THREEFOLD.TECH

The Blockchain Dilemma Problem (dec 2019)

[Introduction](#)

[Blockchain Basics](#)

- [Private, Permissioned or Public Blockchains](#)
- [Private Data and Anonymous or Pseudo-Anonymous Data?](#)
- [Consensus Protocols for Public Blockchains](#)
  - [Proof of Work (High Cost in Compute and Energy)](#)
  - [Proof of (Block) Stake (Low Cost in Compute and Energy)](#)

[The Blockchain Dilemma Problem](#)

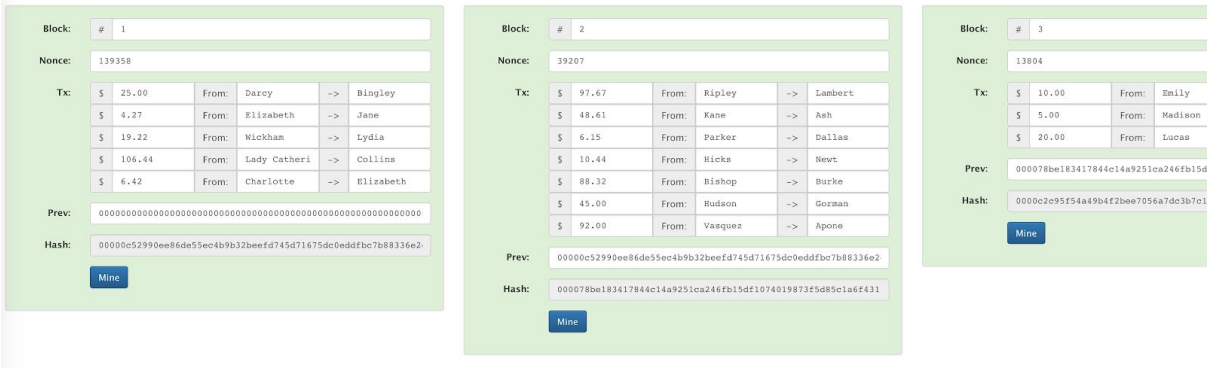
Introduction

Blockchain technology has the power to change the world of IT. There are a huge number of new initiatives using blockchain technology around the world all chasing different use cases. Some care little about the underlying technology but use blockchain-based projects and tokens/coins to get rich quick.

In general there are two types of blockchains: proof of work blockchains and proof of stake blockchains. They differ in the way how they select who has created a truthful block securing a number of transactions (forever, as blockchains provide an immutable record of events).

Blockchain Basics

A blockchain is as the word says a chain of blocks of information. As shown in the graphic below the “blocks” contain information on transactions. Transactions are the transfer of value of a digital currency (token) from wallet A to wallet B. The “chain” aspect comes is where a part of the information stored in a block is a link to the previous block (a unique number). This is a very simple representation of what a blockchain is.



Private, Permissioned or Public Blockchains

The complexity around a blockchain comes from how the blockchain software is run. The software can run in two different ways: a small (or large) number of nodes controlled by one single entity (private blockchain) a person or a company, or a large (or small) number of nodes controlled by multiple entities (public) that do not know each other and where anyone interested to run a blockchain node can join.

By running blockchain software under the supervision of one entity (private, centralised) you can quite easily make sure the information stored in the blockchain (transactions) are not tempered with by only operating a small number of nodes and deploy them in very safe physical locations (private data-centers, vaults, basements of offices etc). A private blockchain does not allow unknown entities to join and run the blockchain software.

A permissioned blockchain is operated by known entities such as stakeholders of a given industry. It is a mix of both private and public blockchain. In this type of blockchain network, a participant may not need permission to join the network but needs permission to transact with another network participant

A public blockchain allows anyone to join the blockchain operation and create a new blockchain node. The blockchain is run by multiple entities (decentralized, public) that have no relationship nor knowledge about each other

For these three type of blockchains, there are different mechanisms to protect and guarantee the validity of transactions and make it tamper-proof.

Private Data and Anonymous or Pseudo-Anonymous Data?

For private blockchains, it is straightforward to see that all data that is stored on private blockchains is private and creates 100% anonymity for its users. The only entity or person that has access to information stored on the blockchain is the blockchain operator. This is comparable to how a bank operates. The bank knows everything about all of its customers and the customers only know about themselves - the non-bank customers do not know a thing.

On a public blockchain, people can join and operate a blockchain node on which all information of that blockchain is stored. While private blockchains get their security from putting their blockchain nodes in secure buildings operated by trusted people a public blockchain achieves its security from having a large number of nodes that have the same data replicated over and over. A consensus algorithm is required in order to accept new data (new blocks) to the chain.

Consensus Protocols for Public Blockchains

The main consensus protocols used today are Proof-of-Work, Proof-of-Stake, Proof-of-Authority, Raft and Federated Consensus. For the purpose of this document, we limit the considered consensus protocols to Proof-of-Work and Proof-of-Stake.

Proof of Work (High Cost in Compute and Energy)

The proof of work consensus protocol is best explained as a race. Consensus is achieved by having all participating nodes solve a puzzle. The puzzle is a one-way translation of an amount of information consisting of the following items:

- All the data that present the transactions in the block - all the data is known by all participating nodes
- The number of the previous block. Remember a blockchain links blocks of information together.
- A (variable) number. This number is the part that can be changed.

The “work” is done by changing the variable number and see what the translation of all data brings. The translation of all this data is a new number, and the requirement is that that number needs to be smaller than what is known as the “difficulty level”. The difficulty level number has a fixed amount of numbers but when the first digits of the number are zero the overall number is lower. So a higher difficulty is built by having a number that has more zeros at the start in the difficulty number.

Once the block is completed, all nodes will get the complete block of transactional data, everyone knows the previous block number and will start to change the variable number to get output from the puzzle algorithms comparing it to the required difficulty level.

The node that will find the number first will announce that is has found a solution matching the required difficulty level and the variable number of shared with all nodes in the network to verify that his solution is correct. If a large portion of the nodes have verified the solution to be valid the solution is accepted and the block is added to the chain because consensus is reached.

Proof of (Block) Stake (Low Cost in Compute and Energy)

With proof of stake consensus algorithms, the consensus algorithm does not solve puzzles in a race to be the first. The first step is to identify and allow a certain number of nodes to be part of the blockchain. This is called a permissioned blockchain because you need to have permission to partake. This permission is given by distributing stakes.

Proof of stake consensus mechanism is solving a puzzle, but the puzzle contains only static elements - not variables - based on different characteristics:

- The block number
- The content (part) of blocks a long time ago (>2000 blocks)
- The transaction number (between the first and the last transaction) in the block of the stake transfer transaction all participating nodes needs to to

- The current timestamp

All these numbers are fixed but the time stamp and every node in the block stake blockchain will solve this puzzle every second until the output of this puzzle matches the required difficulty level.

To make sure the one node that has solved the puzzle to match the difficulty level cannot introduce information in the block which allows him to tamper with the next blocks this node cannot use his used stake for a period amount of time for creating new blocks.

The fact that the puzzle-solving includes historic block data and once a node is assigned to create the block and put it on a chain will not be able to use that block state for a period of time makes it very costly to try to tamper with the content of the block (and the next blocks).

The Blockchain Dilemma Problem

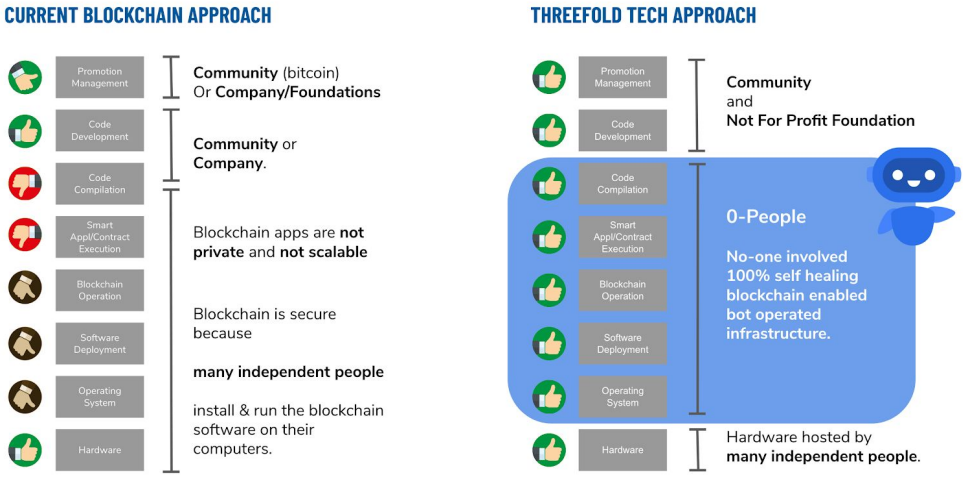
Public and private blockchains have their specific advantages and disadvantages and are very good for specific use cases - but not all. If we list the specifics of both we end up with a table like this:

	Public Blockchains	Private Blockchains
Security	Provided by having a large number of nodes running it.	Provided by having them in secure controlled places
People	Build, managed and controlled by unknown people	Build, managed and controlled by known people
Speed	Slow by design - all data needs to be copied to all of them	Fast(er) and more efficient by design - a smaller number of copies of the blockchain data

So what if we want to have a secure, performant and easy to manage blockchain solution? This is not what can be delivered by either type of blockchains. We have to create a new type of blockchain that combines the best of both worlds and delivers.

The key element in finding a solution for this problem is to take the human element out of it. The fact that when you deploy blockchains solutions in locations without human intervention means that you need to create a different deployment mechanism that takes out people touching code, compiling code, deploying code and in the end operating the machine in which the code runs.

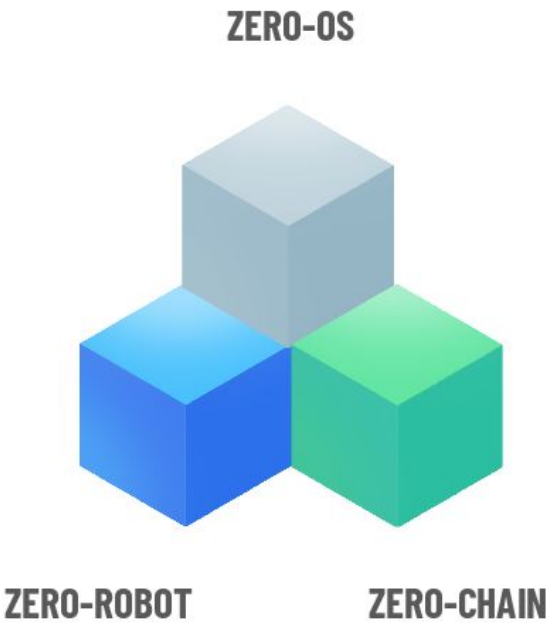
A way to get around the trusted people problem is to select a platform on which software can be downloaded, compiled, installed and operated without human intervention. Such a platform is a unique platform which has not been developed and launched. Such a platform would have to have the following characteristics



To make this system work and solve the blockchain dilemma we need to have three components working together in an orchestrated way.

The three elements are:

- A (simple) operating system that does not allow local and remote logins - a closed operating system that receives instructions to launch or kill applications. This operating system needs to be stateless to keep as simple as possible: **Zero-OS**
- A virtual system administrator that is able to perform system administration tasks to make the system operate, selfheal and execute instructions from authenticated and authorized sources. **Zero-Robot** (3Bot)
- A ledger or database to store information in with regards to authentication, operational and financial transactions. **Zero-Chain**



This system architecture allows for authenticated and trusted virtual system administrators to download, compile and deploy software on a grid of secure Zero-OS nodes with an immutable ledger that records all transactions, operational and financial. This presents a platform on which a public (permissioned) blockchain can be run securely without requiring trusted people to operate the nodes.

In such architecture we can build and deploy a high-performance secure blockchain which are the combined benefits of a public and private blockchain.