access permission and get authenticated via the network. This network is called a "permissioned network," and those who have access to it are restricted. Private Blockchain even restricts what people who have access to it can do. For example, certain people can perform certain transactions. This makes an extra layer of security to be formed over the network.

The rules of participants are set by other participants or observing authorities. All those who participate in this network play a role in creating this decentralized network. Though this has led some to believe that such a private network cannot be called Blockchain since they are in contrast with the definitions that Bitcoin offered of Blockchain and are not truly decentralized.

What Is Federated Blockchain?

Federated and private Blockchains are mostly similar. In private Blockchain, you do not have access unless your identity as a person who has access to the network is authenticated, and only one person or organization can determine these permissions. Private Blockchains are more used in organizations that want to observe transactions only themselves. Since these questions, the main nature of Blockchain, which is its decentralized nature, the third group of Blockchains, i.e., federated Blockchains, are introduced.

Instead of using just one person or organization to define permissions, federated Blockchain uses many organizations to do so and somehow creates a decentralized network. These organizations are called a federation. Federated Blockchain is more used in cases such as financial services, production chain management, and the security of organizational data.

Let's illustrate the point with an example. Ten nodes (for example, ten banks) are chosen in the network as the federation. Among these ten organizations, one node is chosen as default to be able to make changes on the network. These nodes can read and write transactions or restrict other participants. However, can they add a block on their own to the database? The answer to this question is no.

In order for a block to be added to the database, all the nodes in the network need to confirm it. Even if one node in the network does not confirm it, adding a new block to the network will not be possible. This feature is not available in the private Blockchain. The decision-making function in this Blockchain is based on voting.

What Is the Advantage of Federated Blockchain over Other Types of Blockchain?

Public Blockchain has a high level of security, but when a large number of users are added to the network, it lacks enough speed. From the other hand, private Blockchain has high speed but is not a real decentralized network. Therefore, the problems that are seen in a centralized system are also seen in this Blockchain. Then we get to the third type of Blockchain that does not have the defects of the other two types and at the same time has created a decentralized system.

Higher Speed

One of the objections that is posed to the public Blockchain is its low speed. The low speed makes some transactions hard to finish. In the federated Blockchain, since not everyone has the permission to add a block, then the speed of the network is much higher than the public Blockchain.

Scalability

In the federated Blockchain, you do not have the problem of scalability, since the number of nodes that are used for authentication and validation are always under control. These nodes go through special stages to gain access to the local network. Therefore, everything in this network is under control.

Lower Costs of Transaction

Though the public Blockchain claims that it has lower costs, but it is not always the case. As we mentioned earlier, the more people are added to the network; the transactions get slower. This leads to a more complicated issue, which ultimately leads to more costs of transactions. However, in the federated Blockchain, the transactions are simpler and faster. This makes that ultimate costs of transactions to become much lower.

Less Energy Consumption

Mining consumes a lot of energy, and on the other hand, as time passes the energy needed for mining gets more and more. If this continues, the needed energy cannot be provided easily. Federated Blockchain only uses a certain number of nodes for authentication. Therefore, it is much less computationally complex and requires much less energy.

Ripple Is a Successful Case of Federated Blockchain

Ripple is an early version of a federated Blockchain that has kept its centralized nature while being decentralized. Ripple recently received an honorary degree from the global economic banks and some other rewards. These rewards were for banking solutions of X rapid and X current that are currently being used by a number of banks all across the world.

How Will the Future of Blockchain Be?

Federated Blockchain can change the mechanism of Blockchain programs for the better. Organizations can now transfer information with a higher speed and less concern, and customers will benefit from this in the long run. Federated Blockchain still has a long way to go, but the fact is that using only one type of Blockchain is not a good idea, since each of these types can have more advantages over the other types depending on the business in which they are being used.

8

Introduction to Bitcoin, Ethereum, Ripple and the Token Universe

To know more about Bitcoin and other cryptocurrencies, it would be better to speak about cryptocurrencies and Blockchain. You have surely heard about cryptocurrencies, but you might not know exactly what cryptocurrencies mean. In 2008 someone named Satoshi created Bitcoin to be used in trades.

In order to do these trades, you need a network which is called “Blockchain.” In a normal trade (e.g., fund transfer to another card), all transactions are controlled by a central system, but it is not the case about cryptocurrencies; all trades are controlled in a decentralized infrastructure and each system in this network has access to all transactions, and in order to do each transaction, all the systems are included in this process.

In fact, in each transaction related to cryptocurrencies, there are miners to do the transaction and receive the reward (such as Bitcoin) as per the job they do. There should be some complex calculations for mining each Bitcoin. These calculations are actually those who solved the main problem of digital money and minimized the probability of error and fraud.

How Was Bitcoin Created?

The first Blockchain of the world was Bitcoin. Bitcoin was made by one or some anonymous persons named Satoshi Nakamoto, and the identity of this person or these persons has been kept hidden. He first published an article and explained how Bitcoin was supposed to work. Bitcoin is actually a borderless currency.

In a decentralized system such as Bitcoin, the money is not controlled by the government, in the traditional financial system money is dependent on the government, and if a government destroys, its money will be lost too. In the article published by Satoshi, a new database called Blockchain was introduced to the world. Each block in this database stores a chain of transactions.

A chain of Blocks is called Blockchain. Each block is recognized with a number (that each time a number is added to it), and SHA256 hash code is recognized. This code is calculated and decoded via transactions placed in it and its previous hash code. The data in this database are secured by an algorithm called proof-of-work. This algorithm avoids double-spending. It refers to using money which doesn't exist. Each person can mine in this network and about every ten minutes a new block is generated wherein the last specified transactions have been registered. The first version of Blockchain had been in C++ language.

What Is the Difference between Cryptocurrency Coin and Token?

Bitcoin and Litecoin and Counos coin are some types of coin, and the token is everything other than those. However, how do coin and token differ in trades? The coin is a cryptocurrency which acts independently from any other platform. Tokens, however, need another platform to run. Ethereum is one of these platforms. Of course, there are other platforms like Omni and NXT too.

Tokens are made on these platforms. If you visit cryptocurrency exchange markets, you will see that both token and cryptocurrency coin can be traded. In fact, the manner of trading these two is the same, and the only difference is in their nature. Making a token is much easier than making a new cryptocurrency. Since there is no need to code it from the beginning and you make it on another Blockchain. The concept of the token is very wide and can include everything from a new digital currency to an economic good, which is tradable.

Initial Coin Offering

Tokens are offered in an Initial Coin Offering (ICO). The companies increase their capital through different methods to develop their businesses. For example, a startup might decide after some years to sell some of its stock to develop its business. ICO’s purpose is the same too. The companies which want to make new tokens acquire the costs of making and developing them by preselling coins. The participants can preorder these tokens by the currency or other cryptocurrencies and hope to benefit from it in the future.

Ethereum and Ripple

We made you familiar with the general concept of cryptocurrency and Blockchain database. However, Blockchain and cryptocurrency are not limited to Bitcoin. After introducing Bitcoin, some other cryptocurrencies came into existence and introduced themselves to the world of cryptocurrencies.

Ethereum and Ripple are among well-known cryptocurrencies in the world of Blockchain. Blockchain technology has other applications other than Bitcoin, which have a concept beyond merely a cryptocurrency. One of them is Ethereum. You had to spend much time and money to generate a cryptocurrency before Ethereum, but

Ethereum (as pointed out above), helped developers to create their programs in a shorter time and using Ethereum platform through creating a platform.

Although Bitcoin and Ethereum are, to a large extent similar, the focus of bitcoin is one creating an online p2p payment method, while the aim of Ethereum is creating a platform for decentralized programs. “Ether” is a cryptocurrency used in Ethereum. Those who run their codes on Ethereum platform spend their costs via Ether. However, what are these codes? They are idiomatically called smart contract. The smart contract refers to any program which is applied for trading a value or property.

Ripple is the other famous digital protocol which runs in a p2p network called RippleNet. The cryptocurrency which is traded in this network is XRP. The computers in this network are the gateway.

Your trades are done through the gateway you have assumed secure. All cryptocurrencies are traded in the Ripple network, but if your transaction is with XRP, it will be conducted quickly; otherwise, some other stages should be passed. At first, your gateway calls an IOU.

What Is IOU?

Everyone in Ripplenet network can request any currency except XRP. However, currencies which are not XRP are requested through IOU. IOUs are actually tokens through which even dollar can be traded. In order to do that, in the first stage, the person trusting you and is sure you can trade your aimed currency asks you to pay him/her that amount.

For instance, suppose that A owes $10 to B and wants to send this amount to A in Ripplenet network. At first, A asks for an IOU, and on the other hand, B knows that A is reliable and affords paying $10. Therefore, B accepts dollar from A too. Meanwhile, there is a third party (C) that B is supposed to give him/her $5. The third-party, too, trusts A and knows that he/she is able to pay $10 dollars. Therefore $10 A wanted to transfer in this network is distributed between B and C, and each one has $5 now.

In the above article, all important points in the field of cryptocurrencies and famed cryptocurrencies have been mentioned. If you intend to invest in this field, which one will you choose? A deeper study on the market seems a priority in this regard.

9

The Status of the Trust and Transparency Economy in Blockchain

We are living in a digital world. Everything around us is constantly changing, and Blockchain technology can be considered as one of the biggest changes that is currently taking place in the world. Blockchain is a vast platform to establish peer-to-peer communications among different people in different parts of the world. In fact, with this infrastructure, we are faced with a database that is shared among different computers.

There is no centralized surveillance from a foundation or person on this network. Yet, the security and transparency of its structure is why hackers can wander around in it. Various security algorithms of Blockchain make all financial and non-financial transactions completely transparent, secure, and irreversible.

Blockchain's Security Algorithms

Since the launch of the Blockchain network, there is constantly the talk of the network in which all transactions and activities are registered precisely, and all users can know about what goes on in this database. Since there is no central surveillance in the Blockchain network, users should confirm the transactions in the Blockchain.

Here we need algorithms to maintain the security of Blockchain transactions. The algorithms that maintain security and the transparency of transactions are called “consensus algorithms.” In the following parts two examples of the consensus algorithms or the security algorithms in the Blockchain network will be addressed:

The POW Algorithm

The POW (proof-of-work) algorithm is the first security algorithm that was developed for the Blockchain system. This algorithm is one of the most necessary parts of the cryptocurrency mining process meaning that through this algorithm, miners can confirm blocks or that registered information on the Blockchain network and by decrypting the encryption of transaction gain their rewards.

Miners, in competition with one another, attempt to decrypt the transactions in the network and thus gain their reward or certain amounts of cryptocurrencies. Not all miners can go through the POW algorithm and cannot properly decrypt the transaction that have taken place. As a result, the security of the Blockchain network is mostly provided, and the possibility of hacker attacks decreases.

In fact, in order to confirm each transaction, you have to decrypt them and in return for this confirmation and decryption gain a certain amount of cryptocurrencies. This process is called the POW algorithm.

The POS Algorithm

Another algorithm that provides the function clarity, transparency, and security of the Blockchain network is the “POS algorithm.” POS is short of proof-of-stake. The mentioned algorithm was created as a replacement for the POW algorithm, and through it, unlike the previous algorithm, there is no need to decrypt transactions and mine cryptocurrencies.

Sometimes, people do not appear as miners but as the creators of the blocks in the Blockchain. In other words, they have registered a group of data in the Blockchain database. In this situation, according to the POS security algorithm, they need to offer assets through which they'd show their good intention of working in the Blockchain. Putting down assets as assurance for the health and validity of activities in the Blockchain is what POS is about and via this algorithm the possibility of malicious acts by frauds, scammers, and hackers in the network decreases.

Security and Transparency

The existence of consensus algorithms in the Blockchain network leads to more security and transparency in people's transactions in this platform. In addition to all of these, Blockchain technology includes different very complex mathematical algorithms to ensure network security. On the other hand, the lack of management centralization in the Blockchain infrastructure and distribution of payment information or transferring data among users has given such transparency to the Blockchain ecosystem that currently there is no other rival for it.

10

A Look at the Protocols in the Blockchain Technology

The blockchain protocol is a common term for the methods and rules that are agreed upon. These methods are actually different systems that are used to come to an agreement and validate transactions in the Blockchain network. Some of these protocols make users buy physical mining devices, and some do not require you to have a physical device.

Blockchain was introduced in 2008 and ever since it has come a long way. Although a large part of Blockchain technology is related to the crypto market. Blockchain is a decentralized database that is made up of a number of nodes.

Nodes are actually those computers that are in the network and form this database together. Blocks are connected to one another via protocols. The protocol is, in fact, a program that is the fundamental structure of the network.

Different protocols are designed based on the need for them in the technology in which they are used. For example, Bitcoin was first designed to create a decentralized monetary transfer system which is disintermediated. Ethereum is more focused on developing a Blockchain platform through which decentralized applications can develop further through smart contracts.

What Is Blockchain Protocol?

The blockchain protocol is a common term for the methods and rules that are agreed upon. These methods are actually different systems that are used to come to an agreement and validate transactions in the Blockchain network. Some of these protocols make users buy physical mining devices, and some do not require you to have a physical device.

Some Blockchain Protocols

Proof of Work

Many of cryptocurrencies such as Bitcoin use PoW as their consensus algorithm. As a result, miners have a role in the general scheme of PoW. Having a share in this process by the computation power of their systems and by making mining rigs that are mostly made up of a number of graphic cards, they participate in this process. The reward of the miner will be paid to them. Getting a physical mining device means that the miner has to pay for it which is usually something around a couple of thousand dollars.

Proof of Stake

With PoS you do not need to buy expensive mining rigs. By having coin and keeping your computer on you will take part in this process. This does not require a lot of energy on the part of your system and you are rewarded as a miner. The more coins you have, the more share you have and as a result of the more reward you get. PoS does not need initial assets to create a mining rig. Anyone who has more assets can make more money by merely buying coins.

Proof of Weight

Some projects like the project that has been launched to store files use this protocol more than others. In the previously mentioned method, the person makes money merely based on the number of coins, but in this method in addition to the number of coins, the number of files are calculated. In fact, this method encourages the user to have an active and meaningful presence in the network, in addition to having coins.

Well-known Blockchain Protocols

There are many Blockchain protocols but among the most well-known of them are Bitcoin, Ethereum, Ripple, and Hyperledger. In the following, we will explain two of the most well-known Blockchain protocols, Bitcoin and Ethereum.

Bitcoin

Bitcoin is one of the first Blockchain protocols. The main features of this protocol are as follows:

- This protocol is a public Blockchain. It means that anyone can become a member of it and does not need permission for access.

- This protocol allows users to make their financial transfers without the need for a third party or intermedium.

- Each node has the full information of Blockchain and therefore forms a decentralized network.

- Transactions have a unique ID, Bitcoin address, the number of Bitcoin transferred and the Bitcoin destination address.

- Miners create these transactions. This means that a number of devices are used to mine Bitcoins. Users are rewarded in exchange for mining. Miners attach this transaction to the next block. Every ten minutes a new Block is processed, and then the transactions that are added to that Block will be registered on the Blockchain.

The registration of each transaction not only needs the information of the current transaction but it also needs the reference of the previous block. The information of the previous is not identifiable, and the miner has to get to that through solving a cryptographic puzzle. Furthermore, in order to solve this riddle, you need a system with high power and speed.

Ethereum

Ethereum Blockchain is very similar to Bitcoin Blockchain. For example:

- It is a public protocol that does not need access permission.

- It has used similar technology in the main column of the protocol. For example, it has used a hash cryptography function, private and public keys, and a P2P network.

- But unlike Bitcoin that is used for cryptocurrency transactions, Ethereum is designed for a wider range of uses. Ethereum creates a Blockchain platform with which users can develop their Blockchain projects such as their own cryptocurrencies. This platform is called Ethereum Virtual Machine. Smart contracts have made this possible. Smart contracts are in fact pieces of code that allow you to run a function. These platforms are in the Ethereum platform and are inspired by Ethereum's exclusive language C++, Java, Python, and JavaScript. Decentralized applications are those in which backend code is run on a decentralized Blockchain and includes smart contracts. The frontend of this code can be written in any language. A decentralized application needs to have the following properties:

- It should be fully open-source

- It should be run anonymously
- It needs to use an encrypted token
- Data need to be saved on a decentralized Blockchain and meet cryptography standards

Therefore, Ethereum uses a wider definition of Blockchain since an Ethereum Virtual Machine includes smart contracts and decentralized applications. Ethereum also allows users to allocate how much of their computer power they want to be used for the transaction processing and the measuring unit for this has been called Gas. Simple transactions require less Gas, while large transactions require more Gas.

Which protocol is better?

All of these protocols are made to perform decentralization in the best way. The crypto market favors PoS more because having coins and temporary participation in this network is much simpler and with fewer troubles. Even Ethereum moved from PoW to PoS protocol.

11

Instant Messaging and Blockchain Technology

Social networks and messengers are altered along with the storm of new technologies such as Blockchain. Developing and designing messengers which work according to Blockchain system, will dramatically change the future of big services such as Facebook and WhatsApp.

However, the question is that the what are the drawbacks of domestic instant messengers; or in other words, what are the new features of messaging services which are developed according to Blockchain which cause their superiority over their previous generation?

Social networks and messengers are altered along with the storm of new technologies such as Blockchain. Developing and designing messengers which work according to Blockchain system, will dramatically change the future of big services such as Facebook and WhatsApp.

However, the question is that the what are the drawbacks of domestic instant messengers; or in other words, what are the new features of messaging services which are developed according to Blockchain which cause their superiority over their previous generation?

Can Blockchain offer more services and facilities by creating a more proper and complete infrastructure? In order to find a more appropriate understanding of facilities and features of Blockchain messengers you should make familiar with them more:

What Are the Limitations of Current Messengers?

Most of the current messengers cannot be managed easily in very wide dimensions. For example, managing groups with a large number of members is a little difficult. In addition to the fact that some current messengers are not designed for a large number of people, limitation of some to offer facilities such as group video calls is one of the demerits of these applications.

Let alone small and nominal facilities such as not being specified the location and geographical locality, the issue of security is one of the basic points which should be taken into account in message exchange, how much do traditional messengers emphasize on the data encryption? When a message arrives the destination, it will be placed in the users' electronic device and registered there.

This message will be placed on the other server and device and in case there is a sensitive and secure message, it will be put at risk to a large extent; that is, after sending a message, its control and management is not in the hand of sender anymore and he/she cannot be sure about eavesdropping and getting access to it.

After the events taking place for the users' personal information in Facebook social network and jeopardized the security of many users, the need to provide the security of social networks got more than before. The issue of information security in a world wherein technology and information has turned into a pervasive part of the people's lives is considered very vital and important. Apparently, in new instant messengers, these problems will be removed greatly.

With the fast growth of smart tools such as cell phones, the number of cyberspace users is increasing day by day or even second by second. As a result, the volume of information which is created in the world will get bigger strongly.

These data need investigation and processing. In order to straighten out this wide volume of information, you should resort to an extensive network such as Blockchain, a network which is not centralized, not located in a specific country and can be managed by self-regulation on the part of users. According to the assessments, in the near future, the volume of information which is exchanged in virtual networks will be much more than what we witness these days.

What Is the Difference between Blockchain Messenger and Traditional Ones?

Before we start explaining features of Blockchain-based messengers, it would be better to elaborate exceptional features of Blockchain. Why is Blockchain considered a secure system to exchange different messages? Blockchain is a database. The followings are of its main features:

Decentralization

Blockchain is a network which is managed by the users themselves; that is, no main and central core undertakes its direction. Hence, there is no possibility of manipulating information on the part of senior authorities such as governments. The network with no censorship, blocking, and information stealing in it does not have the value of investigation and application.

Information Immutability

The information cannot be changed in the Blockchain system. This features shows that Blockchain can become one of the best infrastructures to develop messenger applications. Information immutability in this infrastructure avoids violating privacy and various frauds.

Resistance Against Removal and Censorship

Since Blockchain is an independent network, there is no place for governmental and state surveillance. So no foundation or institution can block and cease it. It means that we face a free information flow with no censor and pressure.

The messengers which work according to Blockchain employ an End 2 End encryption system. In this method of encryption, there is no possibility of observing exchanged data between people by a third party, and it is only the sender and the receiver who can manage the messages.

As a result, no one can access to the messages exchanged between two parties. In new messengers, authentication is carried out via Blockchain, so stealing personal information is not possible in the authentication stage.

Moreover, decentralization of Blockchain system does not let any state or foundation stop the users' activity. In fact, it is not possible to block, limit, control or inactivate the users' accounts at all.

Simultaneous Use as Payment Gateways

One of the most alluring feature of using Blockchain technology to send a message can be the possibility of transferring funds from a digital account to your contact lists. This rowdy feature will be a big leap in transferring minor or major assets besides raising payments' security through facilitating financial transfers.

What Are the Security Mechanisms in Blockchain Messengers?

In these messengers, all the users own a public address and a private key. For example, suppose that two persons named A and B would like to make communication in Blockchain messengers.

They just need their public address to communicate. They can create a safe communication through public addresses. Now if anyone wants to get engaged in this reciprocal relationship, he/she should know the private key of one of these two people. Knowing the private keys of A and B is the only way to come into a two-handed conversation.

As it was pointed out before, first A and B need to recognize each other's public addresses to enter a reciprocal communication. The important question is that in the first stage, how do these two people get access to the public address or ID too?

In normal and usual messengers, a centralized network and system manages the users' messaging to each other. That is, if it is supposed that A and B find each other's public address, he/she should refer to a third party and receive the related information from it. In this case, the possibility of making communication will be there.

However, in your idea, does such a form of communication enjoy sufficient security? Let us name that third party which is centralized network management in traditional messengers (e.g., Facebook, Twitter) as C to simplify explaining this security subject. Supposedly, for forming each conversation between two users like A and B, you need to refer to C, it then gives the public address of the one to the other.

There is no problem up to this stage, because C, despite having IDs or public addresses of mentioned users, doesn't own their private keys. Therefore, there is not the possibility of entering their conversation, eavesdropping and abusing them.

However, it is supposed that C gives its public address to B or vice versa instead of A's public address. In this case, he/she can gain access to the information which has been assumed to be exchanged between the two. It is here that Blockchain comes in. Blockchain with its unique structure can significantly raise the security coefficient in its infrastructure. However, why?

How Can Blockchain Provide New Messengers' Security?

If you pay attention to the previous example, you will notice that with the existence of a third party in a communication in a messenger, it will be highly probable to lose the security of messages and chats. However, with Blockchain, this problem will be solved. How? In the Blockchain network, each user, or let's say, a computer connected to the Blockchain network, is called a "node."

All existing nodes in the Blockchain store all the users' public addresses or public IDs of the network. These nodes are in relation with each other, and any change in the existing data in Blockchain including public IDs will be reported to all the users. As a result, no intermediary like what has been said, such as C can alter the addresses and IDs. Therefore, when A and B want to make communication, they comfortably will find each other's ID or address, and each makes a two-handed private relationship through private keys unique to themselves.

No one will find a way to this conversation except these two, and exchanging message will be completely private for them. In the Blockchain network, no one has the possibility of gaining access to the others' messages, and it keeps network security at a high level.

Blockchain messengers are attractive tools with no control by the states, engineers, computer technicians, and no other person; that is, you confront a totally independent network which is open source and managed by the users. Lack of a central system in the users' interactions, message exchanges and doing financial transactions cause removing communication limitations from the world of Blockchain messengers. Such facilities are highly appealing and ideal.

How Is Storing and Protecting Security of Messages in Blockchain-based Messengers?

Sending messages and emails is an instance of the most challenging affairs that protecting its security through traditional technology tools is almost impossible. In the centralized systems, with the companies, people and generally a third party which intervene in the relationship between two, there is a high probability that the users' messages and private information be disclosed; however, through Blockchain, you can take the initiative and address making communication and interacting with the users without the need to a middleman who observes messages. Removing the third party from the communications can lead to protecting the users' privacy.

Many different types of Blockchain messengers have been developed. These messengers which are available on Android smartphones, computers and iOS phones gives the total control to the user. What does it mean?

It means that with messengers which work according to Blockchain, managing the messages sent by the user is completely on him/her. This user can decide whether the message which he/she has sent to be deleted in the other person's system or not. Besides, he/she can specify the duration his/her message is in the other's device.

In these Blockchain messengers, by deleting a message, you will remove it forever. It is these users who determine the period after with the message will be deleted or removed. In fact, controlling the deletion of a message is in the hand of the user who sends it. Managing the situation in these messengers is on the shoulder of the users.

All in all, the messages exchanged between the users will be stored on their smartphone or computer, and each message will be encrypted with a unique code specific to that user. As a result, it will no way be possible to read it in the other devices. So when you receive a message in your device, that message is just and solely encrypted for you and it will not be possible for others to gain access to it.

Is It Possible to Make Payments with Blockchain-based Messaging Applications?

Another new and practical feature of the Blockchain-based messaging applications is the possibility to make payments with them. These messaging apps have cryptocurrency wallets. In fact, the world of cryptocurrencies and messaging apps are tied together and in a practical mixture, the new generation messaging apps, have taken distance from conventional messaging apps and have raised to higher grounds.

These messaging apps, do not just provide the possibility of exchanging text and image; they also allow users to trade money with each other in a simple way. Of course, it should be pointed out that this money is a digital currency like Bitcoin. For example, two people agree on the amount of money for the trade and then transfer this money to one another via the existing mechanism in the messaging app.

Based on the various messaging apps that are designed and built based on the Blockchain infrastructure, it is possible to develop their digital wallets. For example, it is possible that a messaging app is created on Blockchain that accepts different Stablecoins and cryptocurrencies and offers the possibility of trade and transfer with them. The possibility of trading money with messaging apps, in addition to the great comfort that it offers to users, is ideal in the sense that there is no sign of surveillance from states or financial organizations and banks.

Therefore, transaction and trades between two people from anywhere in the world become possible. Many countries, because of political sanctions, cannot use payment systems such as PayPal. However, with the possibility of making payments via Blockchain applications, this limitation will no longer exist.

In Blockchain Messaging App, No More Double Spending

In Blockchain-based messaging apps, there is no sign of double spending. This term means spending money twice. Of course, this would not be possible for real and non-virtual currencies.

However, in the world of cryptocurrencies, this is possible. When you spend a cryptocurrency, this action is broadcasted to all the computers in the Blockchain network. In order to confirm a transaction, all nodes must approve it. Therefore, reusing a cryptocurrency in such a network is not possible.

Since all the nodes are aware of the previous transaction and will never confirm the transaction with the same amount of money with the info that they had already received. This feature greatly helps the security of new messaging apps and prevents financial exploitation in the network infrastructure.

Other Uses of Blockchain Messaging Apps

Blockchain-based messaging apps are not used only to trade messages or financial transactions. Their capabilities can be used for a variety of matters. Different messaging apps that are designed based in the Blockchain technology, also offer the capabilities of different social networks such as Instagram and Facebook. However, there is an interesting difference between these two.

The creation of any kind of content in Blockchain-based messaging apps can lead to receiving rewards from other users who have liked that content. As a result, in addition to messaging apps of the social networks type, you will also be confronted with the Blockchain type. Networks in which creating content does not require attracting investors and financial supporters. In fact, if you create valuable content, other users who are your audience will pay for the costs of its creation.

What Are the Top Blockchain-based Messaging Applications Being Developed?

Now that technology has infiltrated different aspect of our lives, and we are enjoying its different tools such as messaging in almost any moment of the day, the need for data security is felt more than ever.

According to what has described so far, messaging networks that operate based on Blockchain are much more than conventional messaging apps. In the following, we will address some of the most well-known of these Blockchain-based messaging apps.

Vibeo

Vibeo is one of the most well-known messaging applications that use Blockchain technology in their structure. This messaging app, in addition to various features such as trilateral video call and the possibility to share location, also employs the messaging encryption system and this makes the application that is supported by the Ethereum cryptocurrency to have a reasonable amount of security.

Dust

Dust is one of the first Blockchain-based messaging applications that has entered the market. This messaging app has some unique features. For example, the messages that are transferred between two people are deleted from their devices automatically every 24 hours.

Line

Line application is a very good app to replace WhatsApp. This messaging app supports all kinds of services specific for message transfer and is available in Android, iOS, and desktop formats. One of the prominent features of this application is the possibility of its being used in countries where the use of WhatsApp is prohibited. In August 2018, this large Japanese social network introduced its own cryptocurrency called LINK to the crypto market.

Kakao Talk

Kakao is a Blockchain-based messaging app that has been launched in South Korea. It is possible to make all kinds of video calls with this application. This application intends to launch various innovations by employing Blockchain technology. We should wait and see that in the end, what kind of programs does kakao Talk has for the modern digital world.

Status

Status is a messaging app that operates based on Blockchain and though it you can gain access to the Ethereum network. This application allows its users to make smart contracts and engage in transactions with Ethereum. Among the characteristics of this messaging app is the fact that all conversations in its are encrypted.

E-chat

E-chat is another Blockchain-based application that along with a multitude of messaging services, allows people to engage in trades with cryptocurrencies. By creating content in this social network, the creator can make money as well. This application is available for a variety of Android and iOS phones.

Other various messaging apps operate based on Blockchain. Variety in this market is on the rise. It seems that given the security capacities and different uses such as making financial transactions, the new generation of messaging apps will soon become prevalent and the time to say goodbye to conventional messaging apps will come.

The attempts by large companies such as Facebook to use the Blockchain technology in its new projects shows that sooner or later, Blockchain and its belonging will conquer the world. Technology is always growing, and if in time it undergoes some changes and evolutions, you should never resist against it.

Many of the advanced countries of the world are analyzing and researching different aspect of the Blockchain technology, and its wide range uses. Unique features that Blockchain can offer users in different fields is really something to think about and cannot be ignored easily.

12

Deploying MimbleWimble Technology and Lightning Network in Litecoin Blockchain

Litecoin entered the market as a similar coin to Bitcoin by Charlie Lee in 2011. Litecoin succeeded in introducing itself as one of the famous cryptocurrencies drawing the attention of activists in this field. Lately, Litecoin development team offered it as one of the famous rivals in the field of cryptocurrencies through adding two new technologies of Lightning Network and MimbleWimble.

Lightning Network enters Litecoin to the scene of competition with existing payment solution such as Visa by increasing the rate of transaction per second (TPS). On the one hand, Wimble improves its privacy besides decreasing Blockchain size. In the following parts, each technology applied in Litecoin is described.

MimbleWimble

The concept of MimbleWimble protocol was suggested by an unknown person with the pseudonym of Tom Elvis in 2016. Then at the end of 2016, a version of it was deployed at GitHub by an anonymous one named Ignotus Peverell.

Currently, two versions named Grin and Beam have been deployed from MimbleWimble. MimbleWimble uses two algorithms of CoinJoin and Pederson commitment. The name of this idea and pseudonyms used in its development have been adopted from Harry Potter stories by J.K. Rolling.

The CoinJoin merges some transactions in one. This method provides privacy while decreasing transactions storing size. The idea of the CoinJoin is exactly similar to the people who collect their money and do a series of purchases.

In this condition, it cannot be specified which money has been spent on purchasing which good. Also, in CoinJoin it cannot be specified that how much has been paid to which address by which address. It just can be generally said that from a set of addresses (inputs) payment has been done to a set of addresses (outputs).

Pederson commitment algorithm adds a hidden string named “Blinding factor” to the end of a transaction and hashes it. The result of this hash is called “commitment.” Reversing the commitment and finding the information of the transaction and Blinding factor are practically infeasible.

From the one hand, through having transaction information and blinding factor, commitment can be regenerated, and its deployment can be investigated. In MimbleWimble, network users don’t have the address and transaction parties share Blinding factor.

Through Blinding factor, the amount of digital assets is specified just for the users engaged in the transaction and the others will not be informed of its amount, since transaction parties investigate its accuracy through regenerating the commitment easily. The validity of a transaction is investigated for the others through using one of the features of the Pederson commitment algorithm shown in the following equation (where C is Pederson commitment algorithm, and BF is Blinding factor):

$$C(BF1, data1) + C(BF2, data2) = C(BF1 + BF2, data1 + data2)$$

Applying this feature, the sum of input and output commitment of a sets of integrated transactions is always zero, since no new data has been generated or destroyed, but it has just been transferred from one person to the other. Therefore, the confidentiality and privacy of the users are maintained in MimbleWimble.

Lightning Network Technology

One of the weaknesses of Blockchain-based payment systems is their low speed compared to well-known international payment systems such as Visa and PayPal, which face them with the challenge of inappropriate inefficiency.

There are important parameters effective when productivity, running speed, and confirming transactions of the cryptocurrency are compared. Normally a fixed amount of time is spent to generate a new Blockchain and add it to the Blocks' chain. For example, this time is ten minutes for Bitcoin and two minutes and thirty seconds for Litecoin.

Each block contains the information of many transactions and has size limitation. Therefore, with generating each new block, a limited number of transactions are investigated. The result of dividing the average size of each block by the average size of each transaction is the average number of transactions per block. From the one hand, the result of dividing the number of transactions of a block by the spent time to generate it introduces the number TPSs for that cryptocurrency. The variable of the number of TPS or transaction rate per second is approximate and is not measurable constantly.

In the Blockchain network, just investigating a transaction is not enough for the payment confirmation. The reason for that is Blockchain vulnerability against double-spending attack. In this attack, the attacker can repay his cryptocurrency in a very short time.

Hence, to confirm a transaction, some new blocks should be added to the block related to that transaction. More blocks being added makes the transaction practically irreversible. The number of these blocks is different for different cryptocurrencies, and it is one of the most important parameters compared to confirmation speed of cryptocurrencies transactions. Doing a transaction without confirmation raises the probability of double spending attack greatly.

The number of required blocks to confirm the transaction in the Bitcoin network is 6 blocks equal to 60 minutes while it is 12 blocks equal to 30 minutes in Litecoin.

According to the experiment by IBM on Visa, which was published in 2017, Visa is able to do 24000 transactions per second while it is about 7TPS and 56 TPS for Bitcoin and Litecoin, respectively.

As it was explained, TPS (regardless of its confirmation) depends on many parameters such as block size, transaction size, and the duration to generate the new block. The most obvious way to increase this rate is to increase the block size and decrease the needed time to generate a new block.

An example of such a change is Bitcoin cash, which increased the size of each block to 8MB in the middle of 2017 with branching from Bitcoin. This change increased its transaction rate up to 61 TPS. Although this method seems efficient in the first glance, it will not be enough to generate a fast and competitive payment system to compete with Visa.

The limitations of Blockchain structure to increase transaction rate is idiomatically called Blockchain Scalability Problem, and there have been many innovations to lift this limitation. SegWit, Lightning Network, and Plasma Cash are among recent innovations to solve the Blockchain Scalability Problem.

SegWit protocol, which is shortened as SegWit, was first introduced in 2015 by Pieter Wiulle at a conference. This protocol provided the possibility of storing more transactions in each block through changing data store method. This protocol was deployed first on May 10, 2017, in Litecoin and then on August 23, 2017, in Bitcoin. This deployment was able to increase stored transactions in each block to 8000.

One of the other suggested solutions for this challenge is Lightning Network. The idea of this method is confirming the transaction without storing it in Blockchain. This idea makes two-way payment channels between users through creating a new layer on Blockchain. Lightning Network confirms a transaction and reset to zero its transaction fee at the very moment.

At first, transaction parties make a Multisig cryptocurrency wallet. Such wallets need some signatures to confirm a transaction. Then, each one deposits a specific amount of cryptocurrency to the address of this wallet. Up to this time, it is called "payment channel launch stage." Now payment channel parties can move the aimed amount through changing the balance of the shared wallet and signing transaction between each other.

Finally, after the payment channel is expired, the final balance is stored in Blockchain. Channel expiry will be agreed upon in one of the following ways: elapsing the specified time or to getting to the defined number of transactions. Payment channel provides the possibility of doing each transaction without paying the fee and needless to the miners for each transaction to reach the due time.

One of the other features of Lightning Network is to provide digital asset exchange between two users without a shared channel. Of course, this entails finding a pathway of channels between transaction parties.

Lightning Network uses a protocol named Hash Time Locked Contracts (HTLC) to do transaction between the users lacking shared channel. Imagine that Alice wants to send Bob 1 LTC. Alice and Bob don't have a shared channel, but each one has a shared channel with a third party named Charlie. Bob (receiver of 1 LTC) generates random string A and sends its hash (H(A)) to Alice.

Alice sends 1 LTC to Charlie, albeit under the condition that he can withdraw it just if he sends the amount A to Alice. Like Alice, Charlie sends 1 LTC to Bob, albeit under the condition that he can withdraw just when he sends the amount of A to him.

Bob, who has generated string A, sends it to Charlie and withdraws his 1 LTC. After earning A, Charlie, too, sends it to Alice and withdraws his 1 LTC. In this way, with the use of intermediary nodes, the possibility of a payment in Lightning Network is provided.

Joseph Poon and Thaddeus Dryja first published the idea of Lightning Network in a paper in 2015. Currently, three well-known teams of Blockstream, Lightning Labs, and ACINQ are developing and deploying this idea. Lightning Network was deployed for the first time in Bitcoin, but currently, it has been deployed in Litecoin, Stellar, Ripple, Ethereum and Zcash. When this paper was being written, Lightning Network had 195 active nodes and 1276 payment channels in Litecoin Blockchain.

13

How Will Crypto Finance Evolve in the Near Future as an Emerging Field?

Currently, there are about 19,000 cryptocurrencies in the world. Each one of these cryptocurrencies offers a collection of services and operations. The application of some of them goes even beyond the field of cryptocurrencies.

Cryptocurrencies have had a lot of achievements. For example, the elimination of middlemen like money order companies and institutes that mediated international transactions are among the benefits and services that they have added to the financial and economic world. Cryptocurrencies do not have a physical form and are able to be transacted in the digital world. This is considered one of their benefits and makes possible tracing financial affairs and transactions.

It is obvious that the presence of cryptocurrencies as new actors in the world of economy and financial affairs can create changes and of course, many new challenges. One of the subsidiary and important branches of cryptocurrencies is the advent of crypto finance.

What Is Crypto Finance and How Will It Evolve?

Crypto finance or open investment comprises an important part of the cryptocurrency economy and is growing quickly. Crypto finance operates mostly on applications and financial protocols based on decentralized networks. These applications and protocols want to enter the financial products in the world of economy and financial markets to a more efficient and effective system by implementing systems based on the cryptocurrency mechanism.

To enter the matter of crypto finance, there is a need for awareness of the basis of its activity and infrastructures. Crypto finance is an open and international financial system. With the existence of the Blockchain network and networks similar to it and cryptocurrencies that are able to be transacted and studied with no boundaries or limits in the world, new fields of financial and economic communications are created.

In fact, cryptocurrencies and crypto finance give a chance to all the people across the world to participate in economic and financial affairs. In different places of the world, there are still people who do not have banks accounts or cards, and for this reason with the existence of decentralized systems like the Blockchain and the use of tools like cryptocurrencies, they can do their financial activities in a free infrastructure without the need for bank accounts and middlemen.

What Are the Outlook and Benefits of Crypto Fund?

There are many interesting and great benefits in crypto funding. Among them are the followings:

Public Access to the Possibility of Investment

One of the main benefits that can be imagined for the investment in the infrastructure of cryptocurrencies is the possibility of public access to it. Cryptocurrencies are defined in the digital world. The way to access to the services available in this world is the internet, and the worldwide web can be available to most people across the world.

Given this possibility, i.e., public access to the internet, there won't be any boundary or limitation for the investment. Activities carried out on the internet can proceed 24/7 and with no off day in addition to more speed and convenience in transactions, and this means the market of crypto finance does not sleep.

The Cross-Border Nature of the Crypt Fund

Activity in the world of crypto finance does not involve border limitations. From anywhere in the world with no specific boundaries and with no need for middlemen, financial and economic trades, transactions, and economic communications can be furthered. This possibility is very significant and ideal and can greatly decrease the costs of transactions.

Since there are no longer any middlemen and fees involved. Also, the speed of financial transfers and communications is very high, and as a result, speed and convenience enter into the world of digital investment. The elimination of third parties like banks from financial trades and communications in the world removes the interference of an outside observer, and everything will go smoother and more efficient.

Freedom in Communications and Lack of Obstacles

In crypto finance, there is a lot of freedom. Because due to the lack of a central element to observe, or in other words, to interfere in people's activities, there will be no censorship, obstacle, and outside observing. In fact, each person is in charge of observing his/her own investment and activities and makes decisions for his/her economic affairs with no obstacles. No transaction will be blocked, observed, or evaluated by banks or financial institutes.

How Is the Outlook and Evolution of Crypto Fund?

With the growth and development of crypto fund, the markets that form around them also grow and develop, and with respect to the capacity and nature that is considered for them in the infrastructure of the digital world, the cost and entrance access to this type of investment and markets will become much more than before.

Liquidity in the crypto finance market is also very good. Many investors in the world are looking into entering the world of cryptocurrencies, and thus, a great capacity for investment in this newfound field can be expected.

What Is Tokenization of Real Assets with Crypto Fund?

There are many assets in the world that can be used in investment; like an investment in the field of real estate, gold, valuable artworks, agriculture products, and different types of physical and tangible items.

However, trades and transfers in this type of investments are rather difficult. Investors further the trades of products and physical assets via bureaucratic methods and paperwork. Tracing the trades in this way is costly and time-consuming. Also, depending on the nature of the paper-based transactions, it is rather difficult to trace them and lacks enough transparency and clarity.

What Is Tokenization?

Tokenization is a brilliant process through which real-world assets can be entered into the digital world. By entering a digital system, investors can liquidate them in addition to keeping the nature of their assets. Digitization of the real-world assets takes place in the infrastructure of Blockchain and its similar networks.

The entrance of data related to real assets well provides the possibility of transactions and digital trades. In the basis of a network like Blockchain, data cannot be changed, and thus real assets are traded easily between two people in trades that have no middlemen, and everything happens transparently and fast.

The age of tokenization of real assets is not so long, but in this short period, it has had some achievements. In the infrastructure of Blockchain, the possibility of tokenization exists, and real assets can be brought to the world of Blockchain.

Such capability, with respect to features like “immutability” in the world of Blockchain, greatly helps the security of data and trades. According to the programs and algorithms that exist in the Blockchain network, no user can tamper with the data in this network. As a result, scam, fraud, and security threats for data are greatly decreased.

With the possibility of tokenizing real assets in the digital world, we will face numerous opportunities for the new markets to be formed in the world of cryptocurrencies. Besides, market liquidity will increase too.

World Economic Forum predicts that in the next ten years, 10 percent of GDP will be used in the cryptocurrency assets. Available security tokens in Blockchain infrastructure are the cash form of real assets. These assets can be in the category of tangible assets like the fame and brand name, or they can be accommodated in intangible assets.

Tokens let the investors experience security, speed, and convenience in their trades thanks to new technologies like Blockchain. In order to have a better view of the tokenization process in real assets, you should pay attention to an example in this regard. Suppose that an investor wants to tokenize a luxurious and magnificent hotel and enter it to the digital world.

The procedure is creating a tradable security token and delegate the hotel to some other people called trustee through forming a trust. After the hotel finds the liquidation capability, it will have some token owners who collectively are the holders of that asset.

Then the tokens of the hotel are registered in a smart contract in Blockchain and considering that some people are capital owners, all have some authorities in the smart contract.

What Are the Advantages of Tokenization?

With tokenization, the possibility of blooming the trades in the market of the assets which are hard to be liquidated gets much more than in the past. Moreover, for instance, the assets which have weaker markets or tracing their affairs is difficult due to the problems in real trades, will enter various international trades more simply through tokenization. Actually, tokenization causes the increase of liquidity of real goods.

Through increasing the liquidity of different goods and booming various markets which has been made possible through tokenization, the investors who are absorbed to the digital market will greatly grow through tokenizing real assets, and this is an outstanding achievement for a technology (i.e., Blockchain and cryptocurrencies) which are just ten years old.

In addition to liquidity, there is another important issue about tokenizing real assets, and it is the diversity which will be bestowed on the people's investment portfolio. With different and various goods entering the digital world, the possibility of the users getting engaged in investment in different fields in the world of Blockchain will get much more than before.

Know Successful Cases of Tokenizing Assets

Following the world of cryptocurrencies and the tokens showing the assets of the real world in cryptocurrencies proves that they are growing. The below list refers to some successful examples of tokenization:

1. Tokenizing gold (Royal Mint Bullion)

Royal Mint Bullion (RMB) is a cryptocurrency which works on Blockchain infrastructure, and it is a gold digital representative in the world of cryptocurrencies; that is, the gold traded on Blockchain infrastructure as a real asset will be exchanged through cryptocurrency or RMB. Each cryptocurrency or RMB coin equals to one gram of gold.

2. Tokenizing properties (Propy)

Propy is an international agency wherein there is the possibility of drawing peer-to-peer contract and solves a very big problem on Blockchain infrastructure. The problem is removing limitations which exist for cross-border property trades. This means that with this international agency which works based on Blockchain, the people can address trading properties wherever in the world. Regional rules are applied for buying and selling in Propy.

3. The tokenizing supply chain for the Pharmaceuticals (Mediledger)

The objective of Medildger project is to trace Pharmaceuticals' route in the supply chain through Blockchain. One of the other important benefits of Pharmaceuticals' supply chain traced in Blockchain, is the possibility of identifying counterfeit drugs. With tracing Pharmaceuticals anywhere in the supply chain, no inappropriate and counterfeit drug will enter the chain.

4. Tokenizing artworks (CODEX)

The world of trading artwork requires more care and attention. The probability of fraud, inappropriate pricing, and slowness of process are high too. However, tokenizing artworks in a specified infrastructure, all will be informed about the origin of the artworks. Existing data about each artistic work are confirmed and registered in the system by the users before they are bought or sold and the starting point in the movement of the artwork will be specified and traceable in the supply chain. Hence, tokenizing artworks will be another service offered form the world of cryptocurrencies and Blockchain.

How Will the Future of Cryptocurrencies and Crypto Finance Be Like?

Since cryptocurrencies and Blockchain introduce various facilities to the world and different areas and industries, the global economy will be greatly under their effect. It seems that cryptocurrencies will come in the world of investment and through influencing dollar and actual currencies, will be included in different exchange markets and investment funds. The presence of cryptocurrencies in the exchange market or investment funds the public's participation for investment will increase.

The prevalence of using cryptocurrencies in retails are among the predictions about cryptocurrencies and Blockchain, which should be taken into account. With including these cryptocurrencies to the world of daily trades and the public getting accustomed to them, the world of cryptocurrencies and Blockchain will dramatically grow. The effects of cryptocurrencies on the dollar and important foreign currencies will provide the possibility of using them in the exchange market, trades, and investment funds. Undoubtedly, the future of cryptocurrencies will be very splendid, and we will hear about them more.

14

How Do Cryptocurrencies and Tokens Influence Global Economy and International Financial Systems?

Cryptocurrencies and tokens will alter the standpoint and the world of economy and financial processes. It is the very thing that is assumed by many experts and activists in these fields. Altogether, do cryptocurrencies and infrastructures like Blockchain, which are the environment for the activity of cryptocurrencies have sufficient capacity to make such changes?

In response to this question, it should be stated that cryptocurrencies and infrastructures like Blockchain will be more effective in the world of economy and financial affairs more than what was expected. Bitcoin came into being around 2009, and after that, other cryptocurrencies were added to the collection of new and adventive currencies.

Undoubtedly, new concepts and tools that cryptocurrencies own will have various effects on the world of economy and communications and financial transactions. Holding digital tokens means holding a tradable asset, and that is the beginning of entering new members from the world of trade, economy, and financial affairs.

What Is the Capacity of Cryptocurrencies in the World of Economy and Communications?

It might be strange that how the cryptocurrencies which are just ten years old, cause changes in the world of economy. From the main advantages and impresses of these cryptocurrencies in the world of economy, solutions can be pointed out that well pave the way for removing different problems.

Before the advent and creation of cryptocurrencies in the digital world, there have been frequent attempts to create digital money, but measures taken in this regard were insufficient and couldn't solve different problems like "double spending." By double spending we mean using a token more than once in financial transactions; however, Blockchain and digital currencies completely resolve problems such as double spending with their entrance to the world of communications and financial transactions.

The network wherein cryptocurrencies like Bitcoin are traded, do not let any alteration or tampering with for the users. Besides, the data require general verification in order to be registered in these systems.

Solutions and strategies cryptocurrencies offer have played an effective role in empowering their presence in a short time. For example, let us speak a little about one important issue; i.e., mining cryptocurrencies. Generating cryptocurrencies is idiomatically called "mining." Mining is, in fact, a process in which cryptocurrencies like Bitcoin are generated, and cryptocurrency transactions are confirmed too.

Cryptocurrency miners are also users who join the Blockchain network and similar systems. Blockchain and systems working with this algorithm are highly accurate and extensive, and although they can be used comfortably, an elaborated and amazing design is behind them. Blockchain and its peers are not useful just in financial industries; they have the capability in various extensive affairs.

Which Changes Do Cryptocurrencies Make in the Current World of Economy?

Every new phenomenon comes along with a series of hopes and fears to the world. As it was pointed out earlier, cryptocurrencies can dramatically change the world of financial affairs, economic trades, and communications through their constructive alternatives. Cryptocurrencies operate based on a decentralized system and remove any middlemen from each communication and trade.

It shows that from the very advent of different cryptocurrencies in the world, many great concerns have been arisen among stockholders of trading markets and players of the economy in the world. For instance, banks and financial institutes will be in the route of persistent threat, or when everybody can generate his/her unique cryptocurrency in the market after passing a process, it is clear that actual well-known currencies like the dollar will face problems, challenges, and threats too. Probable evolutions resulting from the existence of cryptocurrencies will be explained about more in the following sections:

Cryptocurrencies Challenge the Dollar

All know that the global economy is strongly dependent on USD. If cryptocurrencies are included in daily trades and financial transactions, the dollar will not enjoy its former importance. Cryptocurrencies which are somehow capable of being traded in a no-middleman way and no matter where in the world the process of trades will be carried out, they will make dollar valueless and its strength ineffective.

Cryptocurrencies Remove the Middlemen from the Trades

Why are cryptocurrencies popular? One of the reasons of popularity and fame cryptocurrencies such as Bitcoin is not needing any middleman for trading. It is obvious that the world of financial and commercial transactions will continue living needless to any middleman more fluently and without any obstacle.

Suppose that financial transactions are conducted in a few seconds in international aspects easily. What’s your idea about such a possibility? Certainly, the world of no-middleman transactions will be more productive than the one wherein days and hours are required to do every transaction.

Cryptocurrencies Open a New Window to Crowdfunding

Crowdfunding is the public attempt for investment and financing different projects. These projects are usually designed and implemented by the entrepreneurs, and the financial need of various projects is met through crowdfunding by different people as the investor. To put it more precisely, through crowdfunding the process of developing various projects owned by startups and other companies will get operationalized faster.

With cryptocurrencies and Blockchain, the process of crowdfunding will become much simpler. The most important tools of crowdfunding in the world of cryptocurrencies and Blockchain are the ICOs. What do we mean by ICO? It is providing the possibility of investment and activity through offering and awarding coin; that is, cryptocurrencies enable some startups and activists in the field of Blockchain to invest and work. Through ICO, different cryptocurrencies such as Bitcoin and Ethereum will not need using traditional methods such business angels or venture capitalists anymore, which provide financial opportunities for the entrepreneurs.

What Are the Effects of Cryptocurrencies on Exchange Tradable Funds?

Cryptocurrencies like Bitcoin are affective on tradable exchange funds. There have been many attempts to launch tradable exchange funds for Bitcoin so far. However, in a country like the U.S., all these have been banned by the government and the U.S. Securities and Exchange Commission. Some experts believe that sooner or later, cryptocurrency exchange tradable funds will start working and can greatly help their price stability. These funds can give the opportunity for cooperation in economic affairs to many inexperienced people in the world of cryptocurrencies.

Cryptocurrencies Create New Payment Methods in the World

Cryptocurrencies can introduce a new generation of payment methods to the world. As the cash was used for payments in the past and debit cards and credit cards were turned into an important member of payment world by developing different methods in this field, cryptocurrencies and Blockchain are changing this field to a new form. In fact, cryptocurrencies, too, are making fundamental changes in the world of payments and can significantly help the growth of their maturity cycle in the world of economy.

Using cryptocurrencies such as Bitcoin, Litecoin, and Ethereum has become very prevalent in some countries for paying taxis, buying an airplane ticket, and many others. Entering cryptocurrencies to retailers means its wide popularity in public. For example, big and credible company Facebook has planned to amazingly help cryptocurrencies' development through offering its unique cryptocurrency, which is a stablecoin and backed by actual currencies like the dollar. The outlook of this company is the possibility of using cryptocurrencies and transacting with them in the infrastructure of messengers like WhatsApp. As a result, everyone can comfortably and simply do his/her financial transactions wherever in the world.

Will the Performance of Foreign Currency Market Get Better through Cryptocurrencies?

Some believe that comparing and creating every kind of communication between cryptocurrencies and the market of foreign currencies is a mistake. However, some follow another idea and believe that there are some similarities between these two. For example, there is a supply and demand mechanism in both markets (i.e., market of foreign currencies and currencies).

Among other similarities of this market is the price volatilities both currencies and foreign currencies experience. As it was pointed out, there are some differences too. For example, in the market of foreign currency, many players are among institutes and big companies, but about Bitcoin and its peers, the condition is not the same. A large and important part of activities of cryptocurrencies is followed up in the world of retails, and there is no place for big players such as companies.

In addition, the world of cryptocurrencies is decentralized, and there is no chance of common tampering with, fraud or scam; therefore, it surpasses the markets of foreign currencies. The other point which should be told about cryptocurrencies is that there is currently a limited number of cryptocurrencies like Bitcoin in the world and it is not a demand algorithm like that of markets of foreign currencies. Anyway, cryptocurrencies have come to the world of economy, communications, and financial affairs as a totally new tool.

One of the most important points you should know about cryptocurrencies is that they are astonishingly capable of making fast and cheap financial communications and transactions. When the people are able to enter trades in a peer-to-peer manner, the speed and quality of the trades get higher. In the market of cryptocurrencies, on the contrary to the markets of foreign currencies, there aren't many middlemen or agents, and as a result, the cost of trades will decrease strongly. In fact, there is no need to pay fees and charges related to middleman.

All in all, it seems that the market of cryptocurrencies can dramatically change the field of economy. Despite fantastic and unique features such as speed and accuracy of and data registration and exchange in Blockchain-based networks and infrastructures in which cryptocurrencies work, there will consider the possibility of making a dynamic and more productive system with cryptocurrencies in financial and monetary markets.

What Is the Relationship Between Theories as well as paradigms of the World of Economy and Cryptocurrencies?

According to the definition of currency offered by the Webster dictionary, the currency is a tool to trade and public use. So cryptocurrencies are listed in this traditional category. If you are familiar with the world of economy, you surely know that there are specific rules about pricing and providing services and products in the rational market. Various factors influence these issues; therefore, the value of the currency is under the effect of the above cases and effective factors on them. Throughout history, things, precious metals, bills, and different forms of financial trades have entered the world of economy.

It seems that Bitcoin and other cryptocurrencies are following the route of currency evolution in the world of economy. Considering the fact that the features of cryptocurrencies are consistent with the definition of currency, we should consider them an evolutionary sequence of currencies. However, making communication between economic theories and cryptocurrencies is a little difficult. You might notice a kind of inconsistency among these sentences, but we should state that featuring all the specialties of currencies in general, cryptocurrencies are hardly excused in case of old economic matters due to the nature they have. For example, one of the cases which cause difficulty in defining and accommodating every kind of communication between cryptocurrencies and economic theories is that cryptocurrencies are unknown among the public.

Cryptocurrencies are designed and generated with a complex technology, and except few numbers of elite, engineers and experts who follow up the process of their life and production cycle well and carefully and are informed about them, the common people are alienated from it. It is clear that the people are not drawn to a product or phenomenon when they are unaware of it.

Now think, who would like to get engaged in the game of different cryptocurrencies, start trading them without knowing them. Such a condition greatly influences the process of supply and demand of cryptocurrencies like Bitcoin; hence, although cryptocurrencies generally have the features of currencies, the process of their behavior and movement in their maturity cycle is a little different from traditional currencies. As a result, their interpretation with old theories is a little difficult.

Is Evaluating the Maturity of Cryptocurrency Infrastructures Currently Measurable?

Like any other phenomenon, cryptocurrencies have metrics and criteria to assess their status in the market. Evaluating these new currencies is possible through different methods. For example, among excellent metrics which can measure the health of cryptocurrency-based projects are elements like the users' degree of activity, the behavior of network developers and the market maturity.

With receiving available data on Blockchain and analyzing them at two internal levels of each project and investigating the position of its data on the public and general network, evaluating performance and behavior of cryptocurrency infrastructures will be possible.

By assessing the users' activity, we mean investigating the behavior of different people and companies about a specific cryptocurrency and their activity is assessed in relationship with the mentioned cryptocurrency. This evaluation is conducted through analyzing activities in a special part of Blockchain.

Then various digital wallets are evaluated carefully in order to identify and assess the number of users, conducted exchanges in the network, examining digital contracts and other activities done on Blockchain and for a special cryptocurrency.

The other element which is investigated as the metric to evaluate cryptocurrencies and their infrastructures is the developers' behavior. This option, too, addresses investigating and evaluating the level and efficiency of the developers' performance in Blockchain network and assesses cases such as codes changes, codes improvement and the degree of the users' participation in different Blockchain projects which has been along with the development by the developers.

In order to assess the maturity of the market of cryptocurrencies, factors such as money and supply are addressed. Investigating the degree of stability of supply and money in different parts of Blockchain and various cryptocurrencies can offer a good view about the maturity of that cryptocurrency.

What Is the Approach of Different Governments toward Cryptocurrencies?

Despite the growth of cryptocurrencies in the short time of their advent, the world has not trusted them yet. The banks and institutes have been terrified by the decentralized network, which doesn't have any middleman and know them as a threat for themselves. In the best condition, they intend to start cooperating with active projects in the world of Blockchain and cryptocurrencies in order to keep themselves in competition. Different governments have shown different reactions knowing that the cryptocurrencies cannot be ignored.

For example, the U.S. government has well understood that new phenomena cannot be withstood through sanctions and bans, so they believe in using cryptocurrencies, but they have prioritized fully-fledged investigation of these cryptocurrencies and think that there is no place of any risk in this regard.

Also, Europe suffers from the same suspicions the Americans have about Blockchain and cryptocurrencies; the only difference is that the degree of pragmatism in the Europeans are much lower than that of Americans and they have many doubts about the phenomenon of cryptocurrencies.

There are some prohibitions in using cryptocurrencies in countries like China and Russia. These limitations on the part of the above countries are imposed despite the fact that they know well that cryptocurrencies can be the savior in many economic problems and challenges. Of course, it should be pointed out that the relationship of Russia and China with cryptocurrencies doesn’t enjoy enough transparency, and it can be likened to a relationship full of loves and hates.

Generally, cryptocurrencies are going ahead in the route of growth and maturity with an outstanding speed, and it is expected that in the next years, they will greatly influence the economy and the people’s lives. What is obvious is their importance and the fact that they cannot be ignored.

15

Consensus Protocols in Distributed Systems

With introducing different types of cryptocurrencies and the public's welcoming them in recent years, distributed ledger technology (DLT) drew the attention of experts as the main foundation of digital tokens such as Bitcoin.

It has led to the development and implementation of different ideas with various advantages and disadvantage in this field. One of the most important challenges in DLT is the public consensus in the atmosphere of distrust among users.

Public consensus determines true information and protects the network against malicious acts. The methods developed to provide this consensus in DLT are called "consensus protocol." In DLTs which have been designed based on Blockchain, two algorithms of Proof of Work (PoW) and Proof of Stake (PoS) make one of the most basic methods of reaching consensus.

On the contrary to Blockchain structure, a structure named Tangle has been offered to create DLT. Unlike Blockchain, Tangle doesn't have a chain of blocks and provides consensus in another way. Compared to Blockchain, Tangle has some advantages and disadvantages which will be described in the following parts.

Consensus in Blockchain

In the Blockchain structure, each block includes some transactions. Blocks are generated by the miners and added to the blocks chain. The blocks' connections (namely, the chain between the blocks) are provided through the result of the previous block in generating the new block. Two famous protocols for agreement and consensus in these structures include PoS and PoW.

Presently, Bitcoin and Litecoin use PoW and so do Ethereum and Dash from PoS as the agreement protocols in Blockchain structures. In **figure (1)** a part of the chain of blocks has been shown in the Blockchain structure. In this figure, each transaction is depicted by a circle, and the transactions' integrity of a block is calculated via Merkle root.

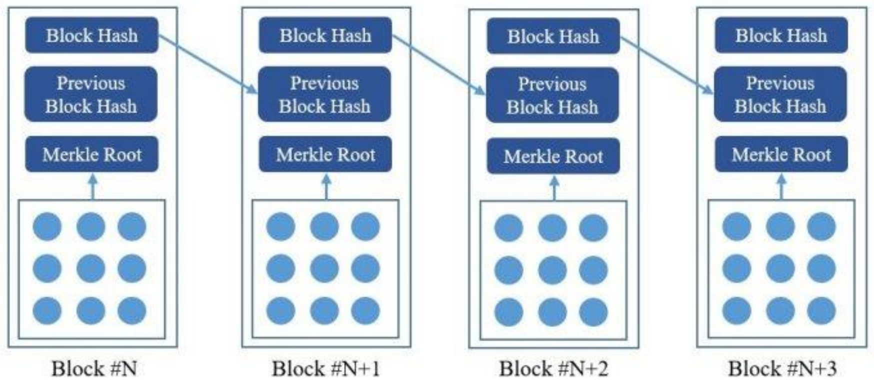

Figure 1) A part of chain of blocks in Blockchain structures

Pow Protocol

In this protocol, the miners enter the contest to find the answer to a math problem. The miner, which succeeds in solving the problem broadcasts its answer along with the new block. Finding the answer of a math problem in this protocol is costly and time-consuming, but investigating the trueness of the answer is comfortable.

The difficulty level of this problem is adjustable in order for the rate of generating new blocks to remain stable. This rate is ten minutes for Bitcoin and two-and-a-half minutes for Litecoin. In addition to difficulty, the odds also play a role in finding the answer, and the miner, which will generate a new block, cannot be specified beforehand. In this competition, the miners should find the amount which result of applying PoW protocol function on it obtains defined conditions as the target.

The functions used in PoW are different versions of the hash algorithm. Currently, diverse samples of this protocol have been developed and applied; the most well-known version whereof is Hashcash. Bitcoin and Litecoin both use Hashcash; however, the SHA-256 hash algorithm is used in Bitcoin, and so is scrypt hash algorithm in Litecoin.

According to what has been explained, it is clear that in PoW protocols, many calculation resources are spent on confirming transactions, creating new cryptocurrencies and adding a block to the Blockchain.

On the one hand, the difficulty level of problems increases in time that entails more calculation power per se. In the experts' opinion, when there are more economic protocols, PoW is somehow wasting resources.

On the other hand, such a high calculation power makes tampering with Blockchain almost impossible for the attacker. Different branches of Blockchain might be made in PoW; in this case, the branch which is longer will be more reliable.

PoS Protocol

It is among other common protocols in Blockchain which offers a distinct method from PoW to make the agreement on generating a new block. The amount of miners' assets (the amount of digital tokens owned) is the agreement criteria for generating new block. Hence, miners should enter the contest in buying digital tokens in the process of confirming transactions and generating new blocks via investment.

As the miner's asset increases, its chance for generating a new block and receiving reward and fee will raise.

All in all, there is no guarantee for a miner with the highest asset to be selected. The most important difference between PoW and PoS is being free of calculation resources in the mining process. So, PoS is idiomatically called “Environment-Friendly”. The competition criterion in PoS of this structure will make it more profitable for the whales.

Tangle

Tangle is recognized as the new generation of DLT. This technology has been developed according to the Directed Acyclic Graph (DAG). It doesn’t have a block-like structure; therefore, it is named Blockless Blockchain too. Such graphs provide high flexibility without extra costs in DLT. Railblocks and Hedera-Hashgraph are popular examples of implementing this idea which are currently used. The most reputable cryptocurrency developed by Tangle structure is called IOTA.

Cyclic graphs are those from a node of which can be started and returned to that node again after passing the other nodes. Considering this fact, acyclic graphs don’t enjoy such routes. By directed graph, we mean directedness of its edges in a way that you can just move in the direction of that edge; the directions are one-way. In **figure (2)** an example of acyclic directed graphs is depicted.

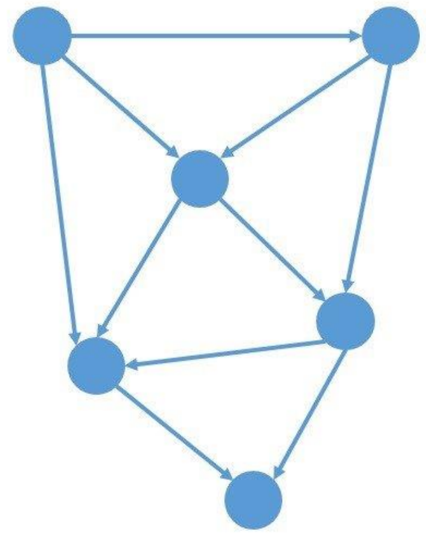

Figure 2) Acyclic directed graph

In Tangle, the transactions are DAGs nodes, and the edges are their confirmations. The new transaction is added as a new node to the graph. This new node is connected to two nodes from the graph.

The direction of this connection is from the new node to those two nodes which have been confirmed. This connection means confirming those two transactions, and all transactions ended to them. The confirmation process is done by the one asking for the new transaction and during which it is assured that the balance of all the accounts is nonnegative.

The first transactions in this structure are called “Genesis” and the transactions related to generating digital tokens. Hence, in such a structure, no new block will be added to the network. The transactions that a transaction confirms directly (through connecting directly) are called “parent transactions,” and the transactions confirmed by them are called “child transaction.” The user should confirm two unconfirmed transactions from the graph before confirming his/her transaction; the process of selecting these two transactions is named “Tip selection.”

This process is started with selecting a genesis and finally ends in the tip of the edge with a random movement. It is natural for the user to conduct tip selection twice to add his/her transaction to the graph. According to what has been pointed out there is no miner in the Tangle structures, so no fee is subtracted for transactions' confirmation. In **figure (3)**, an example of communications between transactions is shown in Tangle structure graph.

In this figure, green nodes are genesis transactions, red one are tips (transactions waiting for confirmation), and blue nodes are transactions which have been confirmed. When a transaction is confirmed directly or indirectly by the other transactions, it becomes a part of the consensus and tampering with it is not possible then.

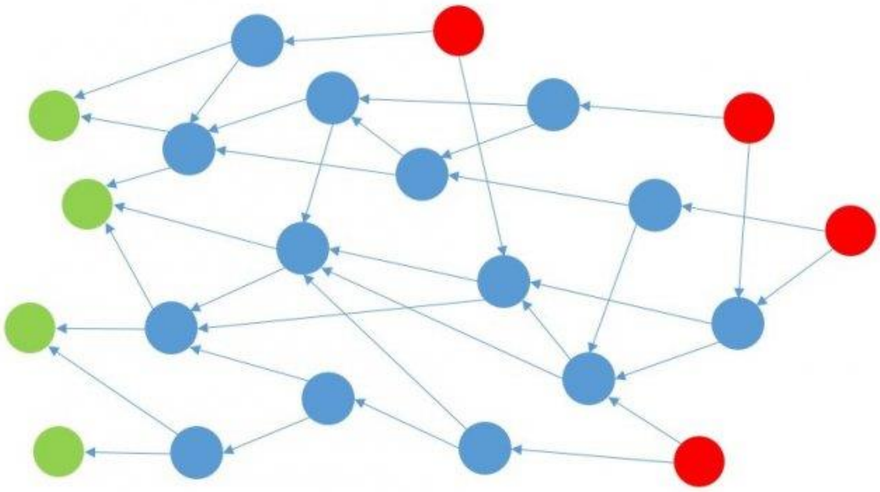

Figure 3) different transactions in Tangle- green nodes are genesis transactions, red ones are unconfirmed transactions (tips) and blue ones are confirmed transactions.

In **figure (4),** transactions which have been confirmed directly and indirectly via purple transaction are depicted in orange. The number of transactions confirming a transaction determines its cumulative weight, and the transactions gets more valid to the extent this amount increases. This feature strongly reduces the possibility of double spending attack in Tangle.

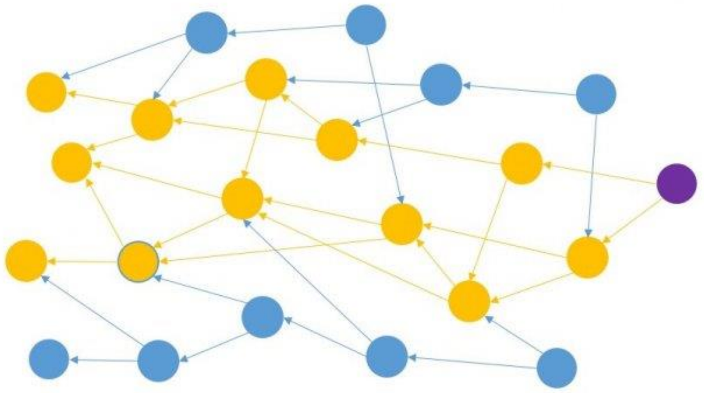

Figure 4) transactions confirmed directly and indirectly by purple transaction are shown in orange

Finally, considering the features of Blockchain and Tangle, the following advantages can be delineated for Tangle technology as a specific sample of distributed systems:

- Tangle spends less energy for confirming transactions, so it is environment-friendly.

- There is no limitation in adding a new user to Tangle and increasing the number of requests leads to the increase of its speed, since new transactions confirm the other transactions, but increasing the number of requests in Blockchain extends waiting line to be confirmed.

- In Blockchain, each block accommodates a limited number of transactions in itself; hence, the network faces limitation of transaction confirmation rate. However, in a blockless structure of Tangle, there is no limitation on the transaction confirmation rate.

- Confirming transactions and keeping accounts balance are carried out with the cooperation of all users. Each user who asks for executing a new transaction should investigate the trueness of other transactions. This idea causes the network not to need any miner through network public participation, and consequently, there will be no need to pay the fees to confirm the transaction.

- Paying fee in Blockchains such as Bitcoin causes transactions with a very little amount to encounter the problem. As an example, the transaction fee of paying charges of a cup of coffee using Bitcoin can be more than the charges of the original good (or service). This very issue makes practicality of such a cryptocurrency uneconomic for simple daily transactions (transactions with the very little amount, which are called micro-transactions). Therefore, Tangle will be a more economic option comparing to Blockchain.

- One of the claims of IOTA developers as the most current well-known structure is its resistance against quantum attacks. Such attacks are made using very high power of quantum computers and provide the possibility of reversing hash function for the attacker. Therefore, many experts believe that by developing quantum computers in the future, the likelihood of tampering with Blockchain will raise, but as IOTA developers allege, due to using Winternitz One-Time signature in this structure, the possibility of making quantum attacks will lower for tampering with IOTA. Despite all positive features of Tangle, its implemented sample by IOTA has a very important vulnerability.

An attacker who owns 33 percent of hash rate of the network, can tamper with it as he/she wishes. To remove such a weakness, IOTA broadcasts transactions named "Milestone" by a unique node called "Coordinator." This node belongs to IOTA Foundation and undertakes protecting the network. The existence of coordinator questions distributed network and somehow creates central management for it. The simplest way to eliminate the coordinator is to increase the network hash rate through increasing the number of users. However, by launching a research council, IOTA founder succeeded in eliminating dependence on coordinator in May 2019 by offering a solution known as Coordicide. Offering this solution resulted in the market’s positive reaction and increased the value of each digital token of IOTA.

16

Everything You Need to Know about NFTs

NFTs are taking the world by the storm. In this article a deep and extensive analysis of these tokens is carried out.

Recently, hardly a day goes by when you don’t hear something about NFTs on the news or on social media. This rather new byproduct of the Blockchain technology is one of the hottest topics right now.

To both professional and novice traders, they might seem like an amazing investment opportunity or even downright absurd. This wide ranging perception with regard to these digital assets is indicative of the fact that most people have yet to realize their full potential. In this article, NFTs will be brought under the full spectrum of a detailed analysis.

What Exactly Is an NFT?

NFT, which is short for a non-fungible token, is a digital asset that is exploding at the moment. NFTs are being sold for prices as high as millions of dollars. These digital assets can take almost literally any form, but mostly art, or rather anything that would be construed as art; as such they could include anything from pictures, paintings, music, gifs, to things like tweets and gaming collectibles.

Perhaps the two most prominent features of NFTs are that their price and value is completely subjective and also the fact that they are purported to be completely unique.

These non-fungible tokens are traded with the help of cryptocurrencies and, as mentioned earlier, could encompass a wide array of assets. One move in the NFT world that really caught the attention of the general public a couple years ago was the purchase of founder of Twitter, Jack Dorsey's very first tweet.

His first tweet, published back in 2006, got sold off for approximately 3 million dollars. But why pay so much for tweet? Why pay millions of dollars for something that everyone has access to? And why pay money for something that everyone can just screenshot and keep a copy?

These have been the questions that most come up with the topics of NFTs ever since they came to fore.

The main reason that can be argued as an answer is that NFTs offer a unique and private form of authentication for ownership over something. So, when someone owns something, whatever it may be, they have a verified and legitimate proof to show their ownership.

History and More Detail

When did exactly NFTs come to occupy the financial hype status? Well, the so called non-fungible tokens have been around ever since the year 2014. Back then, they were mostly used to collect and trade gaming collectibles.

But in the last couple of years, they gained a substantial amount of traction in the buying and selling of artwork, especially the digital kind. In fact, this traction has continuous getting stronger, so much so, that in 2020, the global NFT transactions went over 300 million dollars.

So, an NFT is a collectible digital asset that could come in the form of music, video, art, gaming collectibles, etc. So, in essence, they are considered to be assets for investment.

However, they can also be in the form of cryptocurrency, but distinct from the prevalent forms of cryptocurrency because they cannot be exchanged like-for-like; hence being non-fungible.

The special feature of NFTs compared with other cryptocurrencies is the extra amount of information that they can carry. So, even though there are many different kinds, they can, for example, be a music file or a digitally rendered artwork. So, basically, they can hold any form of valuable data that can be stored digitally. In this case, instead holding the physical version of the Mona Lisa, you will receive a JEPG file of a unique painting.

But what exactly would be the different between your especially owned NFT JPEG file compared with any other JPEG copy on the internet?

The point here is that NFTs carry with them unique identification and authentication codes. These codes manifest a token that has digital scarcity. This is exactly the opposite of all the digitally rendered creations that can be found all over the internet. This scarcity and limited supply is what gives NFTs their value.

So, when you have an NFT, even though other people can just as easily access it simply by Googling it, you are its rightful, legal, and legitimate owner; and so to speak you have the bragging rights over the item. Something that literally no other person on earth would have. Thus making NFTs a tamper-proof, unique, and valuable form of ownership.

How Does an NFT Function?

Much like any other recorded crypto transaction, NFTs are also units of data that are stored on a digital ledger or otherwise known as a Blockchain network. But, as pointed out before, these bits of information do not merely hold financial transaction information. Indeed, they can hold any kind of extra information, taking the form of video, music, GIF, JPEG, etc.

NFTs are purchased and sold off like any other artwork or asset. As such, various factors in the market, including scarcity, rarity, supply, and demand regulate their value and price.

For instance, some of the most popular NFTs are bought and sold in marketplaces that implement the Blockchain network of Ethereum. So, when you purchase an NFT, the information relating to this purchase and transaction are all recorded in the Blockchain network of Ethereum. That is precisely what makes the owner of the NFT distinct from any other use who would merely right click and save the file.

All in all, it can be said that NFTs are like a form of cryptocurrency transaction that is recorded on a digital, public ledger or a Blockchain network. But with the difference that they cannot be traded or exchanged one by one or at equivalency.

How Are NFTs and Cryptocurrencies Different?

So the non-fungible tokens and the cryptocurrency are all based on the very same technology – Blockchain. The technology that has been taking the world by storm.

So, as we know, the Blockchain technology offers a public ledge on which information and data related to transactions can be recorded. This can be done in a way that the records are unchangeable, tamper-proof, completely transparent and all around fully safe and secure.

Both the NFTs and the cryptocurrency implement this technology to records their transactions.

So if both of them are recorded on the Blockchain, what is the difference between NFT and crypto?

The most important distinction between these two is the notion of fungibility. Cryptocurrencies can be traded and exchanged with one another denoting the same value or equivalency. But as we have already seen in this article, NFTs are not tradable one-by-one sine they lack equivalency like cryptos. And that is the difference between these two.

What Are NFTs Used for?

There are various advantages in using NFTs and the technology pertaining to it as a whole.

For starters, now with the help of these tokens, all artists can easily monetize their work. Something that would have been inconceivable before. Since they had to go through the conventional monetizing process, most probably having to go through a third party agent that benefits from commissions.

However, now with the help of NFTs all artists, not matter how professional or amateur, can sell their work on their own without any intermediary directly to the customers.

In addition, an unprecedented degree of privacy and assurance has been provided for the artists. Prior to the Blockchain era, it was evidently and clearly not unheard of for artists to be beret of the rights to their work. A clear example would be Margaret Keane, who did not enjoy the full benefits of her work until much later due to her work basically being plagiarized and stolen.

But with the help of NFTs artists can own the rights to their artworks like never possible before. The full information of the creators in addition to the new owner can be recorded in the metadata of the NFT, which could include the signature of the creator, or any other data.

So NFTs are empowering artists and content creators in a way that has never been possible up to this point. But this is not where the functions end. As Metaverse is becoming bigger and bigger, NFTs are gaining a much more important role, as a very serious and legitimate method of investment and also transferring ownership over value.

Risks and Controversies

With all the benefits and advantages tied to the non-fungible tokens, there are a lot of controversies surrounding these tokens.

One of the major criticisms posed toward the NFT world has to do with environmental factors. Since creating an NFT requires a huge sum of energy and electricity, the generation of which, in turn, requires a great deal of non-renewable natural resources.

There have been some murmur as to when NFTs can become carbon neutral. But still, the verification and authentication process of these tokens still heavily rely on proof of work algorithm, which of course, consumes a vast amount of energy.

The environmental factors are among the reasons why some are holding back from entering the market. But there are also some risks that are linked with NFTs.

Just like any other form of investment, NFTs can also be very risky. The value and price of these tokens are never guaranteed. No one knows if they might go down; especially as demand and attention is increasing, which in turn would increase the supply to a great degree. In addition, authenticating and verifying whether you are purchasing the NFT from the original creator can be a difficult task.

The Future of NFTs

Everything considered, the road ahead of NFTs seems rather uncertain. Some say that at any moment this trend could end. At the same time, it may not even be a trend, and actually become the next big thing in the world of investment. Especially with as Metaverse is growing ever larger.