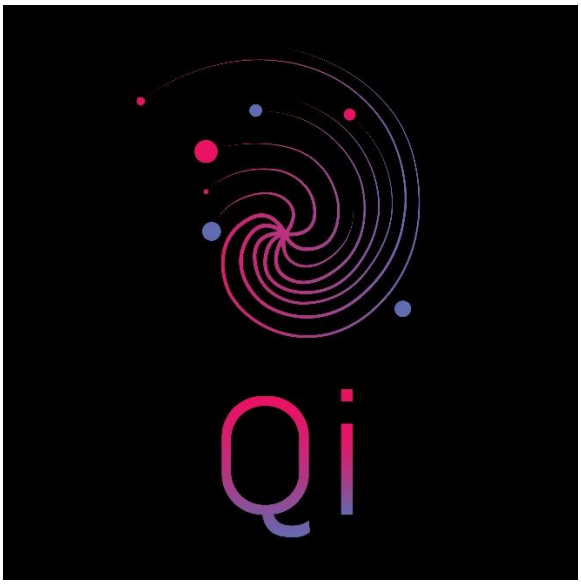
Qi Blockchain - White Paper

Sensei Miyagi, Founder and CEO



Executive summary

Qi pronounced Chi is usually translated as “vital life force,” but Qi goes beyond that simple translation. According to Classical Chinese Philosophy, Qi is the force that makes up and binds together all things in the universe. It is paradoxically, both everything and nothing. Qi is a decentralised POW (Proof of work) blockchain with an application native currency which is leveraging functionality of creating fungible and non-fungible *assets* using Remote Procedure call (RPC) methods. Qi is able to handle 300 times more transactions per second than Bitcoin and 10 times more than SWIFT. Qi is scalable hence other companies are already using it as primary payment method of several fully developed I-store apps with real use cases. There is a limited amount of only 150,000,000 Qi coins and transaction fees remain almost zero ensuring a futuristic and feasible way to transact. These coins will be mined over almost a hundred years.

Qi enables the deployment of smart contracts and decentralized applications (dApps) to be built and run without any downtime, fraud, control, or interference from a third party. Decentralized applications—also known as "dApps" or "dapps"—are digital applications that run on a blockchain network of computers instead of relying on a single computer. Benefits of dApps include the safeguarding of user privacy, the lack of censorship, and the flexibility of development. The use of blockchain enables a dApp to process data through distributed networks and to execute transactions. Qi can be used for a wide variety of innovative applications in finance, web browsing, gaming, advertising, de-fi, identity management, web 3.0, metaverse and supply chain management all over the world.

Background

Bitcoin is now known as the cheapest, fastest and most reliable way to transfer economic value to the Internet in the form of a peer to peer. Despite the brief fork between the incompatible versions in March 2013, the bitcoin network has been operating continuously and smoothly for over 5 years. Despite the loss and theft of private bitcoins, the network itself has never been successfully attacked or blocked.

Despite the many technological advantages of bitcoin, it is far from achieving general consumer acceptance or business acceptance. Given the current trend in transaction volumes, the slow growth in bitcoin usage is showing no signs of change in the foreseeable future. This is happening without the availability of many easy to use bitcoin wallets and the fact that bitcoin can now be used online for many common businesses like Microsoft, Dell and Overstock.

There are many reasons for the small acquisition of bitcoin, including:

(a) Final satisfaction with existing payment systems

(b) Difficulty purchasing bitcoins

(c) Volatility of bitcoin value related to government disbursement

(d) View that bitcoin is not secure,

(e) Inquiring about the legal status of bitcoin

(f) The unpredictable and unforgivable nature of bitcoin operations

In addition to the acquisition of the end user, many have suggested that bitcoin could help improve internal processes in the traditional financial sector, by reducing costs, reducing payment times and eliminating mediators. One fast technology is possible to use bitcoin as a currency and a channel for instant payment by banks. However, the volatility of the bitcoin value associated with government spending makes this ineffective in practice. The most promising direction is to use bitcoin infrastructure to make goods other than bitcoin itself.

Blockchains and tokenization

At the heart of bitcoin lies the blockchain, a world-class ledger that keeps a complete history of all bitcoin transactions. The blockchain is verified and stored by every node in the bitcoin network, of which there are approximately 6,000 in June 2015. The bitcoin protocol ensures that, preventing temporary interference, every network has the same blockchain version, without the need for it this agreement must be determined by the central authority.

New transactions can be created by any node and distributed across the network in the form of a peer to peer. Any node can take a set of these pending items and create ("mine") a new block containing and a

link to the previous block. The new block "confirms" the transaction and redistributes it across the network. To prevent fewer mining controls, bitcoin uses “proof of work” to make it more complex and expensive to build a new block.

As well as bitcoin transactions, the blockchain can be used to store any digital data. While some view applications such as "blockchain blocking", a low-level bitcoin environment means it will not be successfully stopped. This has led developers of Bitcoin Core, the official bitcoin client, to launch an official way to add unmistakable metadata to transactions in early 2014. This method is used by services such as Proof of Existence and BlockSign to inform the existence of a document by embedding a digital signature of that document within a transaction. Some tools like php OP_RETURN enable large pieces of data to be stored and accessed on the blockchain, making it a standalone private data store.

The transaction metadata is used by several protocols, such as CoinSpark, Counterparty, Omni Layer and Open Assets, to support third-party assets in the bitcoin blockchain. First, the export business creates a new set of tokens representing assets, by sending transactions with specific "asset genesis" metadata. As part of this process, the supplier may enter into a contractual obligation to allow these tokens to be exchanged for real equal assets at any time. Identity of tokens is freely transferred between administrators using other transaction metadata through "transfer" metadata, without the need for the issuer's permission or another authority. In fact, the token serves as a digital carrier liability, with the ownership of a bond determined by the data embedded in the bitcoin blockchain. In the financial world, a token issued by an institution with a strong credit rating can be viewed by other institutions as being almost identical to an asset.

Bitcoin’s shortcomings

Aside from the promise of token-making rules, there are a number of reasons why the bitcoin blockchain is not yet ready for institutional financial transactions. Problems can be divided into two groups, the first of which is related to growth and cost:

- ***Limited capacity***

  - ✔ The bitcoin blockchain currently supports around 300,000 transactions per day, as determined by its maximum 1MB block size. This volume should be shared among all network users and is obviously not sufficient for most financial systems. For example, the Visa network currently handles 150 million transactions per day at USA. While the larger size of blocks is likely to grow in the future, there is an ongoing debate over how this can happen faster without expelling ordinary users and increasing the frequency of forks in network sync. In any case, facility users cannot control the speed of this change, which will ultimately be determined by the acceptance of the miners.

- ***Transaction costs***

  - ✔ The standard fee per bitcoin transaction is currently BTC 0.0001 (2.5 cents at $250/bitcoin) and is collected by the miner of the block in which that transaction is confirmed. While this fee is optional, transactions with lower fees can encounter

significant delays in confirmation. This sum is already a nontrivial tax on transactions of small monetary value. Furthermore, when the demand for bitcoin transactions outgrows the supply of available block space (see previous point), this fee may increase substantially, as transactions are forced to bid with each other to compete for inclusion in a block.

- ***Irrelevant data***

  ✔ Institutions that use the bitcoin network need to process and store a lot of information that they do not like. When a new bitcoin node is introduced, it starts by downloading, verifying and maintaining the entire history of all bitcoin transactions. Going forward, it should also verify all new transactions and blocks made, even though most are not related to the user of that node.

- ***Mining risks***

  ✔ Bitcoin proof of mining performance is an open global race to solve the complex mathematical problem needed to build a new block. While this process is well suited to the general network of objective distribution, it poses a number of risks to institutional users:

  - ❖ Unexpected delays in transaction verification, in the created times defined by Poisson distribution 10 minutes
  - ❖ Risks of other miners who refuse to verify
  - ❖ 51% attack power, when a group of miners controlling more than half of the network computing power come together to rewrite an important period of the latest blockchain history. While such an attack is unlikely to occur, it is in conflict with the need for a non-reversible transaction agency once it has been completed.

- ***Lack of privacy***

  ✔ Design By design, all bitcoin transactions are visible on all network nodes and therefore, worldwide by blockchain testers like blockchain.info. However, the existence and level of transactions cannot be hidden, and participants risk that their identity will be disclosed at some point in the future, when their entire transaction history may be reversed inferred.

- ***Openness***

  ✔ Anyone with an Internet connection can connect to a bitcoin network and work with other participants. This makes bitcoin an attractive channel for illegal transactions, as Know Your Customer (KYC) checks cannot be enforced at network level. While regulated institutions may be able to ensure that (or their clients) only work with

well-known partners, this requires that everything be done individually, creating a significant burden on the structure and performance of the work.

Other blockchains

To begin to answer this question, we can say that bitcoin is very far from the active social blockchain. Hundreds of other blockchains are built, each with its own cryptocurrency, network of nodes and contract rules. Other examples include Litecoin, BitShares, Nxt, Dogecoin and Namecoin. Many but not all of these blockchains work on software available from the bitcoin source, with only minor modifications to mining algorithms or other parameters.

Despite this increase in innovation (and, in many cases, pump and dump schemes), bitcoin retains its status as a prominent cryptocurrency. The obvious reason is the large number of individuals and businesses that already own or receive bitcoin currency. However, there is also an important network effect in relation to mining. Bitcoin is a cryptocurrency supported by deep mining power, making it very safe from 51% attacks. This gives it a very high visual value and therefore a very large market capitalization. As a result, bitcoin offers a huge financial reward to miners and this leads to attracting and retaining more miners than any other currency, increasing its value continuously. This beautiful loop will be harder than any other blockchain to beat unless it provides important new functionality.

The bitcoin blockchain uses a per output transaction model, in which all transactions have a set of inputs and a set of results. Each input "uses" a single issue for a previous transaction, with a blockchain that ensures that this release cannot be used elsewhere. The full history of the transaction formed a chain connected to several roads, culminating in a "coinbase" transaction in which miners were given new currency units. All transaction revenue flows through that transaction, which is distributed across all of its outcomes according to the values listed internally. As a result, most standard payments require two outputs - one with the intended recipient value, and the other containing the “change” that returns to the sender for use in the next item. The transaction only works if there is enough bitcoin in its deposit to cover the written value of its issue, with the difference that makes the miner’s money.

Some blockchains, such as Nxt and Ethereum, use a simple per address transaction model, where transactions have no inputs and individual outputs. Instead, each transaction transfers funds from one address to another, without showing any previous transaction in which those transactions are to be taken. The transaction only works if the shipping account has enough balance to make the payment specified. This model has both advantages and disadvantages compared to the bitcoin’s per output model

All of these blockchains are open, allowing anyone on the Internet to connect, operate or personalize. However this is not a requirement. First, one would think that a small group of businesses come together to build their own blockchain similar to bitcoin, and access is limited to specific IP addresses.

This will give them more than a million times more power in mining than other members using regular computer processors. As a miner of all blocks, they can unanimously agree on any guaranteed transaction or rewrite blockchain history at any time. In addition, they can avoid detection while doing so, by using a different public address to collect mining rewards for each block.

As a miner of all blocks, they can unanimously agree on any guaranteed transaction or rewrite

blockchain history at any time. In addition, they can avoid detection while doing so, by using a different public address to collect mining rewards for each block. Other factors to consider is storage and the main reason why EOS won`t ever be feasible as it uses in excess of 2TB of data storage at a price.

Transition from POW to POS

The proof of work (POW) consensus algorithm is the most commonly used in the blockchain technology. Both Bitcoin and Ether, the 2 well-known cryptocurrencies, use it.

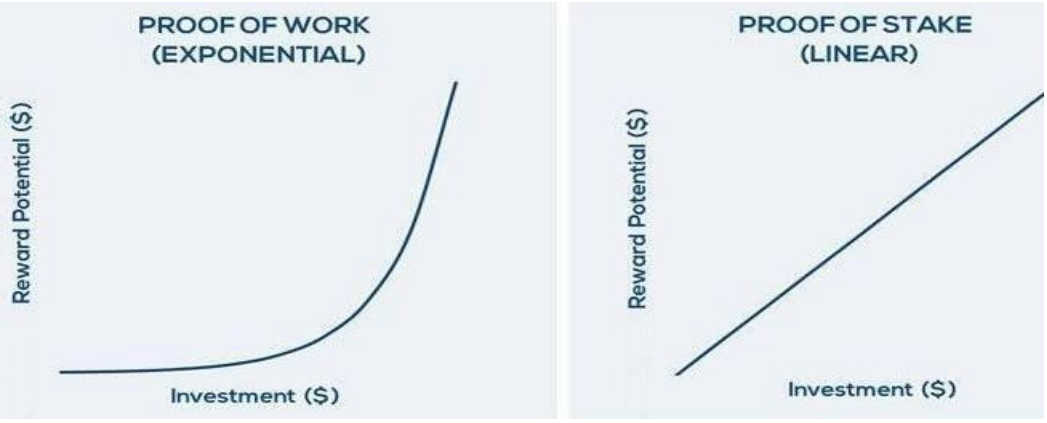
The initial intention of the POW consensus algorithm is to guarantee a stable value of the currency by consuming a large amount of energy, manpower and material resources. As a consensus set of rules within side the early stage of our project, through our POW we focuses extra on making sure the safety of transactions.

Transactions with inside the blockchain are grouped in a reminiscence pool whilst a block is created each 10 minutes. Every transaction wishes verification, and 'miners' do it. Hence POW makes blockchain very secure. However, this excessive protection comes at a heavy cost. POW is well-examined and used in lots of cryptocurrency projects. Every time a transaction is sent, it takes approximately 10 mins for the community to verify it.

"The excessive strength cost, extended pressure at the environment, related unfavorable media coverage, growing centralization of mining operations, and coffee transaction throughput will in all likelihood make it unviable withinside the lengthy run"

In case of PoS algorithm, a hard and fast of nodes determine to stake their personal cryptocurrencies for the transaction validation. There isn't a want for the complete community to be concerned with inside the transaction validation process, which improves scalability

The PoS set of rules affords for a greater scalable blockchain with better transaction throughput, and some have followed it already, for e.g. DASH cryptocurrency. If the deliberate implementation of PoS in a protocol as well-known as Ethereum is going well, then the crypto network will possibly be moderately confident approximately the cap potential of the PoS set of rules to hold the community safe.



QI Blockchain will permits customers to ship and get hold of finances in only multiple seconds. Our Proof of Stake version makes use of an exceptional technique to verify transactions and

attain consensus. While Proof of Work rewards its miner for fixing complicated equations, In Proof of Stake, the person who creates the following block is primarily based totally on how much they have 'staked

Introducing QI

QI is a public blockchain where only our organization will have authority over pushing transactional data over the network. Therefore, it means that it is open for the public to join and use token transactions. It aims to overcome a major obstacle to the use of blockchain technology in the institutional financial sector, by providing the privacy and control required in the easy to use package. Like the Bitcoin Core software from which it is based, we support Windows, Linux and Mac servers and provides a simple API. We later discussed many other features on the road map.

Mining in QI

In private blockchain, members' identities are known. It is determined who is allowed to participate in the network, perform the process of agreeing to keep the shared ledger. There are usually no traditional token or incentives to encourage members to join and mine. The justice required for the distribution of resources does not exist at all

Because members are anonymous and networks are often not exposed to the hostile online community the demands on the cost of consistency are weak. The blockchain does not need to be protected by huge energy costs. For consistent integrity through hash series and adjectives managed by different groups is usually sufficient.

As a private blockchain, there will not be too many miners in the network, so hashing power will be low. Because of this, we will mine with a simple CPU and very small resources.

QI uses this system using a parameter called mining diversity, which restricts mining diversity ≤ 1. The legitimacy of the block is guaranteed as follows

- Apply all the permissions changes defined by transactions in the block in order.
- Calculate the number of permitted miners defined after applying those changes.
- Repeat the miners with a variety of mines, collecting to find space.
- If a miner of this block has excavated one of the previous space blocks 1, that block is invalid. This enforces a round robin schedule, in which the permitted miners must create blocks in rotation in order to generate a valid blockchain.

The mining diversity parameter describes the robustness of the system, e.g. The number of permitted miners who will need to assemble to damage the network. The value of 1 ensures that every permitted miner is included in the exchange, and 0 does not represent the limit at all. In general, high prices are safe, but a price close to 1 could make the blockchain stronger if some miners are inactive. We suggest a value of 0.75 as a positive compromise. To save resources, nodes will not attempt to mine through a series where they have already dug one of the previous spacing1 blocks.

As well as preventing abuse, the diversity limit helps in a situation where the network temporarily separates uninterrupted islands, possibly due to communication failures. This evil will lead to the deviation of the chain, as each island can see transactions with the other blocks. Once the network is connected, a long-chain fork will be accepted as a global consensus. The diversity boundary ensures that the long blockchain will be an island containing the majority of permitted miners, because another island series will soon dry up.

If mining is banned by certain organizations, one can question the benefits of a blockchain in a central database that accepts incoming transactions, resolves disputes, and answers questions about the state of the database. The answer is threefold

- Each participant retains full control over its assets via their private key. Even miners cannot create transactions that spend another party's funds.
- Database management is still distributed across multiple companies, so that no person or small group can collectively decide which transactions are valid or will be guaranteed
- High durability, because the disappearance or malfunction of one server will not affect further processing of transactions across the network

QI allows the user to set all blockchain parameters in a configuration file, including:

- Target block time, e.g. 1 minute.
- Valid permit types, e.g. anyone can connect, only others can send / receive.
- Mining rewards, e.g. 50 traditional currency units per block, separating half of 210,000 blocks.
- IP ports for peer to peer and JSONRPC API connections, e.g. 8571, 8570.
- Authorized transaction types, e.g. written, written, written.
- Large block size, e.g. 1 megabyte.
- Large metadata for each transaction (OP_RETURN), e.g. 4096 bytes

Many blockchains can run on a single server, each with its own name and configuration file. To create a new blockchain, two simple user steps are required. First, the user chooses a chain name, in which QI creates a configuration file that contains the default settings. This file can be modified by the user, although the default will be appropriate for standard usage cases. Second, the user introduces a blockchain, in which the genesis block is dug granting the creator of all user rights. At this point, we also embed the details of the genesis block and the hash of all blockchain parameters in the configuration file, to prevent subsequent risk changes

When launched, the blockchain uses only one node. To add a new node, QI works from another computer with three parameters: (a) the destination blockchain name, (b) its IP port number, and (c) the local IP address. In order for the user to use this information it has been compiled into a "node address" in the normal way, e.g. chain1@12.34.56.78: 857123. Initially a new node will not be allowed to connect, because the network is private and the node has not yet been given the rights to connect the administrator grants the rights to connect to this address with a simple command that carries out the appropriate transaction. The new node can successfully reconnect and automatically download a configuration file that defines blockchain features. Any incoming link in the same

blockchain only needs a chain name to be specified, with a handshake process between verifying sites that use the same parameters.

The obvious improvements to come are to allow some of the parameters to be changed while the blockchain is running, with special transactions issued by trusted managers. For example, as network usage increases, larger block sizes can be increased to accommodate the expected volume of transactions. Any such changes should consider the computing power of each location in the network

Multicurrency blockchains

Keep in mind that token agreements such as CoinSpark and Counterparty allow third-party assets to be extracted and processed over the bitcoin blockchain, much like traditional bitcoin currencies. These methods can be applied equally to private blockchains

However, in a blockchain that uses confidential protocols, we can improve on these systems by integrating support from third-party assets directly into chain rules.

In bitcoin, all transactions include a code of the amount of bitcoin contained within each result. If the transaction has more code written on its output than the total value entered, it will be deemed invalid by the network and can no longer be distributed or verified in the blockchain. This verification is possible because the entire network node tracks the value of bitcoin in unused transaction results. Because of this, the presence of transactions on the network or blockchain is enough to give users confidence in the accuracy of the embedded bitcoin prices. Also, this enables lightweight wallets ("easy payment verification") to operate securely over the network, without having to store all the blockchain on a user's computer.

The problem with asset classification over bitcoin is that metadata that includes the presence of non-native assets are not subject to this network validation. Let us assume that the ABC bank has issued tokens representing dollars. A cunning user can create a transaction with his or her metadata indicating that it contains $ 100 of the ABC output, even if no ABC dollars are present in the input for that transaction. This transaction will be accepted as valid by the bitcoin network and authenticated in the blockchain, because (a) bitcoin nodes cannot read this metadata, and (b) bitcoin nodes do not follow ABC dollars.

Assets with tokens are therefore second-class citizens in the bitcoin blockchain, compared to traditional chain money. The presence or otherwise of a token item can only be calculated by examining the full history of all transactions affecting that token from its performance. This can be accurately calculated in a "forward" way, examining all new transactions as it enters. However, it still requires a complete network environment, undermining the validity of the token agreements you can use lightweight wallets. QI solves the problem by encrypting the identification and quantity of all assets in each transaction output, using the extension provided in the bitcoin. The transaction guarantee law is expanded to ensure that the total value of all assets in the transaction results is exactly the same as the total value of its input. This equity requirement is stronger than the natural monetary barrier, where the

output may be less than the input, with the difference collected as revenue by the miners.

QI roadmap

Below is a list of additional features that can be added

Blockchain messaging

The private blockchain can provide authenticated and anonymous messages, using the same method as the CoinSpark bitcoin protocol. There are two main uses for messaging. First, it can be used to supplement the important context of a financially blockchain transaction, such as a contract, receipt or invoice. Alternatively, it can be used for pure unwritten communication without related financial transactions. In any case, the details in the blockchain enable the sender and recipient to verify the time and content of the written letter.

Each message has a corresponding hash, which is a long number that puts fingerprints differently from its content. Given any input data with a specific hashing algorithm, it is easy to calculate the corresponding hash. However, in any secure hashing program, it is not possible to generate a piece of data to match a given hash. Safe algorithms are called one-way operations, because they can be calculated on one side.

The message is sent from the developer to the recipient

1. A domain from QI sends message transactions to recipients via metadata containing its IP address and message content.
2. The receiving node detects a transaction and determines this metadata.
3. The receiving node contacts the node that appears with its IP address to receive the message, sign the request to verify the identity of the intended recipient. This interaction occurs through the peer to peer blockchain protocol.
4. The receiving node verifies the legitimacy of the message by checking its hash against the hash included in the actual sale.
5. If the message is valid, the receiving node completes the loop by returning the second transaction to the sender containing the same hash message.

Once the first transaction has been confirmed on the blockchain, the recipient can confirm: (a) who sent the message, because the sender discloses his or her address when signing the transaction, (b) the time the message was sent, , because a hash is part of a signed transaction. However, none of this is sufficient for the sender to confirm that a particular message has been received by the recipient. Indeed, malicious senders can embed even faster than one message while sending a completely different message in step 3 above. We therefore need a second transaction in which the recipient sends a receipt containing the same hash. Once this work is verified, both parties can attest to all the details of the documents that took place.

Like public messaging on CoinSpark, such a system can also be used to spread information freely to all network participants, with a hash message on the blockchain that serves as proof of message content

and publication time. In this case we simply exceed the limit of who can return the message to the original location, and we do not need a second action to verify the message receipt

Decentralized exchange

The per output trading model used in bitcoin enables the performance of tasks where two (or more) groups exchange certain assets securely. A blockchain treats this process as an atom, which means it is successful or completely unsuccessful, so there is no risk that one group will lose its assets without acquiring a corresponding asset from the other side. This is equivalent to the cost of land delivery in the world of traditional finance

As an example, let's consider a simple double trade between $ 15 for Alice and £ 10 for Bob. The exchange is done in a transaction with two inputs and two outputs. The first input comes from Alice and contains $ 15, while the second input comes from Bob and has £ 10 in it. The first output to Alice also contains £ 10, and the second output to Bob also contains $ 15. Assuming the transaction is valid and well signed by both Alice and Bob, it will be distributed and approved on the blockchain

Unfortunately, the process of building such a peer to peer transaction is complicated, with the following steps:

1. Alice and Bob find their mutual willingness to do an exchange with a particular off blockchain process, and they agree on the results of the transaction they will use.
2. Alice's node forms a complete transaction and signs it.
3. Alice transmits a slightly signed transaction to Bob through another off blockchain process, as this incomplete transaction will not be accepted by the network.
4. Bob finds out what is being done and makes sure it is in line with their agreement. If so, his node is signing the transaction again. At the moment the transaction is valid.
5. Bob node transmits fully signed transaction network credentials and credits to the blockchain

This process consists of two steps that take place offline - first, in order for Alice and Bob to find each other and second, to send a slightly signed transaction from Alice to Bob.

The upcoming version will streamline this process by enabling partial transactions that are distributed directly across the network. Such transactions represent an exchange offer, which can be acquired by any party by completing the transaction and transferring it to be included in the blockchain. Fortunately this does not require any significant changes to the bitcoin transaction process and signing process, as bitcoin already has a way for users to make and sign partial transactions, allowing the content of other inputs and outputs changed.

We see how this works by following the example above. First, Alice's QI node creates a transaction where the first input from Alice has $ 15, and the first result goes to Alice containing £ 10. Alice's code signs the original input and output of this partial purchase to give this component a run. This partial transaction will not be accepted on the blockchain, due to the difference between the prices of an asset in its input and output. When Bob's QI node receives this partial purchase, it presents it to him as a possible exchange, and Bob accepts it. As a result Bob's node completes the

transaction by placing a second input on Bob's £ 10, a second output to $ 15 set for Bob, and signing all transaction·

The transaction is now valid, because it contains the total amount of assets in the input and output. Bob's node returns it to the network and can be verified.

In this system Alice needs a way to cancel her post-broadcast presentation. He does this by creating new transactions that take advantage of the effect shown by the inclusion of his offer, which he sends to you. This makes the offer invalid, because it uses the result of a transaction that is no longer available, so it will be discarded by all network nodes. It should be noted that this type of allocated exchange is not suitable for high commercial use (HFT), due to distribution delays arising from the peer to peer network. In addition care must be taken to ensure that one participant is not able to fill the network with unwanted offers. In a private blockchain this can be achieved by limiting the right to make offers to specified user addresses, and limiting the number of outstanding offers made for each address.

Database synchronization

Blockchains are an outstanding technology to ensure that all participants in a low-level network share the same worldview. However it is not well developed in answering queries related to previous work on that network, because it represents that function as a green log of verified tasks. This log is stored in chronological order, collected by block number, with no additional references. There are many useful reports we may want to make, such as listing all address or property functions, which can only be answered by scanning the entire blockchain to search for the same transaction

Deployment scenarios

As a general-purpose platform for private blockchains, it can be used for many use cases. In this section we provide three types of submissions, and suggest the appropriate permits and mining variations that you can use in each case

Centralized currency settlement

Let’s start with a simple case, where a general financial caregiver uses a private blockchain for itself and its customers, instead of a standard database integrated with customer-facing APIs. This use of a blockchain does not change the keeper business model but instead reduces IT costs and stay delays.

In this scenario, the custodian acts as the sole administrator, miner and blockchain issuer, but distributes these functions across the QI node of the intensity and diminishing function. The mineral diversity parameter is set to zero, because all mining is controlled by one trusted business, and there is no problem if only one of these business entities digs all blocks, possibly because of other nodes failing.

After creating the network, the administrator will start by giving its clients permission to connect and perform things on the blockchain. It then creates assets with various currency tokens to be made. These tokens are sent to customers by exchanging the corresponding deposit of money into the trustee's bank account, and represent the right to redeem the money to the trustee at any time. Clients can send money directly to each other using the transaction to deliver the corresponding tokens. Changes to trademark

ownership have been completed ("resolved") if these operations are verified in the blockchain by one of the storage locations.

As well as direct payments, this blockchain can also be used as a transparent peer to peer exchange, where the caregiver is responsible for resolving the exchange transaction. As mentioned earlier, a client can create a signed transaction that reflects the offer of the exchange, perhaps between dollars and euros, and then spreads it across the network. Any other client may accept an exchange by providing missing input and output and transfer the completed transaction.

Apart from the fact that this is an intermediate program, there are a few advantages to using blockchain over standard data. First, the blockchain offers a single unified view of the gaming environment, so clients do not need to keep separate records. As there is no possibility of a disagreement over the nature of the transaction, no reconciliation is required and trade breaks cannot occur. In addition, residence times should be significantly reduced to the point where it is necessary to block the block. Another advantage is that the system is less tolerant, with tight peer-to-peer connections between nodes and many surveillance miners providing demolition

Bond issuance and peer-to-peer trading

Let us consider the second case, in which many financial institutions work together to build a banned network of corporate bonds. While previously these bonds could not be issued by a registrar and traded through OTC (over the counter), the blockchain enables both functions to be executed quickly and transparently.

In this case, there is no basic control in management or mining. Instead, each network participant has mineral and commercial rights, with a small number of "senior" participants holding administrative rights to delegate rights to others. Mining diversity is set at a high value of about 0.9, meaning that consensus can only be disrupted by at least 90% of permitted miners working secretly and aggressively. In addition, legal provisions are being made to ensure that such an event represents a serious breach of contract, with the defendants seeking redress in court

The patent is only granted to companies that issue bonds in the blockchain, through a short window at the time of issuing the bond. The commencement of the obligation is marked by the construction of new token assets by the credit bureau. Tokens for these assets are sent to creditors for the purpose of obtaining money transferred to the company. If we choose this transfer to happen again

the blockchain, an additional currency asset could be issued by a trusted party and used for this purpose. As in the previous scenario, participants could buy and sell these currency tokens using deposits and withdrawals in the issuer’s bank account.

Bond rights holders are legally defined in terms of a blockchain status in certain areas at a time. For example, interest payments are made according to the ownership of the asset in the first block of its time stamp after its due date. At maturity, bonds redeemed by their tokens are sent to the issuer to provide cash payments to the responsible holder.

Each exchange involving bonds is possible atomic, using a single blockchain transaction that must be exchanged. However, if the mines are run jointly by competing entities, less signed transactions cannot be used to create power-enabled exchanges through a blockchain network. Let’s assume that an

attractive exchange offer is passed as a partial transaction, which leads several participants to create a complete transaction that accepts what is offered. In this case, the next block miner has the ability to choose which of the competing trades is guaranteed. If a miner has a share in the outcome of the competition, perhaps because they have done some of these transactions, a clear conflict of interest arises. Indeed, because of the obstacle to diversification of mines, participants may refrain from mining entirely until the transaction they want to confirm confirms. As a result of these risks, the matching of organizations to exchange operations needs to take place in an external process, where the blockchain only works to resolve those conversations quickly.

Consumer-facing rewards scheme

Let's expand the use of blockchains to include consumer goods, where several US food bands come together to form a leak system. This system allows for profits collected from one restaurant to be used in another, without providing centralized database control to any single company or external contractor

This use case brings the difference between the spine and the blockchain network boundary. The theme contains standard QI nodes, which store the entire blockchain and verify all transactions and blocks as they enter. In parts there are lightweight bags, which can also be networked but do not keep the blockchain or secure transactions with blocks.

Each company that participates in the reward scheme operates on a full node with administrative, mining and creative rights. Mining diversity parameter is set to about 0.75, allowing other nodes to fail without stopping the blockchain. Apart from this, the blockchain allows unrestricted access to connect, send and receive transactions.

Scheme buyers use lightweight wallets, which act as mobile applications, which connect to complete nodes to receive and send transactions. The inline input of bulk assets within the transaction output enables these lightweight wallets to operate securely over the network without the need to separately track the movement of goods. Since blockchain has no limit on communication, sending and acquiring rights, anyone can start using the system by entering a wallet that generates its own private key and address.

The goods themselves are vouchers, issued in the name of each company and denominated in US dollars. These vouchers are offered to customers as a reward for purchases at participating restaurants. They can also be used by customers at the purchase price of any of the restaurants participating in the program. Finally, each company is able to use discounts issued by another company to receive cash at (us) 30% of the sticker price

Ensuring privacy

In any blockchain, all transactions are publicly visible to all participants, and this creates an important problem with privacy. First, blockchains give each participant a chance to get a global picture of the combined volume of the seized and traded assets. Depending on the usage case, this feature may or may not be desirable. The most serious problem, however, is that participants learn the public addresses of other participants when working with them, enabling them to integrate full and future trading activity into the future.

An easy way to solve this problem is for each participant to work under many different addresses.

When sending or receiving a transaction, they can use a different address depending on the identity of the partner. This prevents any group from getting a full picture of their colleagues' activities, because they do not know what other addresses they are working with. Stakeholders can move goods between their addresses as needed and, when necessary, take care to ensure that the transaction is not separated from payments to other businesses. Alternatively, a trusted middle class can provide a "mix-up" service, allowing assets to be deposited and withdrawn using different addresses, while ensuring that there is no visible connection between deposit and withdrawal activities

The most important method of secrecy is promised by cryptographic techniques such as homomorphic encryption and zero knowledge evidence. In a general sense, this enables the calculation of certain calculations to be performed, with their accuracy proven publicly, without disclosing the inputs and results of those calculations. In blockchain the techniques can be used to hide the value of the transaction to everyone except the sender and receiver of that transaction, while enabling all network participants to ensure that transactions are valid. If blockchain participants are unable to detect large numbers of transactions with each other, it becomes a small thing to hide the actual activity behind the activity screen screens that move small amounts.

Lightning Network

Lightning Network (LN) is a second layer added to Bitcoin's network enabling transactions to be done between parties off of the blockchain—called off-chain transactions. Lightning Network has been often considered a game-changer in the cryptocurrency's evolution. It is designed to speed up transaction processing times and decrease the associated costs of Bitcoin's blockchain. In a nutshell, the lightning network allows participants to transfer bitcoins between one another without any fees using their digital wallets. Payment channels are created between the two users so that they can transact with each other—in other words, off-chain transactions. Lightning network is another layer added to Bitcoin's blockchain so that it can process micropayments between participants.

The goal of the network was to create channels in which payments could be made between users without any fees or delays. By allowing the transactions to be done off-chain, the processing time and the number of transactions done via the on-chain network would be improved.

Benefits of QI Blockchain

- Cheaper compared to other blockchains. As an investor looking to make a profit, the cost will not be a problem for small investors.
- The use in the real world will be limitless.
- Our transaction is confirmed in a few seconds at low cost.
- Bulk supply of coins and as trees don`t grow to heaven, QI`s currency is greatly undervalued compared to BTC, ETH, Ripple, BNB, etc.
- No Stipulation code

- The excessive strength cost, extended pressure at the environment, related unfavorable media coverage, growing centralization of mining operations, and coffee transaction throughput will in all likelihood make it unviable with inside the lengthy run
- Sustainable low Transaction fees even in times of high usage
- Use of lightning network
- One of the Fastest blockchains ensuring almost real-time transacting.
- Transaction speed of 1500-2000 tps/sec

Blockchain comparison

	Bitcoin	**Ethereum**	**Ripple**	**QI**
Decentralised	Yes	yes	No	Yes
Scalability	No	No	Not proven	Yes
Secure	Yes	yes	yes	Yes
Speed	4.6tps	20tps	1000tps	**1500tps**
Transaction fees	High	High	Low	Low
Storage	DLT	DLT	DLT (EOS has issue in this regard)	DLT
Consensus	POW	POW→POS	RPCA	POW
Application layer	No	Yes	No	Yes
Environment friendly	No	No	Yes	Yes

QI is 10x faster than SWIFT in terms of transactions per second and it should be noted that Ripple like most cryptocurrencies has infinite number of tokens diluting the value and scarcity.

Conclusion

Termed by Vitalik Buterin, The Blockchain Trilemma addresses the challenges developers face in creating a blockchain that is scalable, decentralized and secure — without compromising on any facet. Blockchains are often forced to make trade-offs that prevent them from achieving all 3 aspects:

1. Decentralized: creating a blockchain system that does not rely on a central point of control.

2. Scalable: the ability for a blockchain system to handle an increasingly growing amount of transactions

3. Secure: the ability of the blockchain system to operate as expected, defend itself from attacks, bugs, and other unforeseen issues

   QI is not only the perfect blockchain but also the perfect exchange of monetary value adhering to all above issues.

   Current financial discourse suggests the imminence of a cashless society, a concept that arose from the global popularization of digital financial services and the development of technologies with the potential for application in financial markets. Cash is simply too expensive in terms of security, transfer, creation, etc. to be feasible for the next generation of money and we are seeing the adoption of digital money by governments and institutions at a rapid rate. Any government around the world can build their digital currency on Qi blockchain for to ensure a secure and transparent network with 100% uptime for their legal tender. The use of blockchain enables any dApp to process data through distributed networks and to execute transactions.