The Potential role of IOTA in DLT Technology.

Bibek Adhikari

Table of Contents

Abstract

The purpose of this article is to inform the reader on some of the most significant difficulties confronting DLT today, as well as potential solutions to those issues. It will look into centralized, decentralized, and distributed systems. It will also explain what distributed ledger technology (DLT), blockchain, and IOTA are and how they vary from one another. Despite the fact that this essay focuses on IOTA, we must comprehend the use, application, challenges, implementation, and so on of Blockchain technology. IOTA is a novel technology that must overcome a number of challenges before realizing its full potential.

Furthermore, there is no agreement on its potential worth, with some predicting it will bring greater disruptive changes than the Internet and others disputing its significance. This paper explains the Trilemma's primary difficulty and how IOTA might overcome scalability, one of the most crucial applications in DLT. It also explains the technology's future and the problems that must be solved. The system must maintain a global picture of the world while competing and seeking to create a consensus among a group of untrustworthy parties. IOTA, on the other hand, is more than just a cryptocurrency. As a result, this study investigates and explores its prospects in various disciplines such as Decentralized Autonomous Organizations, Internet of Things (IoT), Supply chain, Energy and Ehealth, which are attracting increasing research efforts from both academia and business. It also covers the usage paradigms and current concerns surrounding the use of IOTA to develop dependable IoT systems. This paper offers a study of the rapidly emerging field of IOTA, analyzing its benefits, potential downsides, and implications for the future of the Internet, as well as the problems that must be solved. As a result, the topic is 'The Potential Role of Iota in DLT Technology.'

Introduction to DLT

Distributed Ledger technology, more commonly known as DLT, has a long remarkable history. The systems have been developed for millennia. Distributed ledger technology (DLT) is a system for documenting asset transactions in which transactions and details are stored in multiple locations at the same time. Unlike traditional databases, distributed ledgers do not have a centralized data store or administrative capability. In other words, it is a peer-to-peer network in which each device replicates and stores an identical copy of the ledger while independently updating it. Without a central authority, this system has a distinct benefit. When it comes to the Leader, it can be centralized or distributed, with all nodes agreeing on a protocol that determines the true state of the ledger at any point in time.

Historians have recorded the earliest history of DLT in the Roman Empire, hosting a banking system allowing citizens to participate in transactions from different empire regions. Which help Rome achieve its historic status. Digital versions of DLTS first appeared in 1991[1]. The original DLT notion, as it is now understood, was then introduced. Although, the first DLT was merely a concept written about in a paper by two researchers named Stuart Haber and W Scott Stornetta[1]. Their paper, How to Time-Stamp a Digital document, began to take the form of establishing and modify digital documents as a basis for a digital DLT.

It is possible for DLTs to function in a variety of ways. The primary data structure in most distributed ledger systems is a singly-linked list. As a result, transactions cannot be handled concurrently. The state of the network must be confirmed by consensus in all DLTs. Network participants can validate the network's state with the use of a consensus method. Proof-of-Work (PoW) and Proof-of-Stake (POS) systems are the most common consensus techniques in blockchain (*Will be elaborated in Introduction to Blockchain*) technology. Both approaches achieve the same goal, although in different ways. Network nodes compete to solve a complex mathematical equation in a Proof-of-Work system. In a PoS system, the same thing happens, but it's done differently. Users can validate transactions using stake, an incentive-based mechanism. Therefore, nodes in the network are frequently divided into those that issue transactions and those that validate transactions. [1] [2] [8]

DLT has vast potential to transform the working of governments, institutions, and businesses. This can support governments in collecting taxes, issuing passports, registering land registers and permits, and spending social security funds and voting procedures. In businesses such as finance, music and entertainment, diamonds and other valuable good, art and the supply chain of different commodities, and more, technology creates waves. However, aside from those associated with the products being utilized, distributed ledgers are not immune to risks and limits (e.g., crypto-assets).[6] [7]

Blockchain

Introduction to Blockchain

The introduction of blockchain networks to the DLT sector was a significant step forward. It meant that, for the first time in history, a trustworthy and verifiable digital currency could be used. The blockchain is a distributed database that stores records of all transactions or digital events that have occurred and are shared among participants. It contains every single transaction record. Typically, this storage is referred to as a 'digital ledger.' Every transaction in this ledger is authenticated and protected from tampering by the digital signature of the owner. As a result, the digital ledger's information is extremely secure.

So, the primary idea behind blockchain technology is to create a network of multiple users or computers known as "Nodes" that can conduct secure and valid transactions directly without the need for a third-party intermediary. Any authorized network node can view the collection of records added as a genuine block in the blockchain. As a result, the blockchain system is an irreversible, distributed digital public ledger that can record both financial and non-financial transactions.

The first mention of blockchain-like technology dates to 1991, when Stuart Haber and W. Scott Stornetta published their initial work on a secured chain of blocks. Ten years later, in 2002, David Maziarz proposed the concept of decentralized trust within a network file system. 2009 was the year that Bitcoin revolutionized everything. The introduction of blockchain networks to the DLT market was a huge step forward. Digital money could now be used for the first time. The launch of Bitcoin signals a global uptick in the development of distributed ledger technologies. Even today, these DLT improvements continue to produce exciting discoveries. [26]

Blockchain Technology: Fundamentals and Functionalities

Many researchers and financial people think that blockchain will be a disruptive technology and a vital source of innovation in global markets in the future. It has the potential to revolutionize our society and the new global economy. As we know, blockchain is a digital, decentralized, and distributed ledger that is continually being updated. In a particular network, this technology allows for the recording of transactions and the tracking of assets to construct a chronological "chain" of blocks, and the transactions are bundled into data packages known as "blocks" and linked to those that came before them. This blockchain provides a trail of the underlying transaction and, thus, represents a complete ledger of the transaction history.[3]

Blockchain implements "peer-to-peer technology," which allows users to connect without the need for a central point of authority or control. This enables decentralized transaction processing, which means that anyone in a particular network can send something to anyone other, eliminating the requirement for a central authority to verify trust and transmit something of value. Another distinguishing feature of blockchain is that it is "consensus-based," which means that a transaction may only be recorded if all network participants approve it. Swanson (2015) defines the consensus mechanism as the method through which a majority (or, in certain situations, all) of network validators agree on a ledger's state.[16]

It would be impossible to list all of the characteristics and functionalities of blockchain, but some of them can be seen in the figure below.

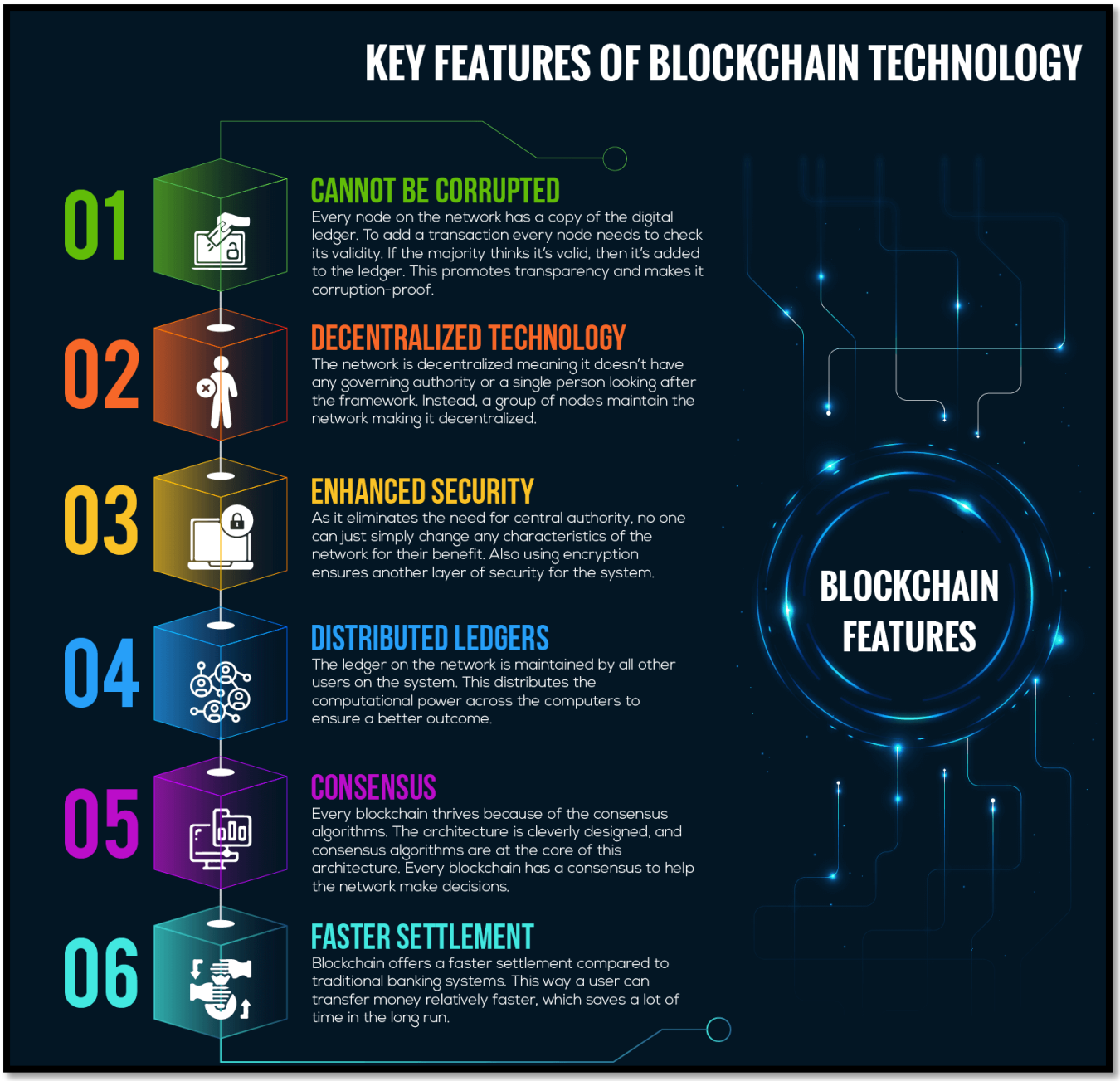

Figure 1: Features of blockchain Technology [38]

Application

Blockchain applications are far more than just bitcoin and cryptocurrency. With its ability to increase visibility and fairness while also saving businesses time and money, technology is influencing many industries in ways ranging from contract enforcement to government efficiency.

We can accept or reject Blockchain technology, but we cannot deny its role in cryptocurrency and decentralized technology for various purposes. It is impossible to ignore the fact that $23.7 billion has been spent in blockchain applications globally, with 3738 blockchain enterprises established since 2013.[19]

Here are some real-world blockchain application examples for this technical yet innovative technology. Although this is by no means an entire list, they are already influencing how we do business.

Digital Currency

Cryptocurrencies are just like any other type of currency. You can purchase and sell goods and services with them, as well as trade with them. The difference between them and typical paper currencies in our wallets is that there are no tangible coins or notes - the money is entirely virtual. [25]

Each coin is essentially a computer file that is kept in a digital "wallet" and can be accessed via smartphone apps or internet-enabled devices. These files can be transferred (in whole or in part) from person to person using blockchain technology. The ability to transfer currency with a single click of a finger without the involvement of central authority makes the technology appealing for use as a currency. There is an involvement of miner in mining digital currency. A miner is a participant in cryptocurrency transactions who, in return, plays an important role in both the creation of new cryptocurrencies and the verification of transactions on the blockchain.

Medicine and Health Industry

Blockchain in healthcare, while still in its early stages of adoption, is already showing promise. Indeed, early blockchain systems demonstrated the potential to cut healthcare costs, increase information access across stakeholders, and expedite business processes. An innovative method for gathering and sharing private information could be precisely what the doctor prescribed to ensure that an already overburdened industry can cut extravagant expenses.[20]

Medicalchain (London), Nebula Genomics (San Francisco), and Patientory (Atlanta, Georgia) are the companies that use blockchain platforms for the more accessible and more secure flow of sensitive medical information between doctors and patients. [27]

Money Transfer

Blockchain is especially popular in banking due to the money and time it may save financial companies of all sizes. According to a recent ComputerWorld article, blockchain can commit the significant banks $8-$12 billion per year by eliminating bureaucratic red tape, making ledger systems real-time, and cutting third-party fees.

Several companies operate based on a blockchain-based money transfer system. However, Zcash, Ripple, Veem, and Ivy are a few of them.[22]

Internet of Things

IoT -The Internet of Things is the next natural step in the evolution of blockchain applications. IoT offers millions of applications and many safety concerns. As the number of IoT products grows, hackers will have more opportunities to steal your data from everything from an Amazon Alexa to a smart thermostat.

Blockchain-infused IoT adds a greater level of security to prevent data breaches by leveraging the technology's transparency and virtual incorruptibility to keep things "smart.". [27]

Logistics

Due to the enormous number of logistics companies crowding the field, a frequent criticism in the shipping industry is a lack of communication and openness. According to a collaborative study conducted by Accenture and logistics giant DHL, over 500,000 shipping companies in the United States alone, resulting in data silos and transparency difficulties. According to the paper, blockchain can alleviate many of the challenges that plague logistics and supply chain management.

According to the new study[23], blockchain provides data transparency by providing a single source of truth. Blockchain can increase industry trust by acknowledging data sources. Additionally, the technology can make the logistics process leaner and more automated, potentially saving the industry billions of dollars every year. Blockchain is not only a secure solution, but it is also a cost-effective solution for the logistics business. Here are a few companies that are at the forefront of logistics blockchain technology.[23] [27]

Citizen Services and Government

One of the most unexpected applications of blockchain could be to improve government services. Due to a lack of basic information, approximately one-sixth of the world's population cannot engage in political, economic, and social life. Blockchain technology offers a significant chance to tackle this problem by developing cryptographically secure digital identity systems. To provide a variety of citizen services and to eliminate certificate forgery and identity theft, governments, and non-governmental organizations (NGOs) can employ digital IDs. Voatz voting App is one example that works in the field of Government, Cybersecurity, Politics.

Blockchain also creates waves in social media, music, gaming, real states, energy, non-fungible tokens (NFTs), automotive, and manufacturing. [27]

Figure 2:Applications of blockchain [39]

Implementation of Blockchain Technology

Technology	Implementation
Ripple 	• Ripple is the company and XRP is the coin. • Its products are utilized in payment settlement, asset exchange, and remittance systems similar to SWIFT.
EOS 	• It blockchain-based platform that enables the development of business applications. • EOS cryptocurrency tokens are used as a payment system on the network.
VeChain 	• It is a blockchain platform that is intended to improve supply chain management and business processes.
Ethereum 	• It is a decentralized public ledger that is used to verify and record transactions. Users of the network can create, publish, monetize, and use applications on the platform, as well as use the Ether cryptocurrency as payment.
Bitcoin 	• Bitcoin was developed to allow people to send money over the internet. The goal of digital currency was to establish an alternate payment system that would be free of central control.

Blockchain Issues and the Blockchain Trilemma

Problem with Blockchain

There is no doubt that Blockchain technology will transform the world around us. However, in order to comprehend what it has to offer, we must first recognize its drawbacks. We will go over all the concerns in this part. I will use Bitcoin as a reference example from time to time because it is the most popular cryptocurrency that possesses all the blockchain qualities.

Distributed Computing System

Blockchain is a network that relies on nodes to function effectively. The quality of the nodes determines the quality of the blockchain. The network does not rely on the nodes' involvement and participation. A distributed computing system, on the other hand, works to ensure that transactions are verified according to the rules, that they are recorded, and that they have the transactional history for each transaction. Each of these operations is analogous to blockchain, but each one lacks coordination, mutual help, and paralleling. Evidently, blockchain is a distributed network, but it lacks the elements that make a distributed computing system so valuable to businesses[32], [33]

Scalability

The Blockchain scalability problem refers to the blockchain network's limited ability to manage massive amounts of transaction data on its platform in a short period of time. It is connected to the fact that the amount and frequency of records (known as blocks) in the blockchain are limited. There are several significant issues affecting blockchain scalability, including:

Limitations

The first Bitcoin scalability issue includes limits. When a new transaction is processed, every node contributes information to the ledger. As a result, as payment history grows, there is a risk of buckling the total system. All data should be entered accurately; otherwise, the level of trustworthiness may be lowered. On the hardware side[37], there are various constraints. When two blockchains become this large, it is impossible to host a node for both.

Block size

Another significant Bitcoin scalability issue is block size. Initially, each block on the Bitcoin blockchain had a size of 1 Mb and could hold up to 2,020 transactions. However, as the network's transaction volume has grown, another blockchain scalability issue has emerged: the time-consuming process of transaction execution.[37]

Response time

Every transaction in the network must go through a validation process. When there are a lot of transactions in the queue, they normally have to wait a long period for their validation. A new block, for example, takes about 10 minutes to build in the Bitcoin network. The longer a transaction sits in the queue, the longer it takes to process it. This rises at busy hours.

Fees and mining

The process of confirming transactions becomes more complicated as the popularity of cryptocurrency grows since mining requires more processing power. Every transaction necessitates the payment of transaction fees. You can pay a greater price if you want your payment to be verified faster. As the network grows, many new users want their transactions to be executed. As a result, a large number of unprocessed transactions are waiting to be validated in the queue.

Too Much Energy Consume

Every transaction must go through consensus processes to confirm its validity. Obviously, the consensus process needs a significant amount of effort to construct each node. Not to mention that all nodes must communicate with one another to confirm that a transaction is genuine. Consensus techniques, on the other hand, such as proof of work, demand a lot of processing power, which raises the overall power usage. The findings suggest that Bitcoin alone consumes as much electricity as a medium-sized European country.
To put it on prospective here are some fun facts:

- Ethereum’s annual energy consumption used to process its crypto transactions is roughly equivalent to Nigeria's annual energy consumption.
- According to a Cambridge University study Bitcoin training consumes more electricity than Argentina does in a year.

Cost And Implementation Struggle

The true cost of using blockchain technology is enormous. Even though most blockchain solutions, including Hyperledger, are open source, they demand significant investment from the company that want to pursue them.

Expertise Knowledge

It is difficult to implement and manage a blockchain project. Going through the entire process involves extensive expertise from the business. They must recruit many blockchain professionals, which causes a problem and is seen as one of the blockchain's downsides. [33]
If we continue to outline the shortcomings of blockchain technology, we will run out of space. However, the blockchain trilemma can be used to summarize the fundamental difficulty of Blockchain technology.

Blockchain Trilemma

In a nutshell, the Blockchain trilemma is a set of choices that precludes blockchain technology from attaining all three goals of decentralization, scalability, and security.

The most concerning problem of our day is the scalability of blockchain networks, especially since consumers are paying hundreds of dollars in transactions of various sizes, thus resolving the blockchain trilemma is a hard job, but the endeavour is worthwhile given that it will lead to a sustainable and long-lasting crypto industry. The blockchain trilemma is a notion coined by Vitalik Buterin, the creator of Ethereum that suggests a set of three fundamental properties that are difficult to sustain in a blockchain network at the same time. Often creators are forced to sacrifice one for the other two which leads to problems for users and developers alike. they better understand the significance of each aspect we will review them individually, so let's start with one feature that is the hardest to attain that is scalability.[34]

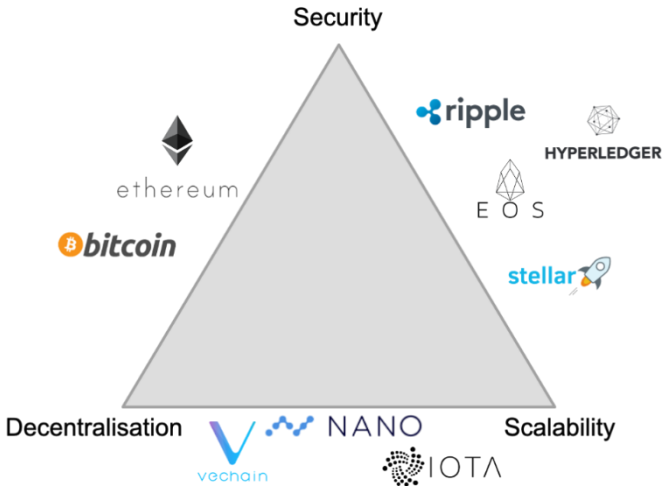

Figure 3: Blockchain Trilemma [41]

Instead of a binary future, scalability measures how efficient blockchain networks are in processing transactions. Scalability is a scale that can reach both ends of the spectrum at any time, depending on the workload. Specific crypto project's incredible speed listing numbers are comparable to large payment processors such as Visa and MasterCard. However, such blockchains are rarely capable of supporting claimed transactions when serving millions of users. We can't talk about widespread global adoption until we fix the blockchain's scalability problem, generating network congestion and hundreds of thousands in fees. Hardly anyone is willing to use projects like Bitcoin or Ethereum when they're highly inefficient.

So why is scalability advantageous? First, it enables blockchains to support a higher workload than the existing standard for public and decentralized networks. Ideally, it should be able to scale well even in harsh conditions and demand with our technology, and developers must sacrifice security to scale networks enterprise blockchain solutions. Second, switching to permissioned networks, which lack decentralization but provide breakneck transaction speeds, is challenging to accomplish without damaging the underlying concept of decentralized technology.[35]

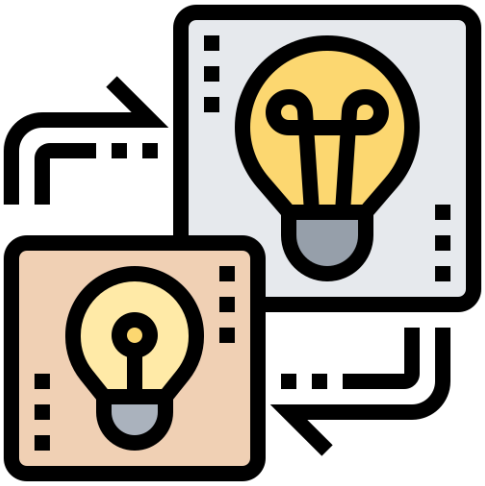

Figure 4: Scalability[34]

After all, the only thing developers must do to ensure that no central authority prevails and that enough nodes are powering the network is to implement decentralization in a blockchain network. The benefit of decentralization is that everyone has equal standing with other users. No one has unique rights or advantages, and unlike banks, nobody can limit your freedom or freeze your account because the feature has shown to be a significant asset. However, in this industry, blockchain technology is constantly being pushed to the forefront of the new technological revolution that, while decentralization is nice to have, does not compensate for the fact that developers must give it up to improve a blockchain's transaction speed achieve peak decentralization. Blockchain networks utilized the proof of work consensus model. The higher number of nodes, the more decentralized blockchain is. However, evidence of works disadvantages is that it consumes too much power and cannot scale well with many users. [34] [35]

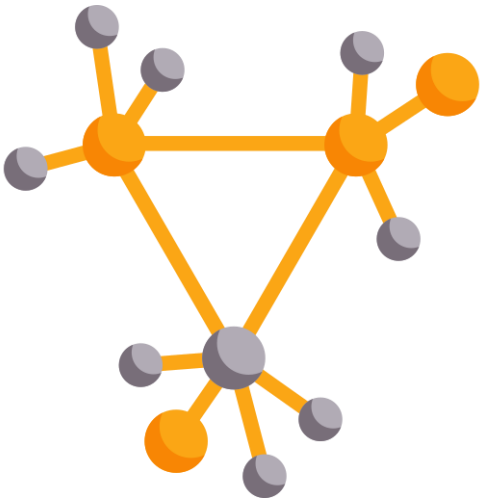

Figure 5: Decentralization [34]

Finally, we have a feature that is crucial for blockchain networks security. Without security, malicious activities can disrupt blockchains by manipulating transactions or performing famous exploits like the 51% attack if the data stored on the Ledger can't be immutable. And foreign actors can disrupt a system so quickly. What is the value of decentralized technology if banks and other legacy financial institutions are still around? The blockchain network has a smart contract functionality feature; nonetheless, the problem is significantly worse, even though hackers cannot change the Ledger. They can use features such as flash loans to steal millions of dollars from investors. In this context, security is a critical factor that cannot be overlooked. The purpose of a safe blockchain is to maintain stability and function, which is a word decentralized and data that cannot be altered. Security is not a feature that must be sacrificed for scalability or decentralization neither speed nor concentration of power is impacted by the scale of security. Which leads provides developers with lots of breathing room while developing a blockchain.

Figure 6: Security [34]

To summarize, security is a critical component of current blockchain systems since it allows hostile actors to disrupt networks and change data stored on a Ledger. As a result, Blockchains would be entirely unstable and useless without them.

Now we get to the section where Iota ((will be discussed further in a future IOTA article.) plays a critical role in resolving the Blockchain Trilemma problem. I am not saying Iota can solve the whole Trilemma, but current IOTA DLT solutions can guarantee a maximum of two of these three properties simultaneously. This problem is known as the "scalability trilemma. " Iota is the only DLT that will most likely be able to solve the Crypto Trilemma. Scalable, quick, and accessible. No other decentralized technology manages this, and once the coordinator (discussed in Upcoming Topic) is gone, Iota will be the first.[36] .

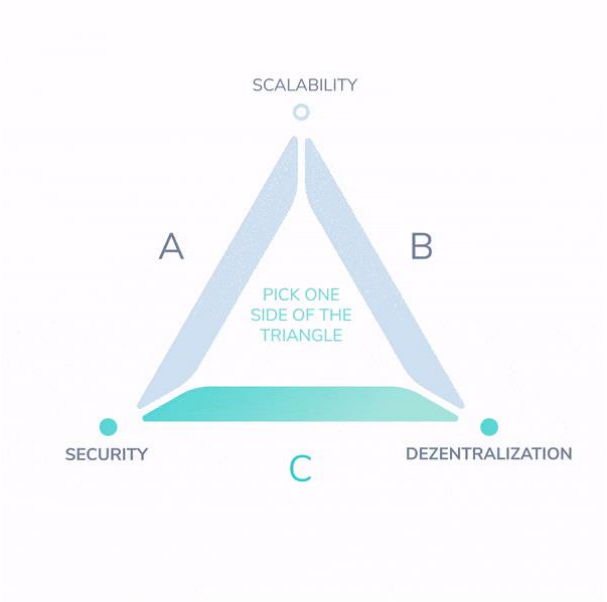

Figure 7: Scalability Trilemma

IOTA

IOTA Foundation

In 2017, the IOTA Foundation was founded as a non-profit organization in Germany. It was founded by Dominik Schiener and David Snsteb. It was initially funded through a crowd sale in December 2015. Initially, the IOTA founding team did not keep any IOTA tokens for themselves. The community was kind enough to donate around 5% of the overall supply to the IOTA Foundation, the non-profit organization that manages IOTA.[31]

Introduction

IOTA is the first distributed ledger designed for the "Internet of Everything," a network exchanging currency and data between humans and machines. Iota is one of the most prominent and distinctive cryptocurrencies. It was just a few years after the debut of Bitcoin that iota was postulated as a quicker, more efficient decentralized Ledger to create the first permissionless feeless and production ready distributed Ledger technology for the true Internet of everything. They termed the DLT Tangle, and it is built on a mathematical idea known as the directed acyclic graph, which, like the Bitcoin blockchain, can be used as a Ledger to track and execute transactions without the usage of blocks and chains. Iota was able to combine a minor validator and a user into a single entity because to the design. This eliminates the requirement for transaction fields. When you use iota, your device takes on the responsibility of processing two or more transactions in the tangle. This process requires nothing more than some computational power from whatever device you're using. This not only makes iota exponentially fast in theory, but it also makes iota free to use. This is significant since iota was created primarily to support micro transactions for the Internet of Things,

which implies that you may transmit even fractions of a cent to other users. As we speak, iota is entering a turning point in its evolution as it moves closer to realizing its vision of enabling a true machine economy. [29]

Digital identification is a vital idea that a distributed ledger may achieve. Authentication must be ensured in a distributed infrastructure such as the internet to create confidence between two or more parties. A tamper-proof digital identity of Internet-of-Things (IoT) devices and even human persons might be stored in such a ledger. The digital identification history would be unchangeable. This means that identity would only need to be approved by some authority once but would earn trust for the rest of its life.

Blockchain is the most prevalent DLT that has the potential to enable comprehensive digital identification to date. The two assets with the most significant market capitalization are Bitcoin and Ether, traded on the Bitcoin and Ethereum blockchains, respectively. However, despite its popularity, Blockchain technology has two fundamental flaws when it comes to high-load applications, such as Internet-of-Things:

- limited scalability
- fees per tx(transaction)

However, the two assets mentioned use cryptographic functions that are not quantum secure (yet). In response to these difficulties, the IOTA Foundation created the Tangle technology in order to provide IoT with a proper distributed ledger. Because millions of devices will send a tremendous amount of txs, a scalable ledger is required. This includes micro-txs, which send little tokens/money, and zero-value txs, such as messages or sensor data. This means that if a device had to pay the price for each piece of data it sent to peers, many IoT situations would be unprofitable. The Tangle has many similarities to the Blockchain but allegedly solves the beforementioned problems. [29]

We must understand that IOTA does not seek to replace Bitcoin as a currency or Ethereum as a generic DLT-facilitator. Rather, it focuses on IoT use-cases, particularly in the automobile sector(Explained more in Mobility), where the Tangle can demonstrate distinct advantages over the Blockchain.[28]

Features of IOTA

IOTA Tangle

When bitcoin was released first in the world in 2008, it started a revolution. People claimed that the blockchain would solve many problems and that it has countless applications. Blockchains indeed have exciting properties. However, they have one significant limitation, and that is that they don't scale very well. This is precisely the kind of problem that the creators of iota wanted to solve. So, instead of using a blockchain, iota uses something called a DAG or tangle. DAG is short for directed acyclic graph, and it is a storage system where individual items are linked to each other. Directed means that the link between these items always has a direction, and acyclic means that you cannot create loops inside the structure. This might sound complicated so let's look at a simple tangle diagram below.

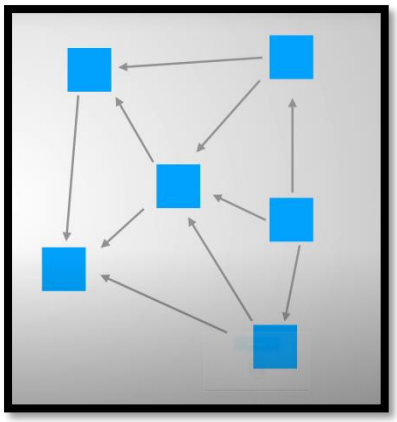

Figure 8: A simple tangle

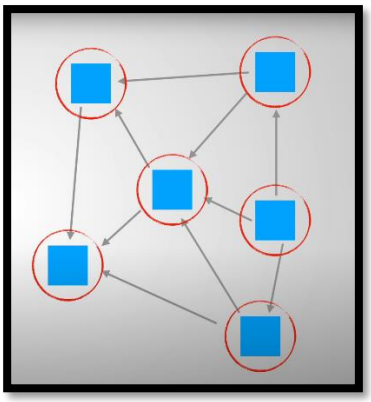

Figure 9: sites/ transaction

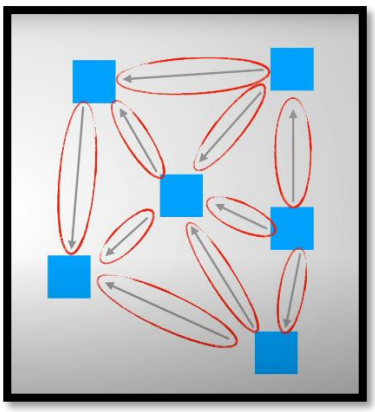

Figure 10: edges

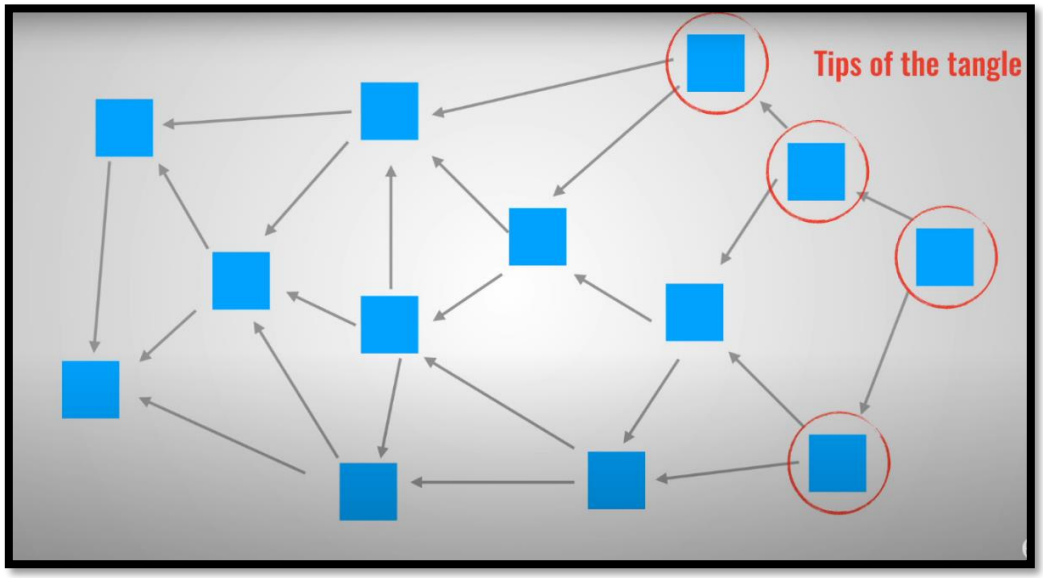

Figure 11: Tips of the tangle

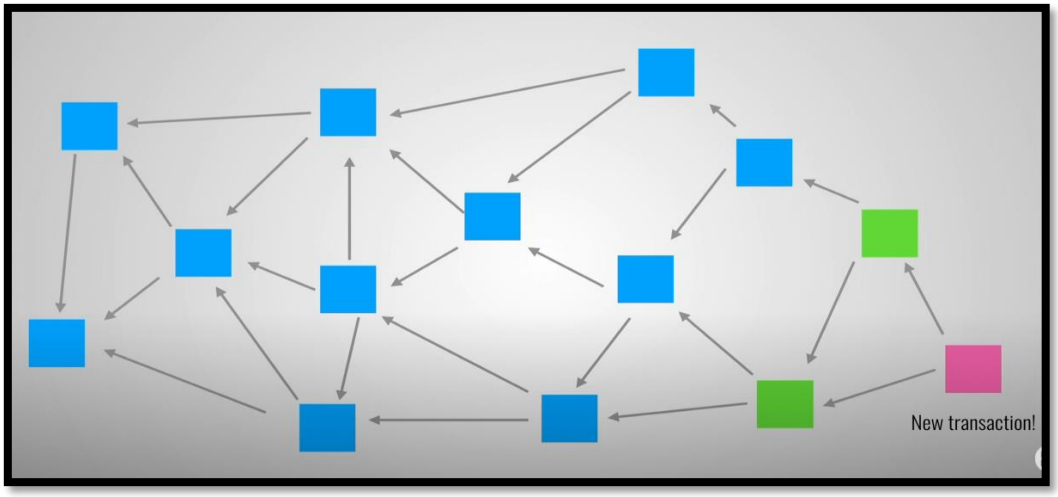

Figure 12: New Transaction

Each square represents a single transaction and is also called a site. Each site contains all the details about the transaction, so it centers the receiver and the number of coins transferred. It also connects at least two other transactions. These are called edges, and they validate the transactions. For example, looking at image 12, a bigger tangle, we find a few transactions with two or more incoming edges. This means that these transactions are unconfirmed, and they are also known as the tips of the tangle. To add a transaction to that tangle, we must attach a new transaction to one of the tips of the tangle. An algorithm selects two of them at random and makes sure that the transactions don't reflect one another. If one of the tips is a fake transaction, it is ignored, and a new tip is selected. If everything checks out, it attaches our transaction to the two tips this answer transaction to the tangle and verifies two other transactions. The new transaction now becomes a new tip of that angle. This technique makes a DAG tangle. It is incredibly scalable for every transaction that is added to the tangle. Two others are being confirmed. This means that the network doesn't slow down when there are a lot of transactions. In fact, it speeds up. Now that's all great, but how can we know we can trust the transaction?

In traditional blockchains, people often use the number of confirmations to check whether a block should be trusted. While iota has a similar technique, each site has a weight. The weight number signifies the amount of work that node has done to make this transaction. In other words, a higher number means that the nodes spent more time doing the proof of work for that transaction. Each transaction also has a cumulative weight. This is a sum of its own weight plus the sum of the weights of all transactions that approve this transaction. [31] [30]

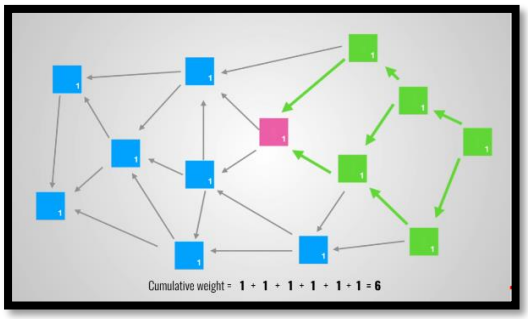

Figure 13: Working of tangle

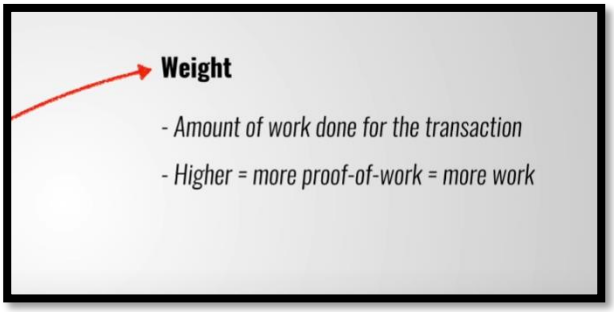

Figure 14: Weight

It seems quite complicated, but it really isn't. Here is an example of a tangle where every transaction has a weight of 1 put the weight of an individual transaction in the bottom right of each square now let's check how trustworthy this big transaction is by calculating its cumulative weight to do that we sum up the weight of the two transactions that have approved it, but those transactions were approved by other transactions as well so we keep summing up all of these waits until we get to the end of a tangle, in this case, the cumulative weight of the site is 6. Transactions with high cumulative weight are usually older and have more direct or indirect verifications, so we can trust those transactions more than others.

Fees

IOTA doesn't have explicit transaction fees. The act of generating a transaction can be considered a fee, but the difference is important. The main focus of IOTA is to be a micropayments system, so eliminating transaction fees is essential. IOTA has fundamentally reengineered distributed ledger technology, enabling secure exchange of both value *and* data, without any fees.

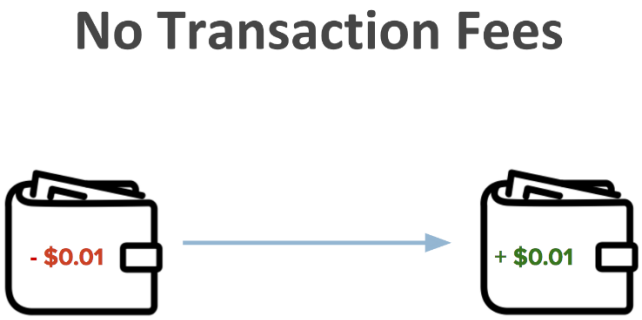

Figure 15: Fees concept [69]

Transaction

Iota's transaction process is likewise unique. Because there is no such thing as always-on connectivity, you must be able to conduct transactions and secure data even while you are offline. The Tangle's appeal is that it allows you to branch out and back into the network with ease. IOTA allows a group of devices to split off and yet conduct transactions in an offline situation by using several communication protocols.

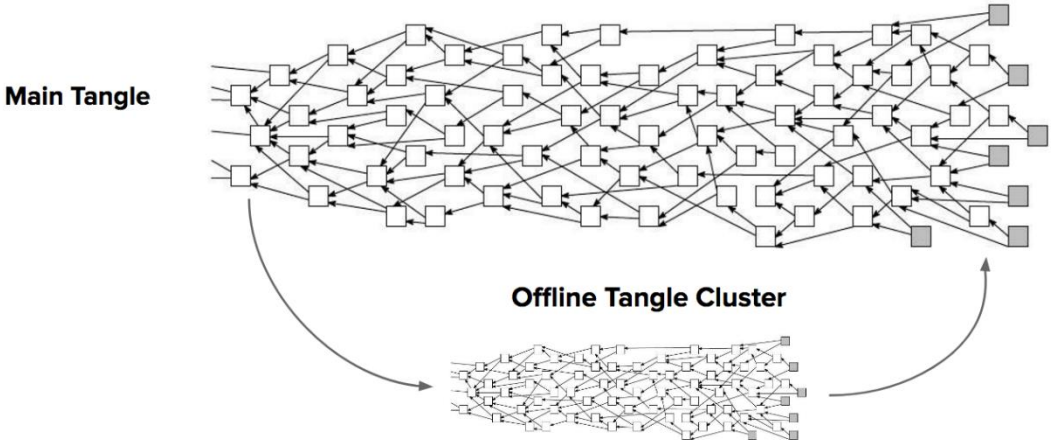

Figure 16: Transaction [69]

Scalability

In theory, OTA should scale as it grows. Transactions can be processed in parallel, and since each transaction confirms two previous transactions, the confirmation time should decrease as more users join the network. Because IOTA does not have blocks, it should not experience any volatility. Therefore, the more transactions are made, the more secure and the more efficient the Tangle gets.

The major challenge of the blockchain trilemma is scalability, which IOTA overcomes, hence IOTA is not a victim of the blockchain trilemma. [60]

Figure 17: Scalability

Decentralised

The number of parties controlling transaction validation is frequently used as a metric of decentralization, hence IOTA at scale may be significantly more decentralized than most blockchains, whose block generation tends to centralize with economies of scale. Despite the fact that it does not use a blockchain, Tangle's distributed ledger is nonetheless a decentralized platform. This means that no centralized authority has complete control over the network or transactions. [60]

Low Resource Hungry

As Tangle is not a conventional blockchain requiring Proof of Work, there is no need for powerful computing equipment, making processing affordable and green [60]

Quantum-Resistance

Another aspect of IOTA is its future-proof inclusion of quantum-resistant hash-based signatures rather than elliptic curve cryptography. It employs Winternitz [62](*One-Time Signature Scheme type of security protocol*) signatures in particular. It is worth noting that this is not specific to IOTA. The Ethereum and other crypto communities are working to incorporate quantum-proof encryption into their protocols.[61]

Coordinator and Coordicide

The Coordicide project, as mentioned in the Iota paper [41] focuses on the removal of the coordinator through the introduction of many network components. Despite the addition of these new components, the Tangle's core design elements remain unchanged. The main objective of IOTA Foundation is to maintain IOTA order is scalable secure and truly decentralized. Achieving this requires eliminating coordinator the mechanism currently used to help reach consensus in the

network. Although the coordinator was crucial to getting iota where it is today, it poses a single point of failure in the network and therefore must be removed. Solution the iota foundation has proposed is called cohort aside. It is a six-part modular solution this is desirable because if one becomes obsolete it can easily be upgraded or replaced of the six modules.

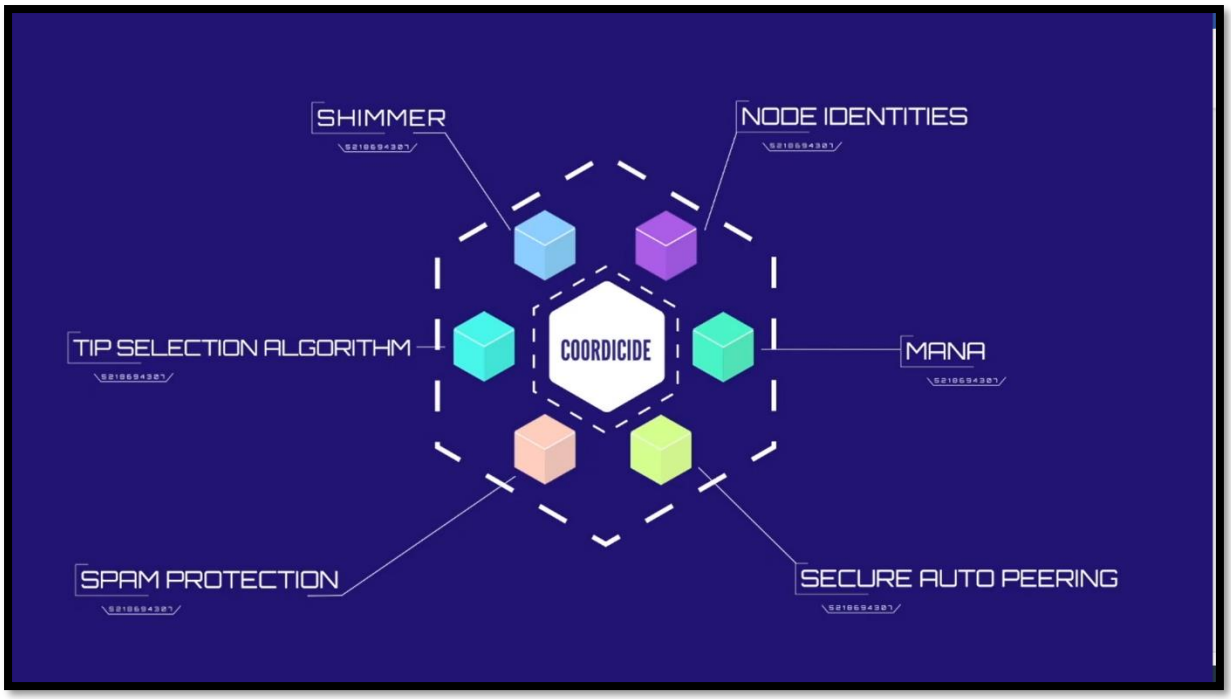

Figure 18: Coordicide

Shimmer

The most important is shimmer, a new voting scheme in iotas consensus layer shimmer is named after an extraordinary behavior exhibited in nature where swarming insects synchronize their movements to defend themselves. Without any centralized authority they decide when to change their state entirely by observing the behavior of their peers. Shimmer works in the same way just with notes instead. Notes query other notes about their current opinion of the Ledger and adjust their opinion based on the proportion of other responses they have observed. Nodes will use a voting mechanism known as fast probabilistic consensus a quick and very accurate technique to see if the nodes all agree on the same state of the Ledger. It's through this ongoing process that consensus forms organically as can emergent property of the network.

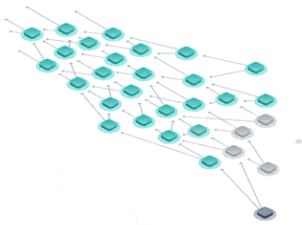

Figure 19: working of Shimmer [44]

Mana

The other noteworthy module is node entities and the concept of mana[43] In a network without the coordinator of voting system like shimmer is not valid if nodes cannot be identified. Every node therefore generates the unique identifier that it will use to sign transactions or cast votes ensuring authenticity. however, relying on node Identities alone makes distributed systems vulnerable to something called Sybil attacks or bad actors try to control a peer-to-peer network by forging multiple fake identities. Other cryptocurrencies mitigate this by harnessing proof of work or proof of stake however because iota uses neither developer proposed a reputation system called mana. [43]

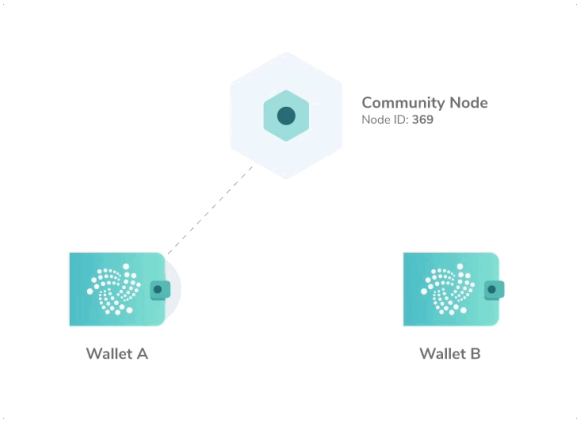

Figure 20: Working of Mana [45]

Mana relies on the notion that reputation is difficult to gain but easy to lose. Nodes gain mana by propagating valid transactions in assisting the network but will lose mana very quickly if it purposefully disagrees with the network. The more mana a note has more trusted it is and the more trusted and node is the more transactions it is allowed to facilitate. Although shimmer node entities and mana are key concepts of court aside. Implementation of iota will be the first cryptocurrency to solve scalability trilemma, scalable secure and decentralized all at once when coordinator is gone. [45]

Use Cases of IOTA

IOTA promises to form the backbone of the Internet of Things' financial system. It also includes capabilities such as secure texting and a data marketplace. These characteristics are all part of IOTA's vision of the future machine economy, in which millions of devices exchange data and payments in real time. This could involve anything from an electric car paying for a charging station to weather sensors throughout the world selling their data to academics working on predicting weather trends [60]. IOTA is poised to play a central role in the next industrial revolution, enabling economic relationships between machines and bridging the human and machine economies.

Let's look at some real-world applications of IOTA.

Mobility

According to ABI (Automotive Industry Research) Research, 8 million consumer automobiles with self-driving capability will be available in 2025. Car data can be safely sent to other automobiles or equipment via the Tangle. Cars are safer/more dependable as a result of real-time IOTA software updates, which track car usage and ownership, enabling fraud prevention, pay-per-use, and usage-based insurances.[63]

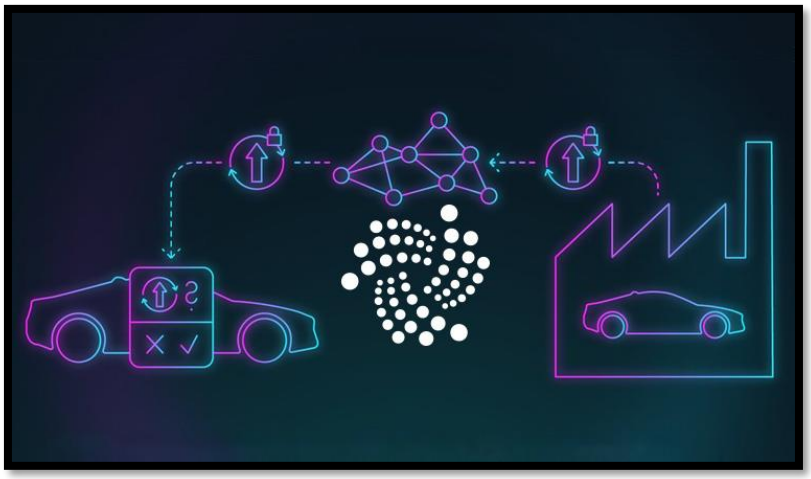

Figure 21: IOTA Mobility [63]

Supply Chain and Global Trade

Approximately 10% of supply chain goods are fraudulent. The supply chain lacks traceability, transparency, and confidence, which the iota supply chain program may address. [64]

The following are the strategic priorities of the IOTA project pilot [64]: Keep a detailed record of everything. Trade facilitation, as well as document flow and transparency.

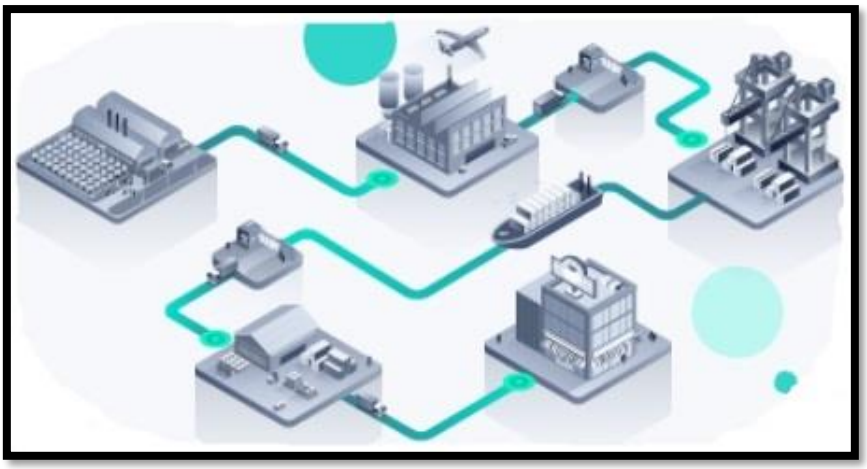

Figure 22: IOTA Supply chain [64]

Ehealth

Giving people the ability to share and developing a new healthcare model, IOTA protects patient data while decentralizing access.

- Research Data Integrity: The IOTA ledger can be used to validate research findings.
- Remote Patient Monitoring: Using healthcare interoperability standards, the IOTA (MAM) protocol protects data streams from remote sensors.
- Pharmaceutical Trials: By logging every step and test result onto the Tangle, we can ensure an immutable record and process of drug trials.
- Health Data Exchange: The MAM protocol[65] (Masked Authenticated Messaging) enables granular and secure data sharing between healthcare professionals, citizens, and caregivers.

Figure 23: IOTA Ehealth [66]

Energy

The IOTA Tangle is a scalable and zero-fee secure communication and transaction protocol with disruptive potential in the energy business. Decentralized peer-to-peer energy trade and autonomous flexibility marketplaces have the potential to form self-sufficient positive energy communities. IOTA offers Plug & Charge and micro-payment-based Seamless EV Smart Charging. Sustainable energy traceability and the provenance of REC tradeable certificates aid in remote control of energy assets and demand response systems for grid stability / peak shaving. [67]

Figure 24: IOTA Smart Energy System [67]

Challenges to IOTA

As we all know, there are always two sides to every coin, and nothing is flawless. Similarly, iota is confronted with a slew of obstacles; here are a few of them.

The Coordinator (Coo): Coo is a highly centralized node that performs a transaction every minute. The Coo network is not yet large enough to prevent attacks; this will take time. Another significant concern with the Coo is that the IOTA team has not provided specific instructions on when the Coo would be shut down. They haven't even offered a scale for how big the network needs to get before it becomes self-sustaining.

Hardware Requirements: Certain hardware upgrades will be required for IoT devices participating in the IOTA network for IOTA to attain its full potential, and this is still in the works. It can have an immediate or indirect impact on power, cost, and compatibility.

Network: IOTA is also concerned with network usability. Multicoin Capital purchased[68] IOTA to test its functionality; however, due to network difficulties, they were unable to withdraw their IOTA from the exchange.

Applications and Choices

The popularity of blockchain technology has skyrocketed in recent years. Many of the difficulties arising because of our increasingly connected society can be addressed by distributed ledger technology and real-world commercial concerns. Blockchains are being applied to a wide range of fields, from financial remittance to supply chain logistics to secure user identity verification. For these reasons, enterprises all over the world are developing their decentralized applications.

There are several questions to consider when developing a blockchain application. People frequently ask the wrong questions, resulting in a less-than-optimal response. Compounding the problem, the ecosystem evolves every minute of every day, making it practically hard for a new developer to master the ins and outs of the present environment while still keeping up with the latest research[56].

I've come up with basic points to help you decide which DLT technology to use for your desired tasks. It may not supply precise answers, but it will provide a clear picture of the fundamental ones.

- Privacy requirement for your application[58].
- Grow and scale of your application
- Digital asset and Strategy
- Accessibility requirements for your application

Privacy requirement for your application

Blockchains come in a variety of flavours. Some are centralized, which means that a single authority controls the network and the information that regular users have access to. Others are decentralized, which means that work and data are distributed over the entire network. There are even hybrid methods that connect a centralized sub chain to a decentralized leading network.[58]

Suppose your application requires any amount of private information to be shared between users, such as real-world names, addresses, business papers, and so on. In that case[56], you should generally avoid a completely decentralized approach, as any data will be permanently available to the public. If, on the other hand, your application promotes corporate transparency and trust lessness, you will want to keep the necessary data on a public chain so that it can be and verifiably retrieved.

Figure25: Privacy [48]

Keep in mind that not all your application's data must be stored on a blockchain. You can exchange information peer-to-peer without ever using a blockchain. If it is not essential or desirable to permanently preserve or publicly validate your data, it is nearly always preferable to keep it off-chain.

Your users may want to demonstrate that they have the correct private information while not disclosing the actual data. To demonstrate the existence of data without revealing it, a cryptographic hash can be used to provide a unique tag for that data. Cryptographic hashes are one-way streets; you can easily use the data to recreate a hash, but you cannot use a hash to recreate the data. Anyone else with that data can use the same algorithm to obtain the same hash and comparing hashes can tell you if you have the same information. Placing hashtags on the blockchain reliably and cost-effectively informs the world that you have a specific set of data without revealing what the data is.[58]

The concept of anonymity is another facet of privacy. There should be no method of determining which users performed which actions in a genuinely anonymous system.

Contrary to widespread assumption, most blockchains are pseudonymous rather than anonymous. That is, while it may be difficult to directly associate a user with a real-world identity from within the network, it is possible to do so utilizing information connected from external services.

In the end, keeping completely anonymous is dependent on the users' diligence rather than the system's essential design.

Grow and scale of your application

Blockchains are databases that can hold any information from a traditional application. The fact that they are spread, on the other hand, significantly alters their ability to scale.

It gets progressively harder to retrieve essential information from all accessible nodes as distributed systems expand in size. It takes time to find and route information between nodes, which we term latency. It also necessitates effort, which we refer to as computational overhead. Much of this routing must be done in the correct order, so that any network has a minimum delay. In general, increasing the number of nodes in your blockchain network will cause it to slow down.

Figure 26: Growth and scale [49]

There are distributed ledger technologies (DLTs) that aren't blockchains out there. As their networks grow, several of these other DLTs continue to run at the same, or even faster, speeds. These are typically built on directed acyclic graphs (DAGs) [59], which can be viewed as a collection of interdependent, interlinked blockchains.

If your application does not require a lot of complicated queries or fine-grained permissions, a DAG may be a suitable fit. And IOTA is one example for it.

If you want to correctly build and scale your system, you must consider things such as

- The DLT selected
- The algorithm for reaching agreement
- The separation between nodes
- The users' geographical distribution
- The transaction's intricacy
- The internet access speed and computers involved
- What is the distance between your nodes and clients?
- How complicated are your questions? Costs, latency, and computing overhead grow as searches become more complicated.

It's realistic to anticipate that most applications will run far faster in the industrialized world than in emerging ones. When we try to grow little systems, they don't always function. To build a durable,

long-lasting application architecture, problems about the application's performance and size must be addressed early on.

Digital asset and Strategy

This is where we start talking about token and cryptocurrencies, two concepts that naturally go hand in hand with blockchain technology, although perhaps not in the ways you think. People in the sector frequently mix up the terms "blockchains" and "cryptocurrencies."

Cryptocurrencies are protocols that run on top of complicated distributed databases, allowing us to create finite supply in a digital realm; in other words, they cannot be copied and pasted and hence preserve value.

Most cryptocurrencies have historically been developed on top of blockchains or other distributed ledger systems, such as DAGs. For the casual user, these definitions become especially hazy because some blockchains are dedicated solely to the maintenance of a cryptocurrency, whereas cryptocurrencies like Ether (the transactional token that facilitates operations on the Ethereum network) can serve as both a store of value and a type of "cryptographic fuel" that allows users to purchase computing capacity spread across the Ethereum network. In other words, the value of Ether is both a result of perception, similar to the value of the US dollar or the euro, and a product of its inherent functionality, similar to the value of oil. [56]

Figure27: Data and Oil [57]

Previously, we explored protocols such as proof-of-work and proof-of-stake. These protocols define the rules and reward mechanisms that encourage users to use a trust less distributed network. The responsibility of confirming the trustworthiness of a counterparty in a transaction is abstracted away from use using complicated mathematics in distributed ledgers. In reality, confidence is still placed; it's simply in a technology system rather than a human being. [56]

The implication is that distributed systems must be built to deliver enough value to their users while keeping a relatively fair and unblemished track record, until the risk to the user is worth it.

The communal confidence that no party could outwit the mathematical search for a prime number on a classical computer is so strong with proof-of-work that there is almost no requirement for trust and almost no risk to the miners. [56] Proof-of-stake consensus necessitates users putting money at risk in order to participate. This risked ante discourages miners from interfering with or otherwise undermining the system. As a compensation for their risk, the system pays them a gradual trickle of interest. This is often where all cryptocurrency starts in proof-of-stake systems.

As new consensus procedures are established, all of this is growing more varied and complex.

Monetary policy, as used to manage an economy or a reward system, is determined by the amount of supply and demand for a currency. When we widen the scope of this concept to include any quantitative or context-specific resource, it becomes evident how complicated these systems and their corresponding economic systems have become and will become.[56]

It is incredibly impossible to predict what distributed ledgers will accomplish for economics at this time. However, there are a few questions that business executives can ask themselves right now in order to create the most intuitive and resilient systems possible.

Accessibility requirements for your application

All software exists to help people achieve their goals. Users will need to be able to access your blockchain project at some point. Consider the kind of capabilities that users should have. These could be the types of currencies they exchange, the ease with which smart contracts can be launched, or the levers they use to contribute to the administration of a decentralized system.[56]

If we build a list of accessibility needs for an application, we can include as many as we like, but there are a few criteria we should not overlook, such as user interface, web APIs, data storage, and so on.

Ask Yourself

Before making a final decision on the platform for your application, I would recommend asking the following questions.

Do you intend to run your platform on a private or public chain?

Most private chains, including those constructed on private forks of public or private ecosystems such as Hyperledger, rarely require tokens or bitcoin. If your company is going down this path, you should really assess whether tokens or coins are even essential. [51]

Is there a price for using your platform?

If you use one of the public chains, you'll discover that each transaction costs cryptocurrency or something similar. Pricing models on systems such as Ethereum [52]are mainly static, whereas those on EOSIO(type of crypto currency) are far more dynamic and reliant on the state of the community.[52]

Even if you construct a system with a centralized gateway and microservices, as many clients do, if you're porting to a public chain, your firm will be susceptible to the tolls required to pay for those calculations. These costs should be estimated and considered into future cost and design decisions.

Do you anticipate that your platform will be compatible with other chains?

As the time, monetary, and computational costs of transferring tokens and coins between ecosystems diminish, context-specific utility tokens are likely to depreciate rapidly.

For instance, if an American in Europe could instantly convert his or her dollars into euros at the point of sale at no cost, why would he or she bother converting currencies ahead of time? The value of the euro is determined by the supply of the currency. If there was no reason to keep it because one could always convert it later, the euro's value would fall, and demand would concentrate around the most liquid currencies.[56]You should consider the extent to which you believe conversion costs will be decreased into their economic expectations.

Energy and Power: We already know how much energy is needed and how this affects the cost of running DLT systems. Before introducing innovations, we must assess how environmentally friendly the system is.

Environmental and human Impact: At the end of the day, whatever technologies we develop, we must consider how they will affect the environment and humans. After all, the goal of employing technology is to make human life as simple as possible. IOTA is one of the few initiatives that is actually being used as a solution for real-world problems.

Conclusion

In this study, we explored several aspects of DLT technologies. To be honest, nothing is flawless, and as technology advances, so will its drawbacks. We can like or detest them, but there is no denying that DLT and DAG technology are innovative. The manner in which personal data is held, as well as the manner in which products and services are transacted, is changing. This technology will have an impact on all industries around the world. And we have the option of selecting the technology based on our application's requirements. There is always a trade-off between decentralization, security, performance, energy consumption, and other variables. The major challenge of the blockchain trilemma is scalability, which IOTA overcomes, hence IOTA is not a victim of the blockchain trilemma.

The unique characteristic of feeless transactions on IOTA enables a wide range of use cases that are not available on any other platform. Mobility, Energy, Smart Cities, and Infrastructure are the primary industries in which IOTA is conducting case studies. Despite its primary focus on the Internet of Things and the Machine Economy, IOTA is well suited for human-to-human payments as well. IOTA has a unique offering, particularly in remittances, where we'll be able to transact even a few dollars from one country to another. There is a long road ahead, and as soon as the IOTA team finds a solution to the Coo centralization problem, this technology has the potential to take off.

References

1. https://www.securities.io/what-is-distributed-ledger-technology-dlt/
2. https://medium.com/blockstreethq/before-blockchain-there-was-distributed-ledger-technology-319d0295f011
3. https://blocktelegraph.io/blockchain-before-bitcoin-history/
4. https://link.springer.com/article/10.1007/BF00196791
5. https://toshitimes.com/the-longest-running-blockchain-has-existed-on-nyt-pages-since-1995/
6. https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp
7. https://c2sms.com/dlt-platform-error-codes/
8. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269731
9. https://blogs.lse.ac.uk/businessreview/2018/02/22/blockchain-an-overview/
10. https://cryptomaniaks.com/guides/blockchain-for-dummies-ultimate-blockchain-101-guide
11. https://usethebitcoin.com/sweden-could-launch-a-cryptocurrency-e-krona-powered-by-iota/
12. https://www.joshpaiva.com/iota-coin-review/
13. https://files.iota.org/papers/20200120_Coordicide_WP.pdf
14. https://arxiv.org/abs/1911.08787
15. https://link.springer.com/chapter/10.1007/978-3-030-70970-9_2 (Funcanalities)
16. https://www.pwc.be/en/news-publications/insights/2017/blockchain-functional-introduction.html
17. Types of blockchains https://flexiple.com/blockchain/blockchain-applications-in-business-public-vs-private/
18. https://outlierventures.io/research/investments-in-blockchains-2019-23-7-billion-raised-by-3738-blockchain-companies-since-2013/?url=133
19. https://builtin.com/blockchain/blockchain-healthcare-applications-companies
20. https://www.csoonline.com/article/3191619/faq-what-is-blockchain-and-how-can-it-help-business.html
21. https://builtin.com/blockchain/blockchain-payments
22. https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf
23. https://www.33rdsquare.com/best-applications-of-bitcoins-blockchain-technology/ Log
24. https://www.euronews.com/next/2021/06/08/what-are-cryptocurrencies-and-how-do-you-use-them-a-beginner-s-guide-to-cryptocurrencies (Crypto currency)
25. https://101blockchains.com/history-of-blockchain-timeline/
26. https://builtin.com/blockchain/blockchain-applications
27. https://wwwmatthes.in.tum.de/pages/j4kcsh9lbjby/Bachelor-s-Thesis-of-Bennet-Breier
28. https://www.iota.org/foundation/research-papers
29. https://wwwmatthes.in.tum.de/file/10gqfgwknnwc3/Sebis-Public-Website/Student-Theses-Guided-Research/Current-Bachelor-s-and-Master-s-Theses/Technical-Analysis-of-the-Tangle-in-the-IOTA-Environment/BA%20-%20Bennet%20Breier.pdf
30. https://satoshiwatch.com/iota-dag-tangle/
31. https://www.coinfi.com/how-to-buy-cryptocurrency/iota-miota
32. https://101blockchains.com/disadvantages-of-blockchain/

33. https://101blockchains.com/pros-and-cons-of-blockchain/
34. https://academy.shrimpy.io/post/what-is-the-blockchain-trilemma
35. https://blog.fingo.pl/blockchain-trilemma/
36. https://iota-einsteiger-guide.de/2-postkoordinator.html
37. https://applicature.com/blog/blockchain-technology/blockchain-scalability
38. https://in.pinterest.com/pin/453596993721595205/
39. https://cdn.builtin.com/sites/www.builtin.com/files/styles/ckeditor_optimize/public/inline-images/national/blockchain-applications-money-transfer.png?__cf_chl_captcha_tk__=pmd_uLrzgJqjFYtIQHYBr2L4aG1trKaKpNWCJ5wUWjB8xaM-1633888265-0-gqNtZGzNA7ujcnBszQg9
40. https://101blockchains.com/disadvantages-of-blockchain/
41. https://blog.fingo.pl/blockchain-trilemma/
42. https://files.iota.org/papers/20200120_Coordicide_WP.pdf
43. https://blog.iota.org/explaining-mana-in-iota-6f636690b916/
44. https://iota-einsteiger-guide.de/4-5-1-shimmer.html
45. https://iota-einsteiger-guide.de/4-1-node-identitaet-und-mana.html
46. https://blog.iota.org/explaining-mana-in-iota-6f636690b916/
47. https://iota-einsteiger-guide.de/kritik.html (IMP)
48. https://www.vhv.rs/viewpic/hwwxiio_data-security-logo-design-hd-png-download/#
49. https://www.pngwing.com/en/free-png-vcabk/download
50. https://yourstory.com/mystory/10-tips-to-choose-the-best-blockchain-development-/amp
51. https://medium.com/web3labs/how-to-choose-the-right-blockchain-technology-724b3b7ef6ae
52. https://appinventiv.com/blog/choose-best-blockchain-development-platform/
53. https://searchstorage.techtarget.com/definition/blockchain-storage
54. https://www.researchgate.net/publication/304757375_Using_Block_Chain_for_Peer-to-Peer_Proof-of-Location
55. https://frankly.studio/blockchain-uxui-design-3-reasons-why-they-need-each-other-more-than-ever/
56. https://objectcomputing.com/expertise/blockchain/4-questions-selecting-blockchain-platform
57. https://iota-einsteiger-guide.de/marktplaetze.html
58. https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf
59. https://hazelcast.com/glossary/directed-acyclic-graph/
60. https://coinjournal.net/iota/
61. IOTA ($MIOTA) Analysis ,Myles Snider, Kyle Samani, and Tushar Jain, January 23, 2018
62. 191.pdf (iacr.org)
63. https://iota-news.com/iota-in-ota-an-exploration-of-iota-use-cases-in-the-new-mobility/
64. https://iota-einsteiger-guide.de/supply-chain.html
65. https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e/
66. https://blog.iota.org/untangled-episode-2-exploring-ehealth-8f5b3112030e/
67. https://files.iota.org/comms/IOTA_Use_Cases.pdf
68. IOTA Network Struggles Due to Lack of Full Nodes » The Merkle News
69. https://blog.iota.org/a-primer-on-iota-with-presentation-e0a6eb2cc621/