“OneCoin – A Privately Controlled Cryptocurrency based on Blockchain Technology”

by Marcelo García Casil, Co-Founder & CEO of DXMarkets Pte. Ltd.

Paper commissioned by OneCoin Limited.

April 2017

Abstract

Blockchain, a term originally coined by Satoshi Nakamoto as part of the Bitcoin white paper, is the fundamental building block of most currently available cryptocurrencies. Blockchains behave like distributed messaging networks with cryptographic data storage capabilities. In the context of this white paper blockchains are referred primarily as networks, as the main purpose is to explore the viability of private blockchain networks versus public blockchain networks, with the former explicitly being controlled by single organization or more typically a private company. Another way to look at this comparison is to associate public blockchain networks with fully decentralised networks versus private blockchain networks being controlled and governed by a well-defined party.

Although originally conceived as part of a fully decentralised system, blockchains can be rolled out in a centralised manner to create, distribute and control a privately-managed cryptocurrency.

This paper explores the viability of private blockchain networks and in particular the OneCoin Blockchain, a purpose-built private blockchain system for OneCoin Limited.

Blockchains

Blockchains are distributed peer-to-peer messaging networks that rely on a consensus algorithm used by all nodes in a given network to agree on what the latest correct state of their data storage is. Blockchains primary purpose is to track and register financial transactions, and more importantly ownership of assets. Identity and authentication in a blockchain system are managed by asymmetric cryptography.

To ensure that transactions are irreversible and cannot be tampered with, blockchain systems utilise cryptographic techniques to bundle transactions in groups, called blocks, which are stamped with a unique digital fingerprint typically in the form of merkle tree roots. These blocks are linked, or “chained”, to one another so that if any transaction in any given block were to be modified then the merkle tree roots of any subsequent block would fail its verification. This particular feature allows blockchain networks to track with certainty each and every transaction ever processed, and to have them stored in a ledger that is tamper-proof and therefore provides transaction finality.

Disadvantages of public blockchain networks

Despite the increase in popularity of public blockchain networks like Bitcoin, and the strong support they enjoy from the open source community and cryptocurrency enthusiasts, there are a number of reasons why public blockchain networks are not suitable for implementing a privately controlled cryptocurrency.

In addition, token protocols and asset protocols have been implemented in a number of networks besides Bitcoin, namely NXT, Counterparty, Omni and others. These token protocols attempt to address some of the native limitations of their networks, but ultimately

they fail to escape the boundaries of their own networks and therefore are constrained by the intrinsic nature of their underlying blockchain protocol.

Performance

Low processing capacity

Due to their decentralised nature, public blockchain networks must implement algorithms to determine validity of transactions determined by network agreement, or consensus. These distributed consensus algorithms require nodes to communicate with each other in real-time, which in a globally distributed network involves potentially large message times due to the physical limitations of having to transmit information over the internet infrastructure.

In addition, public networks are exposed to cyber-attacks. In particular, public decentralised blockchains can't rely on a central counterparty to distinguish good actors from bad ones, and therefore must implement anti-spam measures for the network to be able to protect itself from bad actors. Since protection in numbers is not a viable option due to the open nature of public networks, then alternative protection mechanisms have been put in place to make it economically inviable for bad actors to attack the network.

Under these schemes, public blockchain nodes are required to provide some sort of evidence upon submitting new validated transactions. The schemes adopted by public blockchains vary, but generally they involve the usage of a scarce resource. The most popular implementation of such a scheme is called proof-of-work and it involves intensive CPU computation. Other approaches, like proof-of-stake, require nodes to lock-in funds (i.e. put them "at stake") when submitting new blocks of validated transactions.

Both approaches have advantages and disadvantages, but the bottom line is that they have a negative performance impact on these networks, which translates into a hard cap of limited transaction capacity.

As an example, the Bitcoin network can process, on average, about 3 transactions per second, or about 200 per minute. If a private company wanted to issue their own cryptocurrency as meta-coin on the Bitcoin blockchain they would be competing with other companies trying to do the same thing, in addition to competing with native Bitcoin transactions. That would put the total daily limit of transactions worldwide for all participating actors at only 300,000. To put this into perspective, a leading credit card company would typically process in excess of 150,000,000 transactions a day. In other words, the Bitcoin blockchain could only handle 0.2% of the capacity of a single centralised payment company. This is a serious limitation.

Although the Bitcoin network has been used as an example for the sake of this comparison, all other public blockchain networks exhibit similar performance. Even if the capacity of the Bitcoin network were to be increased by optimisation, it would still remain several orders of magnitude below the capacity of equivalent centralised systems.

Network costs.

Public blockchain networks can be expensive to operate, in particular due to the intensive computational requirement as is the case of proof-of-stake, which translates into transactions

costs. Even in proof-of-stake or alternative schemes, the network is controlled and protected by unknown actors which have no formal relationship with the cryptocurrency issuing company. Nodes in public networks may hike up the transaction costs at their discretion and without notice. This puts a significant risk for any private company wanting to issue a privately controlled cryptocurrency, and may turn a perfectly profitable model into an unprofitable one if operating margins are tight.

Inefficient data storage.

Public blockchain networks are utilised worldwide by a multitude of actors. Due to the immutable nature of decentralised blockchain systems, all transactions are recorded and stored on a permanent basis. For a private company looking to operate their own cryptocurrency, this means that in addition to their own transaction data they must also store everyone else's data. Using a conservative approach of only 100 parties worldwide utilising the same blockchain, all pushing to this network the same volume, it would mean that each company would be storing only 1% of relevant data (i.e. their own) whereas the other 99% percent would be irrelevant. In other words, utilising this public blockchain network would result in data storage being 100 times more inefficient than in a centralised system, directly translating into storage costs becoming 100 times more expensive. For a system expected to have high volumes this can severely limit long-term scalability.

Security & Data Confidentiality

In addition to the aforementioned issues, public blockchain networks suffer from other shortcomings related to data privacy and network security.

Reliance on unknown actors

In public blockchain networks, nodes can be operated by any participant willing to abide by the network rules and having the required bandwidth and computing resources to validate transactions. Blockchain node operators are incentivised with rewards, in the form of coins or tokens, which are typically generated when a new block is created. This process is also called mining. As these actors have no formal relationship with any private company wanting to utilise the network, they may decide to stop support for a certain type of transaction affecting this private company if it's not in their best interest to support them.

Within cloud computing environments, private companies don't own the infrastructure yet they have SLAs and could potentially hold their providers liable for damages. This is a huge contrast with public blockchain infrastructures where there is nobody to reach out to, nobody to hold accountable or sue. There is no counterparty bound by a legal contract. This is, for the vast majority of companies, simply not acceptable.

A very similar scenario was presented in the past with the advent of the open source movement. Companies were reluctant to utilise open source software because there was no company behind it who could take a liability and commit to an SLA. Flagship projects like Linux started gaining market share only when companies like Redhat decided to front the liabilities generally expected from a software provider.

Data Privacy

It is a fundamental characteristic of blockchain systems to give full visibility about every single transaction to all participants. This is primarily so that all nodes can verify such transactions and protect the network against bad actors. There have been attempts at addressing this factor, in the form of zk-SNARKS, also known as zero-knowledge proofs. However, this approach in itself is still relatively new within the blockchain industry and has yet to be extensively tested for its long-term reliability.

In addition, there is also the fact that that private companies may be forced to selectively disclose certain transactions due to financial regulations, for which they would need to have full visibility over the whole network, therefore making full transaction encryption in the form of zk-SNARKS a suboptimal solution in this context.

Private Blockchain Networks

Private blockchains, by nature, are not decentralised and therefore do not need some of the expensive protection mechanisms that exist in public blockchain networks.

No bad actors

Operating blockchain nodes can be restricted to a set of well-known actors who can be legally bound to operate nodes and validate transactions. In practice, these nodes could also be operated either wholly or partially by the same central entity that controls the private blockchain network.

Having the ability to reliably nominate blockchain nodes eliminates the need to have expensive anti-spam measures and therefore achieve far greater performance than their public network counterparts.

Access control

In addition, a layer of access control can be added so that each participating part in the blockchain network has different permissions, therefore creating different roles that could be granted or revoked as determined by the central entity operating the blockchain system. This particular feature enables the creation of more complex user dynamics, controlling exactly who could read, create and validated transactions.

In addition, computationally expensive mining algorithms can be eliminated and replaced by other more efficient fault-tolerant algorithms. Since economic incentives are no longer required, mining becomes optional and simply a way of well-known and steady supply of new currency. Under certain circumstances mining could be removed altogether and replaced with discretionary issuance of new currency (or minting) by the central entity operating the blockchain network.

Data privacy

In a private blockchain network it is possible to create data access boundaries and therefore determine exactly which participants can see the full blockchain activity. For instance, in the context of blockchain used as a payment system, merchants and customers could be limited to seeing only their respective transactions.

Efficient data storage

For any given organisation, running a private blockchain network (as opposed to a public one) also means that they would only need to store relevant transactions – i.e. their own. This resolves the long-term scalability concerns of public blockchains by keeping storage costs under control.

Network cost

Having a set of well-known blockchain nodes who are bound by law to operate a blockchain system also means that operating costs can be predictable, and therefore not jeopardise the business model of the operating company. Also, the absence of proof-of-work or equivalent techniques, allows the network to grow in size while being cost-efficient.

In public blockchain networks there is an economic incentive for participants to operate blockchain nodes, which rewards being given proportionally to the computing power attributed to the proof-of-work computation, also called mining. Therefore, miners compete in a never-ending arms race to attain computing power, making it continuously more expensive to run blockchain nodes.

A matter of trust

Blockchain systems are sometimes called trust machines, and this is so because these systems essentially create a mechanism whereby unknown parties can transact with each other without having to rely on a trusted intermediary.

It could be argued that a private blockchain network effectively removes this feature by placing trust in the central entity operating the system. Certainly, a private blockchain system is centralised and therefore participants are exposed to counterparty risk. If the operating entity ceases to exist then their blockchain network would potentially also cease to operate (unless it's taken over by another party). This very much resembles the model of existing financial players.

Following this rationale, why would a company decide to run a private blockchain network as opposed to a traditional IT system using a conventional database? There could be many reasons.

Resilience

Despite being centralised, private blockchain systems are distributed in nature and highly tolerant to faults. This means that private blockchain networks can continue to operate for as

long as a node is still active. In fact, the network itself could temporarily split and then later on re-join and consolidate without impacting service continuity.

This even allows for parts of the system to continue operating while being offline or fully isolated from the rest of the network. This can be particularly useful for payment systems.

Transparency

Blockchain systems are tamper-proof ledgers of transactions, and this is essentially guaranteed by the merkle tree roots attached to each block of transactions. In a centralised blockchain system, one could argue that the operating entity could simply re-write every single block if they wanted to modify any past transactions. However, this can be easily remediated by anchoring the private blockchain system into another system of higher trust. This could be a trusted and well-known public blockchain network, or simply a transactional and irreversible information system owned and operated by another reputable counterparty (e.g. a form of git log).

Provability

Although private blockchain systems do not offer fully decentralised trust, they still provide a high-degree of trust in the way transactions are executed. Participants can, at any point in time, have certainty and verifiability about the state and operations of the blockchain network, namely:

- Proof of funds: in a blockchain system, it is possible to verify independently that the counterparty executing a payment has sufficient funds to do so.
- Proof of transaction: both payer and recipient obtain an immediate digital certificate of each completed transaction. While these certificates are not final until they're included in the next block, under normal network operation they provide a high degree of certainty.

The case for privately controlled cryptocurrencies

After having explored the benefits of private blockchain networks, a number of perfectly valid use cases can be identified.

Loyalty points

A company wanting to run a loyalty scheme could choose to utilise a private blockchain network to keep track of point balances. Given the nature of blockchain systems, these points could immediately be integrated with external merchants with relative ease to facilitate point redemptions.

In addition, customers could collect, transfer and redeem these points securely and reliably.

IOU system

IOUs (short for “I owe you”) are tokens representing a financial liability or credit. A remittance or money transfer company could decide to utilise a private blockchain network to represent the IOU credits between branches and external outlets.

Such a system would not require reconciliation of accounts or clearing since the blockchain system would track account balances in real-time. In addition, since blockchain systems record each and every transaction, auditing of a blockchain-based IOU system would be straightforward and inexpensive.

Settlement currencies

Multi-national companies having to process payments in multiple currencies generally rely on centralised netting and treasury functions, that oftentimes require balance reconciliation to avoid discrepancies. Such a company may choose to operate a private blockchain network to keep track of their currency movements, and use an internal netting token to settle multi-currency transactions. This blockchain-based system would never have discrepancies and could track all account balances accurately and automatically.

The OneCoin Blockchain

OneCoin Limited is a company facilitating a number of services including an online training academy and ecommerce. OneCoin Limited operates a large community estimated to be in excess of three million customers, for which it uses OneCoin as an engagement tool and utility token for its community to access the services that the company provides. OneCoin itself can be best described as a digital currency.

The OneCoin private blockchain system (OneCoin Blockchain from now on) is fully owned by OneCoin Limited and has been designed to satisfy the company’s requirements.

OneCoin Limited has commissioned this paper and the design of a next generation bespoke private blockchain software solution suitable to operate the OneCoin digital currency from a reputable fintech company who have been tasked to deliver a state-of-the-art version of this solution. This software solution is licensed exclusively to OneCoin Limited, who are responsible for its implementation and operation. The system itself is capable to fully run on OneCoin Limited’s privately-managed IT infrastructure.

KYC (Know-Your-Customer)

OneCoin Limited operates a KYC process to validate all customers before they are allowed to use the OneCoin platform. The OneCoin Blockchain supports storing hashes of KYC data and KYC documents.

Scalability

The OneCoin Blockchain can handle millions of user accounts on standard high-spec hardware (e.g. equivalent to current AWS 2xlarge instances) and this can be scaled up by upgrading to more powerful hardware (e.g. equivalent to AWS 4xlarge, 8xlarge, 16xlarge instances or higher) as required.

Permissions

The OneCoin Blockchain is fully permissioned and OneCoin Limited, at its discretion, can selectively grant different access to each node and account (e.g. read, transfer, etc.).

Mining

The OneCoin Blockchain supports a proof-of-work style mining and consensus algorithm, for which its difficulty and block times are at the discretion of OneCoin Limited and are set as initial parameters for each blockchain in the system.

Limited Supply

The OneCoin Blockchain has a maximum number of coins to be issued. This cap is set as an initial parameter for each chain and cannot be changed afterwards.

Payment API

The OneCoin Blockchain provides a standard API to allow external parties to use OneCoin as a payment option. This is intended for merchants to be able to accept OneCoin payments securely.

Multi-signature

The OneCoin Blockchain supports multi-signature wallets. This type of wallet provides enhanced security and allows for approval workflows involving multiple parties (e.g. to release funds from a treasury account in a controlled manner).

Accounting System

The OneCoin Blockchain utilises the UTXO model. UTXO stands for Unspent Transaction Outputs and is the processing model utilised by the Bitcoin blockchain and several other blockchain implementations. The UTXO model allows for transactions to be processed in parallel, delivering greater performance.

Anchoring

The OneCoin Blockchain is to be operated fully by OneCoin Limited and, as such, is a centralised system. To guarantee and prove the integrity of its data, the OneCoin Blockchain will supports anchoring using other public decentralised blockchain networks that are perceived as having high trust, namely Ethereum and Bitcoin.

The way anchoring works is by storing the merkle tree roots of successful OneCoin blocks into the public blockchains. The frequency of anchoring (e.g. every x blocks) is defined by configuration and at the discretion of OneCoin Limited in the deployment.

Conclusion

Blockchain systems are incredibly powerful and provide the foundation for reliable, secure and instant digital transactions. Albeit revolutionary, public blockchain networks present significant challenges when it comes to being adopted by private companies. Public blockchain networks are innovative in facilitating fully decentralised trust.

In contrast, private blockchain networks are centralised and therefore rely on the existence of conventional trust channels. However, these private systems do not have most of the challenges that exist in public blockchain networks, and therefore companies can reliably use them to represent cash, loyalty points, credit tokens or any other assets having financial value.

Private blockchain networks, if used efficiently, have the potential to greatly simplify internal operations, reconciliations and back-office functions, leading to significant cost reductions and increased customer and partner engagement thanks to simple and secure integrations with external systems.