WHITEPAPER - Initial Release

Feb 2023

REVO

Full dive into blockchain ecosystem

Public decentralized blockchain
Built in shared governance protocol
Fully EVM compatible
Shared redoundant storage subsystem
Enterprise ready
High I/O Sidechains
Decentralized Domain System (DDNS)

Enhancing blockchain technology
with innovative PoS v3 consensus algorithm.
Notarize, store data, verify.

revo.network

Written by
RevolutionChain Italy

Index

1.Introduction

Peer to Peer transfer of value and data

Before the birth of Bitcoin's P2P exchange protocol, the world of information technologies based fast transfer of data solely on communication channels such as TCP / IP (Transmission Control Protocol - Internet Protocol). Nowadays, communication technologies have evolved (Internet, IoT, Sharing, VR / AR) and find themselves making multiple devices communicate in real time, which interact at different levels of digitization.

These devices, together with their global communication systems, base their functioning on a scheme that has its roots in complex centralized systems. As the demand for content sharing increases, people are beginning to put their focus (economic and social) on transfer methods that ensure security and point-to-point interoperability, skipping any type of intermediary that could prove to be a point of failure.

With software and platforms such as Napster, E-Mule, Limewire or Torrent, the urge to find a permanent solution was growing ever greater.

In October 2008, Satoshi Nakamoto released his whitepaper: "Bitcoin: a Peer-to-Peer Electronic Cash System". He was the first to theorize and propose a completely free and decentralized digital value transfer system. In the Bitcoin ecosystem, participants entrust the entire network with direct control of transactions, thus the parties can complete transactions and transfers without establishing a relationship of trust. Being able to transfer value without the need for a single central counterparty would have changed everything.

The technology behind this system was (and is) the Blockchain, which contributed to the creation of a new distributed society. Since its first release as open source software, dozens of blockchain projects have appeared. Some use advanced technologies to allow software to run in a distributed manner (Smart Contracts), others place the emphasis on security, traceability and anonymization.

The growth of blockchain systems faces many challenges.

Blockchain?

The blockchain is a ledger that is shared between the nodes of a computer network. Not to be confused with classic databases, the information inside is saved digitally and distributed, with total redundancy and grant of immutability. They are known mainly with the birth of Bitcoin but it is important to know that the blockchain is just a type of technology that underpins these systems (more commonly called cryptocurrencies).

As reported above, what we can consider as the main difference between Blockchain and Database is how the data is structured. A blockchain collects information together in groups, called blocks, which contain a set of data. These blocks have well-defined criteria of storage space and when they become full they are closed and linked to previous blocks forming a chain of contents: Blockchain. A Database structures its data within tables.

This data structure by its nature creates an irreversible timeline. When a block is sealed, it get's a timestamp and is immutable, becoming part of this timeline.

Transparency

Because of the decentralized nature of Blockchains, all transactions can be transparently viewed by either having a personal node or using blockchain explorers that allow anyone to see transactions occurring in real-time.

Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and broadcast to the network. This means that if you wanted to, you could track Bitcoin wherever it goes from it's first bit.

For example, exchanges have been hacked in the past, where those who kept Bitcoin on the exchange lost everything. While the hackers may be entirely anonymous, the Bitcoins that they extracted are easily traceable. If the Bitcoins stolen in some of these hacks were to be moved or spent somewhere, it would be known.

Of course, the records stored in the Bitcoin blockchain (as well as most others) are encrypted. This means that only the owner of a record can decrypt it to reveal their identity (using a public-private key pair). As a result, users of blockchains can remain anonymous while preserving transparency.

Security

Blockchain technology achieves decentralized security and trust in several ways.
To begin with, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. After a block has been added , it is extremely difficult to go back and alter the contents of other blocks unless a majority of the network has reached a consensus to do so.
That's because each block contains its own hash, along with the hash of the block before it, as well as the previously mentioned timestamp. Hash codes are created by a mathematical function that turns digital information into a string of numbers and letters. If that information is edited in any way, then the hash code changes as well.

Let's say that a hacker, who also runs a node on a blockchain network, wants to alter a blockchain and steal cryptocurrency from everyone else. If they were to alter their own single copy, it would no longer align with everyone else's copy. When everyone else cross-references their copies against each other, they would see this one copy stand out, and that hacker's version of the chain would be cast away as illegitimate.

Succeeding with such a hack would require that the hacker simultaneously control and alter 51% or more of the copies of the blockchain so that their new copy becomes the majority copy and, thus, the agreed-upon chain. Such an attack would also require an immense amount of money and resources, as they would need to redo all of the blocks because they would now have different timestamps and hash codes.

Due to the size of the many cryptocurrency networks and the speed at which they are growing, the cost to pull off such a feat would probably make it impossible.

Blockchain Trilemma

The perfect blockchain boasts three elements: Security, decentralization, and scalability.
Finding a balance between the three is difficult and presents a problem referred to as the blockchain trilemma.

Scalability and decentralization are often held back by security, but security tends to be compromised by any shifts on a network that offer scalability.

Projects either choose to focus on two out of three or work on finding a solution to tackle the trilemma once and for all. Innovative ideas like sharding, side-chains and state channels are used to address the trilemma but they still remain experimental.

A solution to the problem could lead to greater adoption of cryptocurrency and blockchain and wide-spread use of the technology across many industries.

Nowadays, Blockchain integration **is hard**

Interoperability between the various blockchains is almost completely non-existent. For example, the Bitcoin ecosystem is based exclusively on the UTXO (Unspent Transaction Output) model, not compatible, for example, with the entire Smart Contract sector which is instead the basis of a usual system of decentralized applications on Ethereum.

The consensus rules of a blockchain are defined in code when the mainnet is launched, updating live parameters is very difficult, and not always practicable, and putting together an entire community on a hard fork often generates instability.

The few companies that actively use blockchain are forced to rely on fully or partially centralized ecosystems, which at the moment seem to be the only solution to exploit blockchain technology at very high levels of validation speed (TPS - Transactions per second) . However, controlled by central and unverifiable entities, can they still be considered blockchains? Perhaps as a software structure, but not as a guaranteeing model of immutability, security and true transparency.

Current consensus mechanisms almost totally lack flexibility. For example, the Proof Of Work (PoW) places us in front of limitations in terms of demand and energy consumption, not to mention the incentives that must be guaranteed to miners and holders. There is also a real risk of centralizing computational power.

Smart contracts are a beautiful thing, but if there are no simple ways that allow them to operate in everyday life and in industrial processes, they remain only something innovative, but unattainable. De facto limiting its mass adoption.

Gateways, APIs and interconnection systems are sometimes different for each blockchain, there are few standards but the barriers to entry for new developers are still too high making the blockchain a thing for the few.

The personnel training sector is very important. Often many self-styled experts are not even aware that they do not even know what they are talking about.

Above all, now, the world must also find an alternative solution to energy-intensive processes, favoring all those consensus mechanisms that have among their objectives also the reduction of CO2 emissions.

1.1 Design

Multiple integrations of innovative technologies

The blockchain world is full of opensource projects and services that want to consolidate on well-defined technological aspects however. For example, Bitcoin has its roots in protocol security and decentralization, Ethereum is focused on decentralized applications (DApp -Smart Contracts), Solana focuses on speed, Polkadot on interoperability, ZCash on anonymization of transactions through zero-knowledge protocols (zk-SNARK). Other projects, such as Filecoin and Storj, were instead born to favor decentralized storage space. Nano and it's costless transactions can be a good example too.

But this can be dispersive in some contexts, and leads to enormous confusion in business integration processes.

Developing a blockchain in itself is not too complicated a job, the real challenge is precisely to bring together all these technologies and bring an easy, comprehensible and compatible ecosystem to the world.

The concept behind **REVO** is precisely to group all the leading technologies in a single blockchain ecosystem.

This not only allows transactions to be processed autonomously, efficiently and securely, but also able to meet the needs of those companies and Enterprise-level applications which need a certain type of features, effectively breaking down all the barriers that make this technology too complicated for industries to digest.

Supporting technologies (what's coming)

UTXO Accounting model (Bitcoin)

Simplification of blockchain accounting methods. Instead of having to track and archive every single transaction, we just need to keep track of the unspent coins.

EVM - Ethereum Virtual Machine (Ethereum)

Represents the runtime environment for the development and management of Smart Contracts. The managed code has no access to the internet and acts completely independently.

AAL - Account Abstraction Layer and VMx86 (Qtum)

Level of abstraction capable of converting blockchain outputs into account balances, enabling the transfer of information between the EVM and UTXO-based blockchains.
The VMx86 model will allow the deployment of Smart Contracts written with more common languages such as C, C #, Java, Rust ..

Proof of Stake protocol (PeerCoin - Blackcoin)

Proof-of-stake is a cryptocurrency consensus mechanism for processing transactions and creating new blocks in a blockchain. A consensus mechanism is a method for validating entries into a distributed ledger and keeping the database secure.

Transaction Shielding - zk-SNARK (ZCash)

Cryptographic methodology that allows one party to prove to another that a statement is true, without revealing any information about itself. More commonly called Zero Knowledge Proof.

Distributed Filesystem (SeaweedFS)

SeaweedFS started as an Object Store to handle small files efficiently. Instead of managing all file metadata in a central master, the central master only manages volumes on volume servers, and these volume servers manage files and their metadata. Conceived to be simple, scalable and distributed, it is able to save billions of files and serve them very fast.

1.2 Market Analysis

Enterprise priorities

Over the past five years, smart contracts and enterprise blockchain have gone from being just an exciting technology with potential, to a technology that has started to provide immense value to enterprises. 2021 was an exciting year for users of both, during which we saw several announcements from corporations, governments, and investors taking tangible steps towards adoption of these technologies.

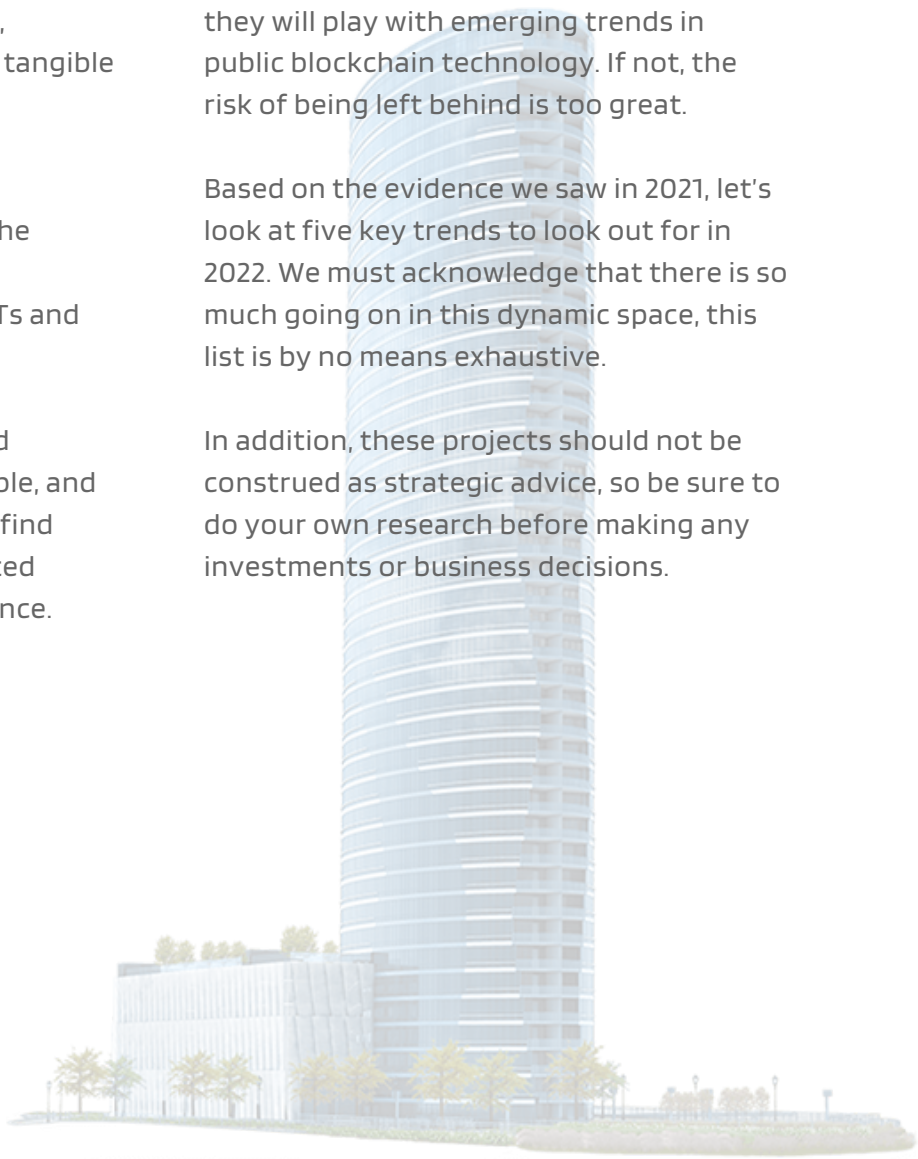
What was even more exciting was the resurgence of decentralized public blockchain applications such as NFTs and DeFi.

The benefits of smart contracts and blockchain grow increasingly tangible, and rapid innovation is driving users to find solutions to the most commonly cited objections of privacy and performance.

In 2022, the biggest trends in enterprise blockchain appear to be stemming from the realization that new capabilities and innovation in customer engagement, product design, business models, and enterprise technology architecture must be considered from the perspective of how they will play with emerging trends in public blockchain technology. If not, the risk of being left behind is too great.

Based on the evidence we saw in 2021, let's look at five key trends to look out for in 2022. We must acknowledge that there is so much going on in this dynamic space, this list is by no means exhaustive.

In addition, these projects should not be construed as strategic advice, so be sure to do your own research before making any investments or business decisions.



NFTs for customer engagement and marketing

NFTs (non-fungible tokens) are an ownership record of a digital or physical asset on the blockchain. Being on the blockchain means that ownership is now publicly verifiable. For example, Twitter is planning a service in which they will certify that a user owns an NFT if that user has it as their profile picture. The underlying asset could be entirely digital (e.g., a digital art, or an ebook), or something physical (e.g., an oil painting). Just like any premier product, NFTs are best created for items that are in limited quantities and are of an exclusive nature, so as to enhance their attractiveness to buyers. The most popular trends so far include "limited-edition" products, such as the exclusive wine in finely crafted bottles available for collectors in limited numbers, heritage NFTs launched by Budweiser, and digital art that helped Beeple raise money for charity. There are many innovations cropping up, such as NFT galleries where new NFTs are showcased, communities, and marketplaces.

So far, much of the corporate focus around NFTs has been on brand marketing. As we move to 2022, we predict that NFTs will be used to enhance customer engagement and boost retention. To do so, NFTs will move from being just limited-edition, exclusive items that are owned, to providing access to associated services and new experiences. They will likely be integrated tightly with business processes running on enterprise blockchain. NFTs become even more powerful when issuers can pack rights and obligations within the NFT.

Metaverse: physical and virtual worlds

If you read about the metaverse, it can begin to feel like science fiction. Just like in iconic movies like The Matrix, actions in the virtual world have ramifications in the physical world, and vice versa. While we're not there just yet, we are heading in that direction. We will soon see several important, related enterprise blockchain applications in 2022. With Facebook and Square both having adopted new blockchain-themed identities, where their next innovations will come from is a topic of debate.

In 2021, we began to see renewed interest in virtual worlds, such as Decentraland. It's already easy to buy a piece of land in the virtual world; you can then construct properties where you can buy, sell, and rent goods of various kinds. A simple way to think about it is that the video games you have been playing can now start offering you a way to be a part of the game itself — Nike, for example, has already created their own world on Roblox. On the other hand, projects such as Gods Unchained are taking a different route by giving you ownership of the assets you buy in a game.

In 2022, we believe that businesses will look at enhancing their appeal by offering integrations with the virtual world. Some common applications we could see are smart homes, tourism, and shopping malls. For example, someone could buy something in the metaverse and it could then be shipped to them in the physical world. It is not far-fetched to think that completely new experiences will be offered to maximize commerce and customer experience.

However, there are some basic enablers that will need to be put in place: The ability to maintain private identities, the privacy of avatar actions, and the ability to make and receive payments, among others.

B2B: supply chain, healthcare and finance

2021 saw the launch of multiple large-scale enterprise projects with smart contracts and enterprise blockchain. For example, the Australian Securities Exchange went live, Deutsche Börse announced a new post-trade platform, and Xpansiv is scaling their platform for ESG commodities.

In 2022, we will likely see this trend of enterprise blockchain applications accelerating. To meet emerging business demands, it is critical to bridge data islands and harmonize business processes across enterprise boundaries.

Enterprises are able to finally connect external collaboration with internal business processes. Blockchain programming languages should provide a way to rapidly develop applications and should be able to run cross-platform — on databases as well as across multiple blockchains. This dramatically reduces data reconciliation needs and improves privacy.

For example, medical insurance claims should be able to achieve straight-through processing and rigorous privacy without the need for data duplication, as the workflow executes from the customer through to the provider, to the insurer, and back. At all times, all parties should be able to see only what they are supposed to see, and nothing else. The same is true of financial transactions, inventory management in supply chain, and other use cases.

DeFi

DeFi, or decentralized finance, is on a rapid upswing, with significant value now locked in across several different protocols. Indeed, several new platforms (in addition to Ethereum) are emerging to provide extremely fast and cheap transactions. In 2022, we will continue to see the rise of DeFi, but we will also see mitigation strategies for risks that participants encounter. The SEC is clearly aiming for more compliance than enforcement, and it has identified transparency and pseudonymity as two of the biggest challenges to solve. We are also seeing DAOs emerging as governance mechanisms. DAOs may also open up the way for regulators to be part of the disclosure and transparency solutions that are put in place. Enterprise and DLT blockchain can likely be the vehicles for that collaboration.

As this space matures further, and adoption becomes more widespread, governance will likely start becoming an important consideration. Further, as the organizational complexity increases, business-process workflows will have to transcend both permissioned and permissionless ledger boundaries. They must also be able to support transaction privacy beyond the pseudonymity provided by public blockchains.

Enterprise blockchain

These five enterprise blockchain trends for 2022 are rapidly taking off. It's important to note that these trends are also interconnected. Particularly when it comes to enterprise technology, it will be important to look beyond the buzz. Enterprise architecture roadmaps would do well to include a review of how enterprise blockchain technology will interlink with the innovations on the public blockchain. As ecosystems expand, interoperability needs will begin to strongly exert themselves in order to meet evolving customer expectations.

Much like how the cloud has done, the only way to meet the emerging trends head on will be to bridge internal and external business processes and not be locked into underlying ledger technology. The benefits of blockchain and smart contracts technology are just too great to ignore for future business and tech innovation.

1.3 Team and expertise

People working on Revo Technology

Revo is a public blockchain technology developed by RevolutionChain, a company that bases its expertise on a very specialized development team. Founded in January 2019 by Nicola Bertelli, the company has set itself as a national and European reference point in the field of consulting, mining, training and core blockchain development.

One of the goals for RevolutionChain is for Revo to become the starting point for a completely open source and free future development, where everyone around the globle can become a part of the blockchain contribution ecosystem.

Nicola Bertelli - CEO & Founder - Core Developer

Nicola has been involved in IT and blockchain development since 2014. During his career he worked as technician on behalf of Unisys, Sisal and Dell, especially in the sys and network areas, gaining consolidated experience. In the blockchain field, he has not only dealt with core software development, but also managed and built mining pools, explorers and complex decentralized systems. He has been CEO and owner of RevolutionChain since it's start, in 2019.

Miodrag Popovic - Core Developer

Miodrag is a long-time developer, in recent years thanks to his knowledge in software programming he has approached the world of blockchain development thanks to ZeroClassic, a decentralized blockchain born from a fork of Zero which is based on the source code of Zcash. Over the years he has specialized in core development acquiring a very deep knowledge of decentralized technologies and related protocols.

Pablo Lizàrraga - Frontend Developer

Pablo is passionate about the world of information technology. In 2015 he began his engineering career in information systems. In the third year of his degree, he decided to focus entirely on programming, in the area of web development. He is now a full stack web developer. He has extensive experience in languages, libraries and frameworks such as Javascript, typescript, nodejs, express, react, redux, sequelize, postgresql, tailwindCSS among others.

Chris Lu - Developer

Chris Lu is a software engineer, developer of SeaWeedFS, a completely open source software that allows the creation of distributed data storage networks in a very efficient and distributed way. He made himself available to follow the decentralized storage project through the use of his technology.

Goran Apostoloski - Design & Web

Goran Apostoloski is a passionate graphic designer and web developer, who uses all Adobe software solutions to create beautiful designs. Involved in crypto since 2013, he got experience in crypto programming, mining, investing and trading. A whole new world that has skilled him up to another level.

Marco Giovanni Zorzan - Software Developer

Marco has many years of experience in the IT field, gained in many sectors. Developer and technician in the automation, iOT and management software sector. An expert in C / C ++, Visual Basic, Java, PHP. For some years he has been dedicated to the development of software solutions and blockchain integration in production chains.

Cesare Carli - Training

Cesare Carli is an IT consultant and professional trainer. Technology and Free Software evangelist since the late 1990s, he is strongly committed to spread knowledge about possibilities and applications in the blockchain field. He spent the first part of his career working in projects financed by the Fourth and Fifth Framework Programme of the European Commission, then he decided to go on as a freelance IT system administrator, besides his training activity. He met Revo in 2021 and this gave him the possibility to face the challenges of explaining to the world how a modern blockchain works.

Gian Piero Leoni - Community manager

Gian Piero entered into the crypto world in 2012, back in the days when mining was predominantly cpu/gpu and early home ASICs. During these years he met a lot of people, initially in the BitcoinTalk forum. He is the owner of one of the first completed Bitmain ASIC SHA miner collection starting with Antminer U1 through to the ANTMINER S17 for a total of 13 different restored and perfectly working ASICs that represent the history of mining. He knows and uses MySQL, PHP and HTML languages. He is also a trader and a pure holder and is convinced that the future is in crypto.

2. Technical Characteristics

Enterprise grade, untamperable sidechains

As already mentioned above, Revo is a public blockchain developed starting from the Qtum source code that immediately set itself quite ambitious goals. What is shown in the previous analysis is that medium and high level Companies need something very reliable, stable and predictable.

For example, a Company that has decided to monitor its supply chain through the use of blockchain technology cannot afford to sustain large market variations in the price of the currency. This is because a system that today turns out to have a certain degree of efficiency, could in the future lead to a sudden change of parameters and values due to market conditions. As we all know, companies base their operations on the basis of a business plan and actions and corrections are implemented according to what is defined by the same: if at any time the cards on the table change, it could be a huge operational (as well as economic) problem.

Revo is a decentralized blockchain, but this does not mean that all applications linked to it must be the same. Depending on the degree of complexity and volumes that a DApp requires, it may be necessary to build a private blockchain to meet its specific needs (speed, zero latency, ability to save huge amounts of data, transactions per second, etc.). However, it is necessary to understand that a private blockchain, by its nature, will never be able to satisfy the requirements of transparency, security and immutability, as it is in fact centralized and governed by a single entity.

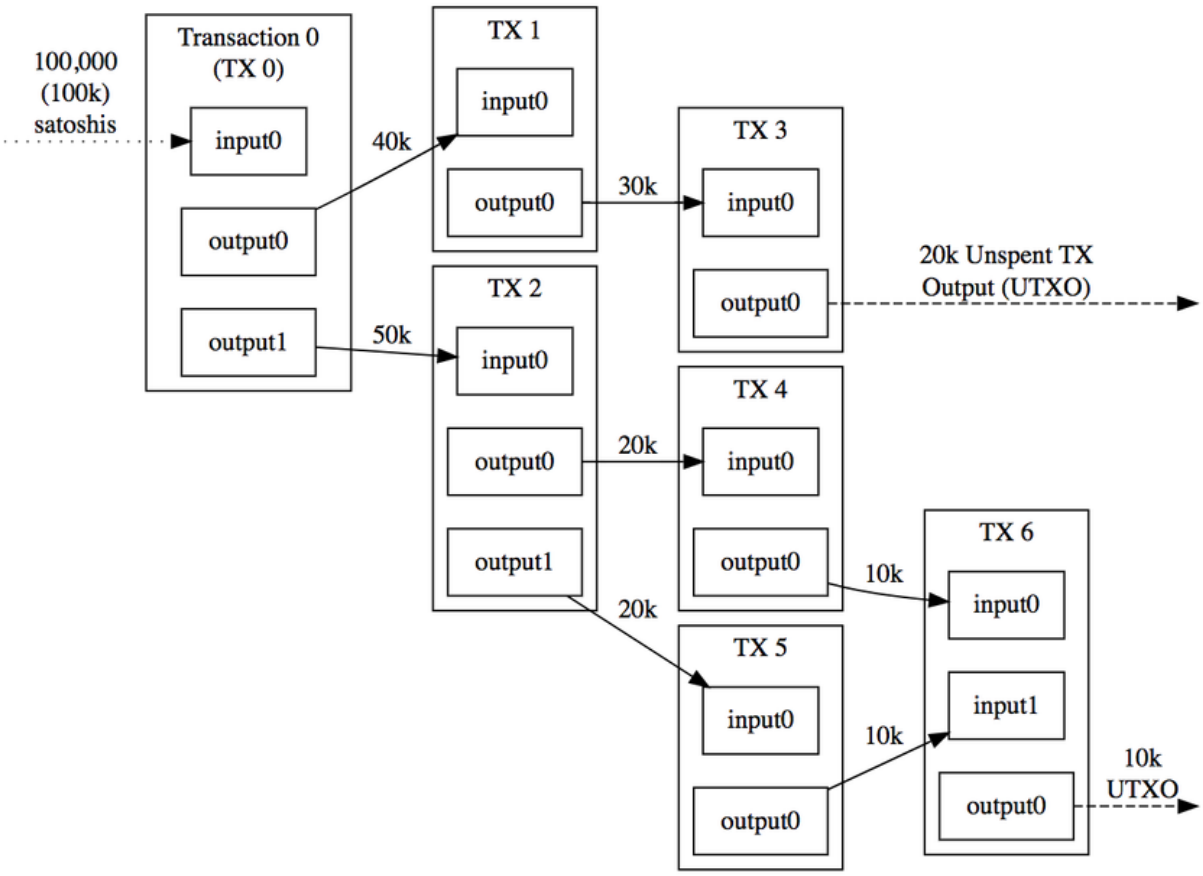
In fact, for the latter problem, Revo provides a framework capable of making operational PoA sidechains interconnected with REVO, the primary blockchain. Thanks to this new type of protocol, the centralized sidechains will notarize their existence on the primary public blockchain (PoI - Proof of Immutabilty) block by block, avoiding the possibility of future tampering.

In this section the more technical aspects will be explored in detail

2.1 UTXO and Account/Balance models

Unspent Transaction Output Model

In Bitcoin, each transaction spends output from prior transactions and generates new outputs that can be spent by transactions in the future. All of the unspent transactions are kept in each fully-synchronized node, and therefore this model is named "UTXO".
A user's wallet keeps track of a list of unspent transactions associated with all addresses owned by the user, and the balance of the wallet is calculated as the sum of those unspent transactions.



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Let's take a look at a simplified example of how the UTXO model works in Bitcoin transactions:

- Alice gains 12.5 bitcoins through mining. Alice's wallet is associated with one UTXO record of 12.5 bitcoins.
- Alice wants to give Bob 1 bitcoin. Alice's wallet first unlocks her UTXO of 12.5 bitcoins and uses this whole 12.5 bitcoins as input to the transaction. This transaction sends 1 bitcoin to Bob's address and the reminder of 11.5 bitcoins is sent back to Alice in the form of a new UTXO to a newly-created address (owned by Alice).
- Say there was another UTXO of 2 bitcoins associated with Bob prior to step 2, Bob's wallet now shows that his balance is 3 bitcoins. Bob's wallet now keeps track of two UTXOs: one from before and another from the transaction in step 2. Each UTXO needs to be unlocked if Bob wishes to spend them.

Account/Balance Model

The Account/Balance Model, on the other hand, keeps track of the balance of each account as a global state. The balance of an account is checked to make sure it is larger than or equal to the spending transaction amount. Here is a simplified example of how this model works in Ethereum:

- Alice gains 5 ethers through mining. It is recorded in the system that Alice has 5 ethers.
- Alice wants to give Bob 1 ether, so the system will first deduct 1 ether from Alice's account, so Alice now has 4 ethers.
- The system then increases Bob's account by 1 ether. The system knows that Bob has 2 ethers to begin with, therefore Bob's balance is increased to 3 ethers.

Benefits and drawbacks

Both models achieve the same goal of keeping track of account balances in a consensus system.

The benefits of the UTXO Model are:

- **Scalability** — Since it is possible to process multiple UTXOs at the same time, it enables parallel transactions and encourages scalability innovation.
- **Privacy** — Even Bitcoin is not a completely anonymous system, but UTXO provides a higher level of privacy, as long as the users use new addresses for each transaction. If there is a need for enhanced privacy, more complex schemes, such as ring signatures, can be considered.

The benefits of the Account/Balance Model are:

- **Simplicity** — Ethereum opted for a more intuitive model for the benefit of developers of complex smart contracts, especially those that require state information or involve multiple parties. An example is a smart contract that keeps track of states to perform different tasks based on them. UTXO's stateless model would force transactions to include state information, and this unnecessarily complicates the design of the contracts.
- **Efficiency** — In addition to simplicity, the Account/Balance Model is more efficient, as each transaction only needs to validate that the sending account has enough balance to pay for the transaction.

One drawback for the Account/Balance Model is the exposure to double spending attacks. An incrementing nonce can be implemented to counteract this type of attack. In Ethereum, every account has a public viewable nonce and every time a transaction is made, the nonce is increased by one. This can prevent the same transaction being submitted more than once. (Note, this nonce is different from the Ethereum proof of work nonce, which is a random value.) Like most things in computer architecture, both models have trade-offs.

In revo, both technologies are present, which are exploited for the correct storage of balances and EVM compatibility

2.2Account Abstraction Layer (AAL) (Qtum)

Creating a magical bridge to the EVM world

Qtum was the first blockchain ever to create synergy between the UTXO model and the one based on Account / Balance. Before seeing how, however, it is important to understand the basic logic for the correct functioning of the code of a Smart Contract.

If, as mentioned above, for each address we have a UTXO set, how would a Smart Contract interpret and select which coins to use during its execution? And what about internal transactions between contracts which would normally be carried out in the VM by just adjusting the balances of the contract in question? How do you model those in a UTXO model where all spending transactions must be explicitly recorded?

When a transaction is sent to the nodes, it is conditional in a language commonly called Bitcoin script, which contains a series of operational codes.

```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

The cryptocurrency wallet software executes these opcodes on your machine. In this example the instructions tell the software to check the transaction to make sure the public key provided matches the signature of the transaction.

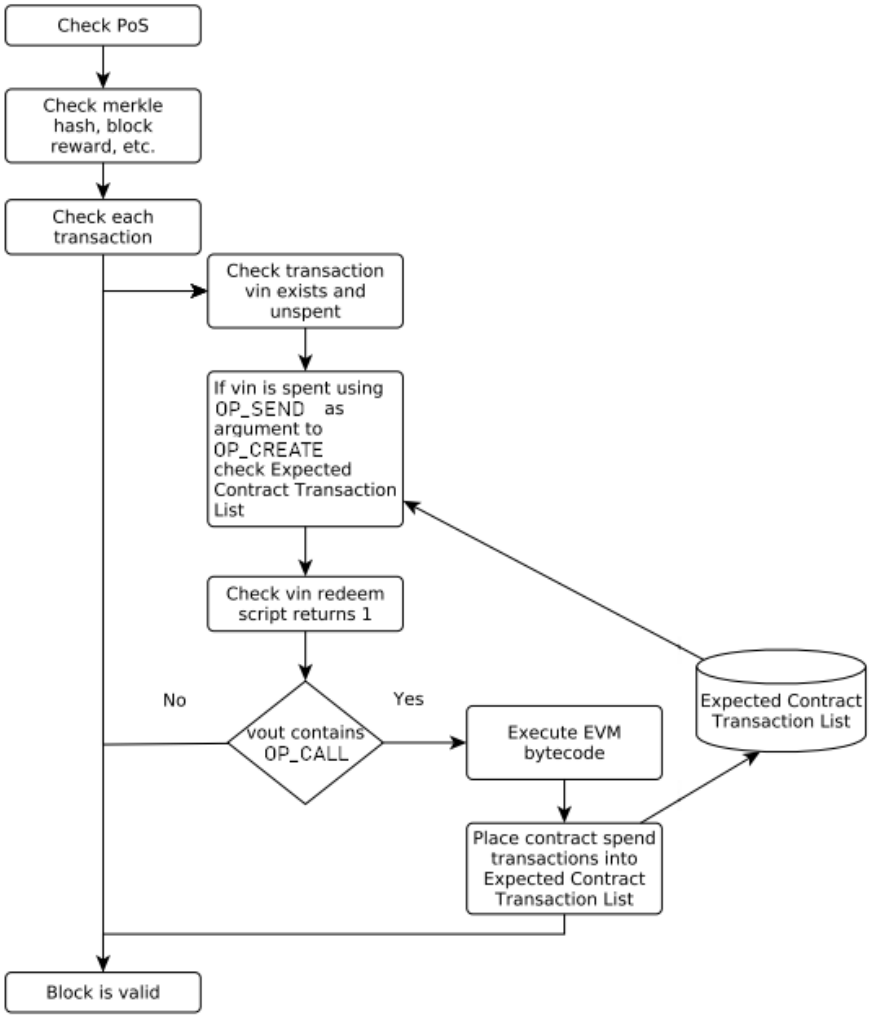
Stack	Script	Description
Empty.	<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	scriptSig and scriptPubKey are combined.
<sig> <pubKey>	OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Constants are added to the stack.
<sig> <pubKey> <pubKey>	OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Top stack item is duplicated.
<sig> <pubKey> <pubHashA>	<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Top stack item is hashed.
<sig> <pubKey> <pubHashA> <pubKeyHash>	OP_EQUALVERIFY OP_CHECKSIG	Constant added.
<sig> <pubKey>	OP_CHECKSIG	Equality is checked between the top two stack items.
true	Empty.	Signature is checked for top two stack items.

AAL adds to Revo a couple of new opcodes to the Bitcoin opcodes, adding support for smart contracts.

OP_CREATE: Used to create new smart contracts
OP_CALL: Used to execute code inside an existing smart contract
OP_SPEND: Used to spend the value in a smart contract

During the block creation process, the validator's software will parse the script inside each transaction, and when it comes across transactions using these opcodes, it will set them aside to be processed through the EVM. The EVM contract transactions are then processed into a special "Expected Contract Transaction List" which is executed by validator nodes. These transactions are then executed against the EVM, with the resulting output being converted into a spendable transaction.

If, during the execution of a contract, the contract calls another contract with a value, that transaction is also turned into an explicit transaction and attached to the current block.



By making the OP_CREATE, OP_CALL, and OP_SPEND transactions all spendable, we can actually manage the size of the Revo UTXO set fairly well. When a contract self-destructs, the OP_CREATE transaction is spent for example, removing it from the UTXO pool.

Another simplification exists for handling when a contract owns more than one UTXO. Instead of trying to pick which coins the contract should use (as earlier versions of Revo did) any time more than one UTXO exists for a contract, a new tx is created combining and condensing them into one UTXO.

A problem also exists concerning refunding gas fees in the UTXO model. Gas Model for Ethereum works by overestimating the cost of contract execution and after execution refunding the remaining amount by crediting it back to the spending account balance. This is relatively easily done in Accounts model through internal transactions but in the UTXO model it is impossible for a validator to partially refund a fee for transactions that don't use up all the gas. It must also be possible to roll back transactions that run out of gas while still crediting the spent gas to validators.

Refunding gas fees in Revo works by creating new outputs as part of the coinbase transaction for that block. All of the input gas is consumed and given to the validator, and the validator must include outputs in the coinbase transaction that credit the transaction senders with the gas refunds. These refunds are enforced using a new block validation consensus rule. Otherwise, it would be possible for validators to not return any gas at all.

Another problem exists in how transactions actually specify and send gas fees. In the UTXO model, gas and transaction fees are both combined and sent together so how can we separate out what is the fee to relay the transaction and how much to spend on gas and how much to refund compared to how much was used. This is done through a new simple fee model:

$$\begin{aligned} gas\_fee &= gas\_limit * gas\_price \\ txfee &= vin - vout \\ tx\_relay\_fee &= txfee - gas\_fee \\ refund &= gas\_fee - used\_gas \end{aligned}$$

After completing the contract execution, the remainder of the gas fee must be returned to the given gas return script by adding an output to the coinbase transaction the validators use to retrieve their block reward.

2.2.1 Address conversion

To physically maintain compatibility with ethereum-based addresses, each REVO address must be converted from base68 to hexadecimal. This conversion procedure is done via the **gethexfromaddress** and **fromhexaddress** commands.

```
20:07:03 gethexaddress RKbx72DueQiR7FmPkLncNZ3zXiVpaggEws
20:07:03 713d7f052e9933b86d597fa89f1c5e6f4e9dcbbe
20:07:08 fromhexaddress 713d7f052e9933b86d597fa89f1c5e6f4e9dcbbe
20:07:08 RKbx72DueQiR7FmPkLncNZ3zXiVpaggEws
```

2.2.2 Connectors (Metamask, WalletConnect..)

The backward compatibility of hexadecimal addresses may seem trivial, but it is really essential to allow connection gateways to work natively with REVO.
MetaMask allows users to store and manage account keys, broadcast transactions, send and receive cryptocurrencies and tokens, and securely connect to decentralized applications through a compatible web browser or the mobile app's built-in browser.

WalletConnect is another example of open source protocol for connecting decentralized applications to cryptocurrency wallets with QR code scanning or deep linking.

These connection gateways are the keystone that will allow all users of the world, even the less experienced, to interact with the blockchain world in a direct, secure and non-custodial way, a real bridge for mass adoption.

2.3EVM

Ethereum Virtual Machine

The EVM's physical instantiation can't be described in the same way that one might point to a cloud or an ocean wave, but it does exist as one single entity maintained by thousands of connected computers running a Revo client.

The Revo protocol itself exists solely for the purpose of keeping the continuous, uninterrupted, and immutable operation of this special state machine;

It's the environment in which all Revo accounts and smart contracts live. At any given block in the chain, Revo has one and only one 'canonical' state, and the EVM is what defines the rules for computing a new valid state from block to block

Some basic familiarity with common terminology in computer science such as **bytes**, **memory**, and a **stack** are necessary to understand the EVM. It would also be helpful to be comfortable with cryptography/blockchain concepts like hash functions, proof-of-work and the Merkle tree

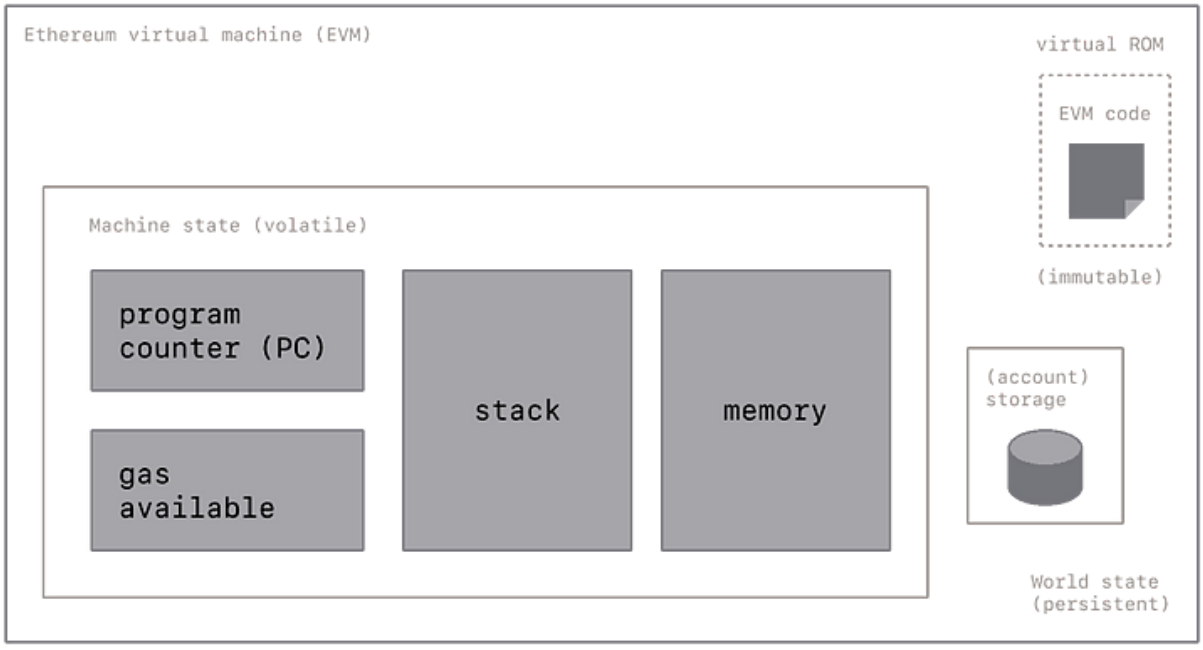
Revo EVM was entirely ported from latest **Ethereum** source code, and included all features and components as it's predecessor.

From ledger to state machine

The analogy of a 'distributed ledger' is often used to describe blockchains like Bitcoin, which enable a decentralized currency using fundamental tools of cryptography.
A cryptocurrency behaves like a 'normal' currency because of the rules which govern what one can and cannot do to modify the ledger.
For example, a Bitcoin address cannot spend more Bitcoin than it has previously received.
These rules underpin all transactions on Bitcoin and many other blockchains.

While Revo has its own native cryptocurrency (RVO) that follows almost exactly the same intuitive rules, it also enables a much more powerful function using Ethereum EVM: Smart Contracts. For this more complex feature, a more sophisticated analogy is required.

Instead of a distributed ledger, Revo is also a distributed state machine. Revo's state is a large data structure which holds not only all accounts and balances, but a machine state, which can change from block to block according to a pre-defined set of rules, and which can execute arbitrary machine code. The specific rules of changing state from block to block are defined by the EVM.



The state transition function

The EVM behaves as a mathematical function would: Given an input, it produces a deterministic output. It therefore is quite helpful to more formally describe Revo as having a state transition function:

$$Y(S, T) = S'$$

an old valid state (S) and a new set of valid transactions (T), the Ethereum state transition function Y(S, T) produces a new valid output state S'
State

State

In the context of Revo, the state is an enormous data structure called a modified Merkle Patricia Trie, which keeps all accounts linked by hashes and is reducible to a single root hash stored on the blockchain itslef.

Transactions

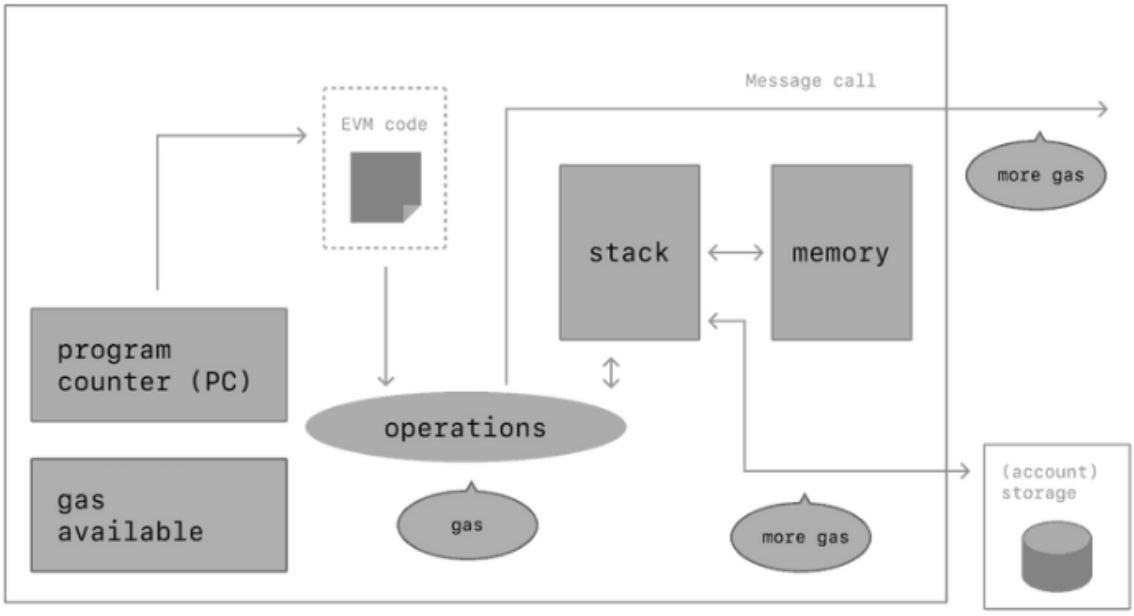
Transactions are cryptographically signed instructions from accounts. There are two types of transactions: those which result in message calls and those which result in contract creation. Contract creation results in the creation of a new contract account containing compiled smart contract bytecode. Whenever another account makes a message call to that contract, it executes its bytecode.

EVM instructions

The EVM executes as a stack machine with a depth of 1024 items. Each item is a 256-bit word, which was chosen for the ease of use with 256-bit cryptography (such as Keccak-256 hashes or secp256k1 signatures).

During execution, the EVM maintains a transient memory (as a word-addressed byte array), which does not persist between transactions. Contracts, however, do contain a Merkle Patricia storage trie (as a word-addressable word array), associated with the account in question and part of the global state.

Compiled smart contract bytecode executes as a number of EVM opcodes, which perform standard stack operations like XOR, AND, ADD, SUB, etc. The EVM also implements a number of blockchain-specific stack operations, such as ADDRESS, BALANCE, BLOCKHASH, etc.



2.3.1 Solidity

Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behaviour of accounts within the Ethereum state. Solidity is a curly-bracket language designed to target the Ethereum Virtual Machine (EVM). It is influenced by C++, Python and JavaScript.

Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features. With Solidity you can create contracts for uses such as voting, crowdfunding, blind auctions, and multi-signature wallets.

When deploying contracts, you should use the latest released version of Solidity. Apart from exceptional cases, only the latest version receives security fixes. Furthermore, breaking changes as well as new features are introduced regularly. We currently use a 0.y.z version number to indicate this fast pace of change.

2.3.2 IDE and Public Compiler

Solidity versions follow Semantic Versioning. In addition, patch level releases with major release 0 (i.e. 0.x.y) will not contain breaking changes. That means code that compiles with version 0.x.y can be expected to compile with 0.x.z where z > y.

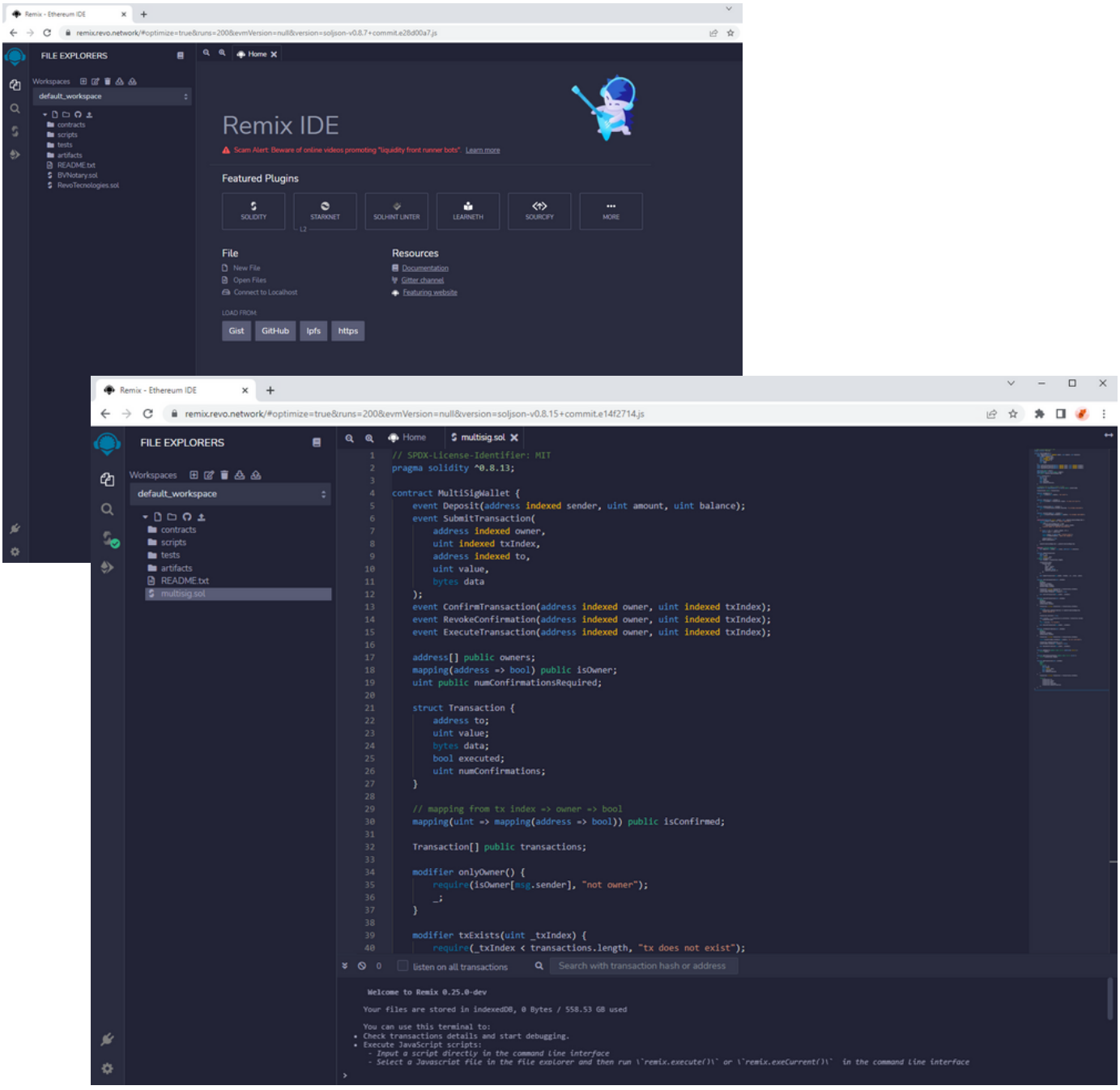
In addition to releases, we provide nightly development builds with the intention of making it easy for developers to try out upcoming features and provide early feedback. Note, however, that while the nightly builds are usually very stable, they contain bleeding-edge code from the development branch and are not guaranteed to be always working.

Despite our best efforts, they might contain undocumented and/or broken changes that will not become a part of an actual release. They are not meant for production use.
When deploying contracts, you should use the latest released version of Solidity. This is because breaking changes, as well as new features and bug fixes are introduced regularly.

On the Revo.network website, you can dive straight into writing and compiling Solidiy code, directly from your browser, without the need to download libraries or install a compiler directly over the linux CLI.

Available for free at any time and from any location it's a great tool to start developing , learning and directly deploying bytecode testing it's own execution.

The Revo Remix Compiler is available at **https://remix.revo.network**



2.4 x86 Virtual Machine

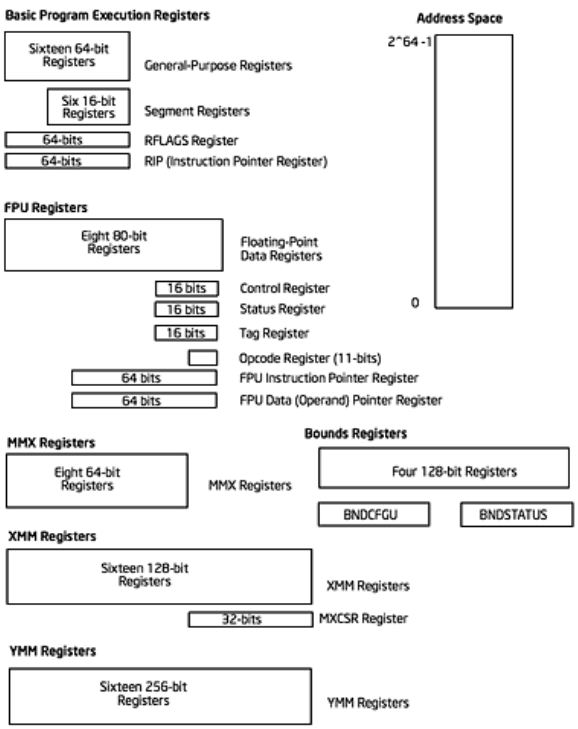
Multiple integrations of innovative technologies

The Qtum team has created an x86 Virtual machine (VM) for executing smart contracts in a variety of programming languages. This VM operates very similarly to the existing Ethereum VM, with some notable enhancements:

- In the Ethereum VM, all smart contracts must be written in Solidity and compiled down to byte code executed on the EVM. In this x86 VM, developers can write their smart contracts in any language that supports a JIT compiler, including C++, Java, Python, and other languages widely used in application development. This gives dApp developers much more flexibility in terms of smart contract development.

- In addition to supporting the existing gas model on common EVM (where users pay for each operation they execute in a smart contract), X86 has also added two new pricing models: fixed-fee per transaction and fee per transaction.

- It supports x86 registers and memory operations through a unified 16-bit instruction encoding scheme that significantly reduces gas costs in common cases compared to the Ethereum VM. This will allow developers to execute more operations per transaction and increase throughput on the Qtum blockchain.



2.5 Lightning Network

UTXO for full compatibility

The Lightning Network is designed to create transactions as fast and cheap as possible. It's part of a newer class of crypto technologies known as "layer 2" blockchains — which you can think of as being a little like HOV lanes on highways. By offloading some transaction "traffic" to the Lightning Network's "layer 2" blockchain, the core blockchain ("layer 1") can move faster.

As Bitcoin's value has grown over the years, the narrative has shifted. We now tend to think of Bitcoin as being more like "digital gold" — or as an inflation-resistant way to store wealth over time.

Why did that happen? In part it's because of the way the Bitcoin network is designed. Bitcoin allows two strangers anywhere to securely send or receive value without a credit card company or payment processor in the middle. It does this using a decentralized network of computers all over the world — all of which need to achieve consensus (or agree) about the current state of Bitcoin's digital ledger.

Nakamoto's solution to this problem was mining, which is a time-consuming and not environmental friendly process.
The Lightning Network was invented, in part, to help Bitcoin function more like the digital cash that Nakamoto envisioned. It processes transactions "off-chain" much more quickly and cheaply than Bitcoin's core blockchain — with fees that are typically fractions of a cent. Lightning transactions are also less energy intensive than transactions on the main blockchain. While the main Bitcoin blockchain (layer 1) can typically handle fewer than 10 transactions per second, the Lightning Network (layer 2) can theoretically handle millions of transactions a second.

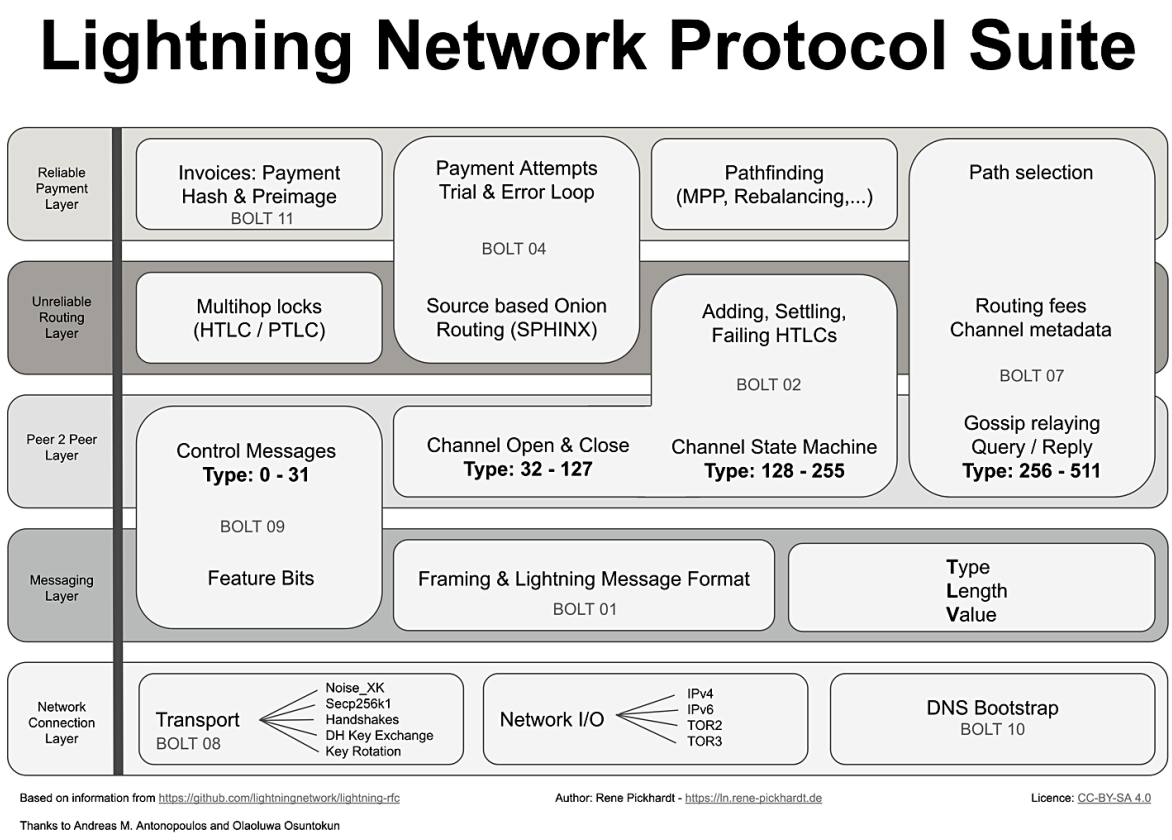
The Lightning Network uses smart contracts to establish off-blockchain payment channels between pairs of users. Once these payment channels are established, funds can be transferred between them almost instantly.

Cleverly, the network doesn't need to create pairs between all users. For instance, if User A has a channel with User B, and User C has a channel with User B but not User A, funds can still be freely transferred between all networked parties. Lightning addresses look like typical Bitcoin addresses, and the payment process is very similar for users.

At any time, users can close their payment channels and settle their final balances on the core blockchain. Because only the opening and closing of payment channels are recorded on the core blockchain, the entire network can move faster. Additionally, Lightning Network transactions can be more private than those made on the main blockchain (because layer 1 transactions all appear on a public and transparent ledger).

2.5.1 Compatibility

Thanks to the UTXO Model that Revo applies for his own address/balance structure, compatibility with Lightning protocol is already granted.



2.6. Proof of Stake

Light consensus model

Proof-of-stake is a cryptocurrency consensus mechanism for processing transactions and creating new blocks in a blockchain. A consensus mechanism is a method for validating entries into a distributed chain and keeping the database secure. In the case of cryptocurrency, the database is called a blockchain—so the consensus mechanism secures the blockchain.

Proof-of-stake reduces the amount of computational work needed to verify blocks and transactions that keep the blockchain, and thus a cryptocurrency, secure. Proof-of-stake changes the way blocks are verified using the machines of coin owners.

The owners offer their coins as collateral for the chance to validate blocks. Coin owners with staked coins become "validators." Validators are then selected randomly to "mine," or validate the block. This system randomizes who gets to "mine" rather than using a competition-based mechanism like proof-of-work.

To become a validator, a coin owner must "stake" a specific amount of coins.

Under PoS, block creators are called validators. A validator checks transactions, verifies activity, votes on outcomes, and maintains records while under PoW, the creators are called miners. Miners solve complex mathematical problems to verify transactions.

To "buy into" the position of becoming a block creator, miners need only to get the sufficient limit of coins or tokens required to become a validator for a PoS blockchain. For PoW, miners must invest in processing equipment and incur heavy energy charges to power the machines attempting to solve the computations.

The equipment and energy cost under PoW mechanisms are expensive, limiting access to mining and strengthening the security of the blockchain. However, PoS blockchains often allow for more scalability due to their energy efficiency.

Objectives

Proof-of-stake is designed to reduce the scalability and environmental sustainability concerns surrounding the proof-of-work (PoW) protocol. Proof-of-work is a competitive approach to verifying transactions, which naturally encourages people to look for ways to gain an advantage, especially since monetary value is involved.

Bitcoin miners earn Bitcoin by verifying transactions and blocks. However, they pay their operating expenses like electricity and rent with fiat currency. What's really happening then is that miners are exchanging energy for cryptocurrency. The amount of energy required to mine proof-of-work cryptocurrency profoundly affects the market dynamics of pricing and profitability. There are also environmental aspects to consider since PoW mining uses as much energy as a small country.

The PoS mechanism seeks to solve these problems by effectively substituting staking for computational power, whereby an individual's mining ability is randomized by the network. This means there should be a drastic reduction in energy consumption since miners can no longer rely on massive farms of single-purpose hardware to gain an advantage.

Security

Long touted as a threat for cryptocurrency fans, the 51% attack is a concern when PoS is used, but it is very unlikely. A 51% attack is when someone controls 51% of a cryptocurrency and uses that majority to alter the blockchain. In PoS, a group or individual would have to own 51% of the staked cryptocurrency.

It is not only very expensive to have 51% of the staked cryptocurrency—staked currency is collateral for the privilege to "mine." The miner(s) that attempt to revert a block through a 51% attack would lose all of their staked coins. This creates an incentive for miners to act in good faith for the benefit of the cryptocurrency and the network.

Most other security features of PoS are not advertised, as this might create an oportunity to circumvent security measures. However, most PoS systems have extra security features in place that add to the inherent security behind blockchains and the PoS mechanisms.

Reward

Revo uses PoS consensus model to check, verify and validate it's own transactions. To become a Revo validator, miners should have matured UTXOs, suggested amount is 100 RVO.

A single UTXOs should have atleast 500 confirmations to become elegible for staking. Revo offers a user friendly set of commands that allow miners to optimize their staking capabilities and chances to validate blocks.

Miners can issue the command **splitutxosforaddress** to split their biggest UTXOs into custom sizes. Bigger UTXOs get's automatically splitted up to certain level each time they stake.

splitutxosforaddress "address" minValue maxValue (maxOutputs)


```
{
  "txid": "197a199c3ac9dd8df574ca77da15c5da31db3f7101e2108638a3b2f94248b9f7",
  "selected": "1020.00",
  "splited": "1020.00"
}
```


For this example, the total input was 1,020 RVO, and the split was 9 UTXOs of 100.0 and one of 119.99566, the wallet sending a "transaction to self". Of course, after either of these commands, the UTXOs must mature for 500 confirmations before they can be used for staking.

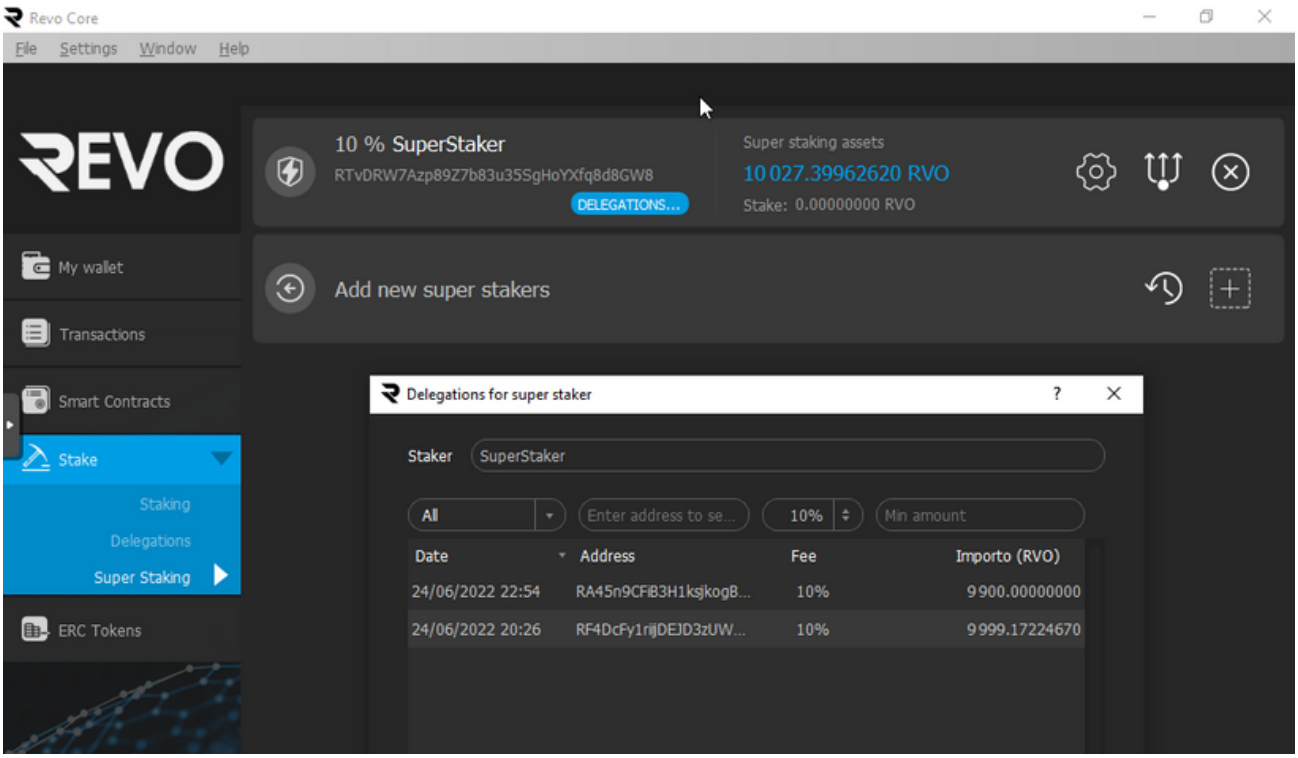
2.3.2 Offline Staking (Contract Delegation)

Revo Offline Staking allows the address for a non-staking wallet (capable of making the delegation assignment transaction) to be delegated to a Super Staker.

Offline Staking is non-custodial: the delegation user keeps full control of their coins and private keys. The address delegation is made via a smart contract transaction from the delegation user's wallet which identifies the delegator's address, the Super Staker address, and the fee the delegator agrees to pay. If the Super Staker accepts this fee, it will begin staking the delegated address UTXOs.

The normal rules for staking UTXOs apply to delegated UTXOs:

- UTXOs may only be used for staking after they mature (500 confirmations)
- The Super Staker will set a minimum size of UTXOs to stake, defaulting to 100 RVO. Delegated UTXOs below this amount will be ignored.
- It is best practice (for optimum returns) to break UTXOs up into sizes of 100 to 200 RVO each. For users of the Revo Core wallet, this can be easily accomplished with the command line version of splitutxosforaddress, described below.



The Super Staker must hold UTXOs to commit to stakes for the delegated UTXOs it is staking. The number of UTXOs (of minimum size 100 RVO) is based on Delegated Weight as a percentage of overall Network Weight, and good values are 30 UTXOs for staking 1% of Network Weight, 50 UTXOs for 2.0%, 100 UTXOs for 5% and 160 UTXOs for staking 10% of overall Network Weight. Super Stakers should monitor their Wallet weight (UTXO weight minus the amount currently staking) and add UTXOs if it drops below several thousand.

Technicals (Proof of Delegation)

The proof of delegation ("PoD") is a compact 65 byte signature made by the delegation{privkey} with the **staker{hexpubkeyhash}** as a message. This is done in order to prove that the delegator has at some point allowed the staker to stake blocks on behalf of the delegator. More specifically, the message that is signed is:

sha256d(staker{hexpubkeyhash})

The proof of delegation ("PoD") is a compact 65 byte signature made by the delegation{privkey} with the **staker{hexpubkeyhash}** as a message. This is done to prove that the delegator has at some point allowed the staker to stake blocks on behalf of the delegator.

This functionality will be activated automatically on the Revo Blockchain Protocol starting from block 21,000,000.

2.7 Sidechains (Enterprise)

Need for speed

As widely described in one of the previous chapters, one of the most important challenges of blockchains that profess to be public while maintaining a closed and centralized consensus protocol (e.g. Proof of Authority) is to guarantee the immutability of data within the blockchain.

Not only that, what is perhaps even more important to understand is that the blockchain, by its nature, will never be able to guarantee the authenticity of the data: this should make us understand that in certain situations it is necessary for an independent third party to be able to certify the correct insertion.

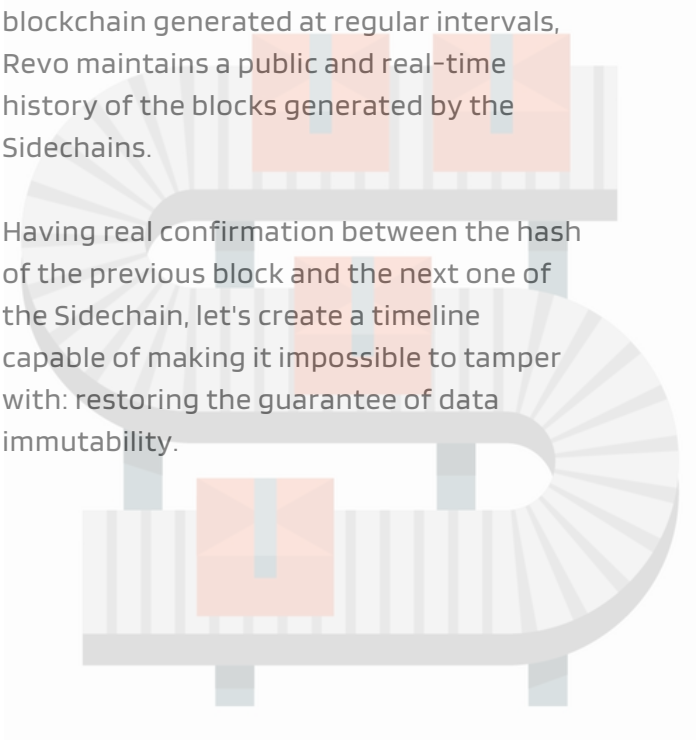
Take for example a large company that produces canned tuna, which decides to address its consumers in a transparent way, providing a tool that allows us to trace the origin of the tuna. This company works with very important volumes of lots, raw materials and supply chain processes and consequently needs data entry to be done very quickly and precisely. Usually for these types of processes different technologies come into play, which must interact with each other without delay. Just think of a conveyor belt that moves our tuna cans from the packaging department to the labeling department.

The smart contract that generates the identification codes for each label cannot wait for some miner to validate its transaction, the production chain would stop or suffer significant delays.

For this reason it is necessary to develop an internal blockchain, where the validation of transactions takes place instantly.

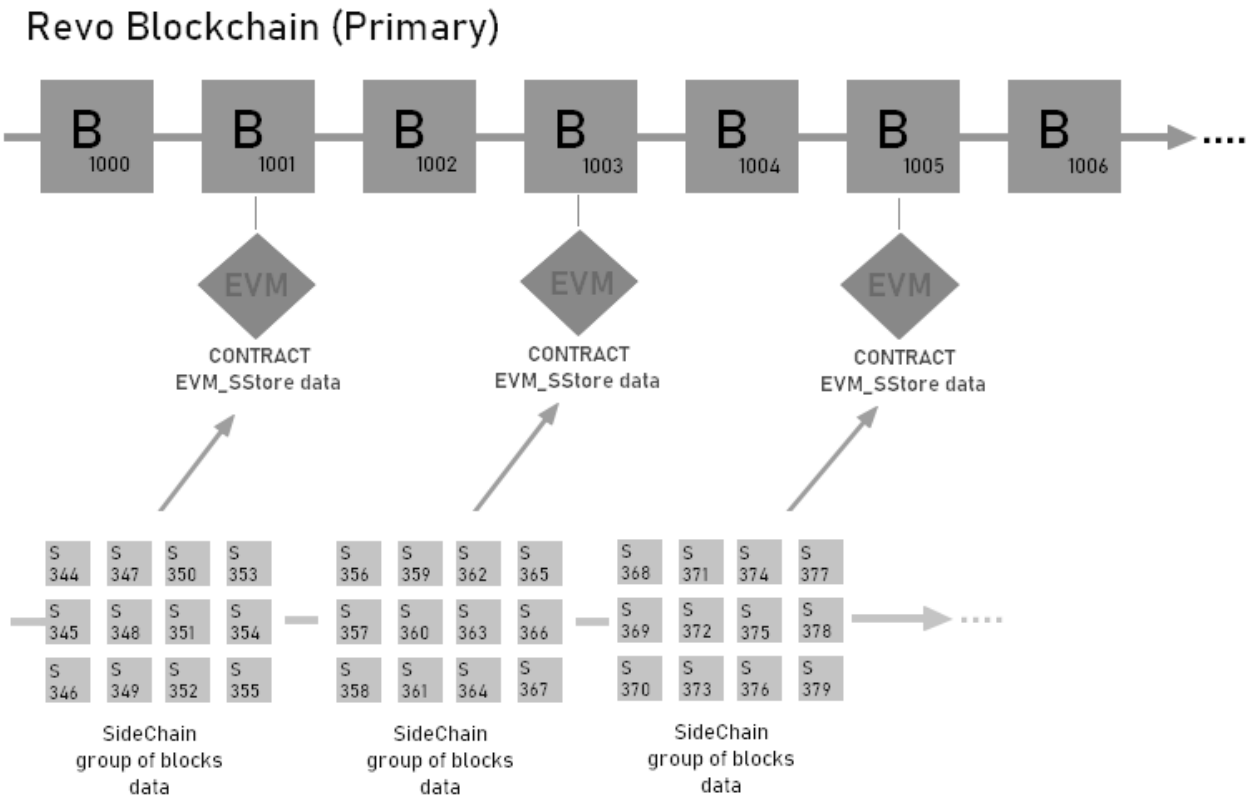
Revo implements an innovative technology, based exclusively on smart contracts, which allows Sidechains to self-notarize on the primary blockchain (Revo itself). Compared to other systems, which only notarize the hash of a snapshot of the private blockchain generated at regular intervals, Revo maintains a public and real-time history of the blocks generated by the Sidechains.

Having real confirmation between the hash of the previous block and the next one of the Sidechain, let's create a timeline capable of making it impossible to tamper with: restoring the guarantee of data immutability.



2.7.1 Sidechain Model

The scheme and the operating model of a Sidechain on Revo is in itself very simple: Revo acts as a primary public blockchain (being in fact public, decentralized and free) on which a dedicated Smart Contract is loaded has the task of functioning as a connector and save area for the SideChain timeline. Each data block is notarized on chain in epochs to avoid spamming too many transactions on the primary blockchain.



2.7.2 Network and consensus protocol

The above protocol is in fact a layer 2. It means that it is completely independent from what the primary blockchain is: it only exploits its primary characteristics. Revo exists also in its enterprise version dedicated to big Companies: is a blockchain working on PoA protocol (Proof Of Authority), designed and optimized down to the smallest detail to guarantee over 10,000,000 transactions per second for intesive use case scenarios.

This does not mean that the SideChains will be a closed environment, far from it. The entire source code of the Smart Contract will be made open source to allow any existing blockchain to self-notarize on Revo, using a native environment with minimal transaction and data saving costs.

2.7.2 Speed, scalability and TPS

The battle for a scalable solution is the blockchain's moon race. Bitcoin processes 4.6 transactions per second. Visa does around 1,700 transactions per second on average (based on a calculation derived from the official claim of over 150 million transactions per day). The potential for adoption is there but is bottlenecked currently by scalability.

A study published by Tata Communications in 2018 showed that 44% of organizations in its survey are adopting blockchain, but also alludes to the universal problems that arise from deploying new technologies. From an architectural level, the unsolved problem of scalability is emerging as a bottleneck to blockchain adoption and practical applications.

As Deloitte Insights puts it, "blockchain-based systems are comparatively slow. Blockchain's sluggish transaction speed is a major concern for enterprises that depend on high-performance legacy transaction processing systems." The world received a taste of the scalability problems in 2017 and 2018: severe transfer delays and high fees on the Bitcoin network, and the notorious Cryptokitties app that congested the Ethereum blockchain network (a network that thousands of decentralized applications rely on).

In order to scale a blockchain, increasing the block size or decreasing the block time by reducing the hash complexity is not enough. With either method, the ability to scale reaches a ceiling before it can hit the transactions necessary to compete with businesses like Visa, which "handles an average of 150 million transactions every day" or around 1,736 transactions per second (TPS).

By comparison, Bitcoin transaction speeds are significantly lower. Currently, the block size is set to 1MB (1,048,576 bytes — although through SegWit, that size can scale to up to a theoretical 4MB) and the average transaction size is 380.04 bytes (assuming that each transaction is from one wallet to x other wallets — so a batch transaction would count as one transaction. I'll talk more about batch transactions later and why I labeled it this way) and seems to be on the rise.Therefore, the average amount of transactions that can fit into one of Bitcoin's blocks, currently, is calculated as:

$$\#\ of\ Transactions\ per\ Block = \frac{Block\ Size\ in\ Bytes}{Average\ Transaction\ Size\ in\ Bytes} = \frac{1{,}048{,}576}{380.04} \cong 2{,}759.12$$

The current Bitcoin block generation time is 10 minutes; i.e., every ten minutes, a new block is mined. In ten minutes (600 seconds), Bitcoin can average around 2,759.12 transactions based on previous assumptions. In other words, the Bitcoin blockchain can currently guarantee only 4.6 transactions per second

Revo implements a fully dynamic and scalable block size, thanks to the decentralized onchain governance protocol. Thanks to a very precise consensus mechanism, the blockchain itself is able to correctly size the block size from a few bytes up to a few tens of megabytes.

By default, the maximum size per block is 2,000,000 bytes, with an average transaction weight of around 320 bytes, along with block spacing of just 30 seconds, Revo can include up to 6250 transactions in a single block, which, compared to Bitcoin leads to a share increase of 1360%, with a theoretical TPS of over 210 validations per second.

Should the need arise to scale in terms of TPS, the community can freely and independently propose and vote on raising the maximum limit for block sizes through the OGP protocol. Given the importance of keeping revo as decentralized as possible, the only physical limitation in terms of scalability is the only network latency between network nodes.

PoA Sidechains

Proof of Authority (PoA) is a reputation-based consensus algorithm that introduces a practical and efficient solution for blockchain networks (especially private ones). The term was proposed in 2017 by Ethereum co-founder and former CTO Gavin Wood.

The PoA consensus algorithm makes use of the value of identities. This means block validators stake their reputation instead of coins. As a result, PoA blockchains are protected by validation nodes which are arbitrarily selected as trusted entities.

The Proof of Authority model relies on a limited number of validators, making it a highly scalable system. Blocks and transactions are verified by pre-approved participants, who act as system moderators.The PoA consensus algorithm can be applied in a large number of scenarios and is considered a viable option for logistics applications. As regards supply chains, for example, PoA is considered an effective and adequate solution.

The Proof of Authority model allows businesses to maintain their privacy and at the same time take advantage of the benefits of blockchain technology. Microsoft Azure is another example of a company applying PoA. In a nutshell, the Azure platform provides solutions for private networks, with a system that does not require a native currency such as ether's 'gas', since the network does not need mining.

2.8 Decentralized Domain System

Self sustained DDS

The domain name system (DNS) is a part of the internet's plumbing users may not often think about unless it stops working. It's a different story for web hosting providers and site owners; they deal with DNS directly because they depend on it to translate human-friendly web addresses into machine-friendly IP addresses. Every website has a domain name registered with a domain name registrar.

The registrars work with registry operators, which manage registries—databases of domain and registrant information— and top-level DNS servers. At the root of the tree is IANA, the Internet Assigned Numbers Authority. IANA is administered by ICANN, the Internet Corporation for Assigned Names and Numbers. It maintains the root zone files and delegates domain name management of top-level domains like .com to registry operators.
It's a complicated hierarchy, and for the most part, it works well. There are, however, weaknesses with this system, which was invented in 1983, almost a decade before Tim Berners-Lee published the first website.

When top-level DNS servers go down, so do large chunks of the web, which happens with alarming regularity. The system depends on the trustworthiness of registrars and registry operators, and it's a weak point criminals and censorious governments can attack.

A decentralized domain name system is a possible solution, and blockchain-based DNS looks like the most promising candidate in 2022. Decentralized DNS isn't in a position to take over from the centralized DNS we're all familiar with just yet. But it's worth understanding how it works and the role it could play in bringing resilience and independence to one of the most centralized and hierarchical aspects of the internet's infrastructure.

Decentralized domain name projects aim to remove DNS's dependence on ICANN and the registries. Blockchains, the technology Bitcoin is based on, are one way to achieve this. A blockchain is a distributed public ledger—a database duplicated across many computers. Blockchains are organized into sequential blocks of data where each block is connected to the previous and subsequent blocks.

In the case of Bitcoin, the blockchain acts as a decentralized record of transactions, but it's easy to see how this could replace some DNS functionality. Instead of registering a domain name with a registrar, you would register it on a blockchain. Because blocks are ordered and the blockchain is distributed, no one can register a name twice, just as they can't spend the same bitcoin twice.

Decentralized DNS systems don't aim to replace every part of the domain name system. Instead, they act as alternate roots. Much of DNS is already decentralized. Anyone can use cPanel, Plesk or ISPConfig to set up an authoritative domain name server for their own domains. However, the registries are centralized, and one organization manages the root zone file. That's why you have to register domain names with a registrar; they're agents of the central authority. It's also why you pay regular renewal fees. A centralized global naming system is expensive to run.

We're in the early days of decentralized DNS, and there are several active projects with similar aims. Namecoin was one of the first. It was released in 2011 but hasn't seen widespread adoption. Unstoppable Domains is another entry in the field. Handshake is an interesting new contender which bills itself as a "decentralized naming and certificate authority."

Like the other decentralized naming systems, Handshake is a blockchain-based root zone alternative with an interesting solution to a problem that plagued earlier efforts—domain squatting. It was easy to register any domain, so squatters gobbled up tens of thousands they never intended to use. Handshake, in contrast, uses an auction to allocate domains.

Like Bitcoin, the Handshake blockchain uses a proof-of-work "mining" system to add new blocks, generating a coin called HNS. HNS coins are used to bid in Vickery auctions for top-level domains. For the same reason, Handshake-registered domains do have associated renewal fees.

Decentralization is the primary motivation behind blockchain-based domains, but there are other potential benefits.

- Anonymous — Just as Bitcoin transactions are anonymous, so are blockchain-registered domains.

- Censorship resistant — A centralized DNS system is vulnerable to censorship. The operating authority could be influenced to remove registered domains from the registry. Blockchains are distributed, and no single entity controls them, making censorship much harder.

- Secure — You might have noticed that Handbrake also calls itself a "decentralized certificate authority." Today, we rely on centralized certificate authorities and SSL certificates to verify the identity of sites we connect to. Because they are practically tamper-proof, blockchains can perform the same function. Additionally, CAs can be hacked or subverted, something that's much harder to achieve on a distributed blockchain.

The use of ERC721 Tokens in the form of digital assets, including for the proof-of-possession purposes in real life is being actively discussed today. However, smart contracts work much better with digital entities (especially those existing only within a smart contract environment). In this case it can really manage them with no need to have an intermediate layer to manage real world assets from the blockchain and control thereof.

Domain name is an unconditional value of the digital world. Domain names that sound good and give people a strong idea of what activity a website is about, can be sold or bought for several hundred of thousand, and even million dollars. The DNS itself is in fact a type of address book, a registry which keeps records of domain names and servers related thereto. And, as long as blockchain is a distributed registry, it is very well suited to a fully decentralized DNS, so no supervision on the part of zone owners and regulators is required.
In turn, being the completely digital tradable assets, domain names are ideally suited to be ERC721 Tokens: they are unique (each domain name is unique), have their own value and can be sold or transferred from one owner to another.

Here is how it works on Revo:

- When registering a domain name on the Revo blockchain, you receive an ERC721 Token identified by the hash of the domain name (converted into a uint256). The token contains the owner's wallet address and the textual domain name

- The smart contract system also enables configuration of the addresses of the domain servers.

- Once received, you can store the token and accordingly use the domain name, transfer it to another person or put it up for sale on any exchange that works with ERC721 Tokens.

2.9 Decentralized storage

Virtual Datacenter

With the rising interest in blockchain technology, interest has also risen for the one killer Blockchain app. We believe that the blockchain killer app will be decentralized storage technology.

From solving our challenges of safely storing data to not having all of our personal info in the hands of a few monolithic entities, decentralized storage has the potential to be both disruptive and help usher in even greater use of blockchain technology.

When it comes to data storage, here are our options:

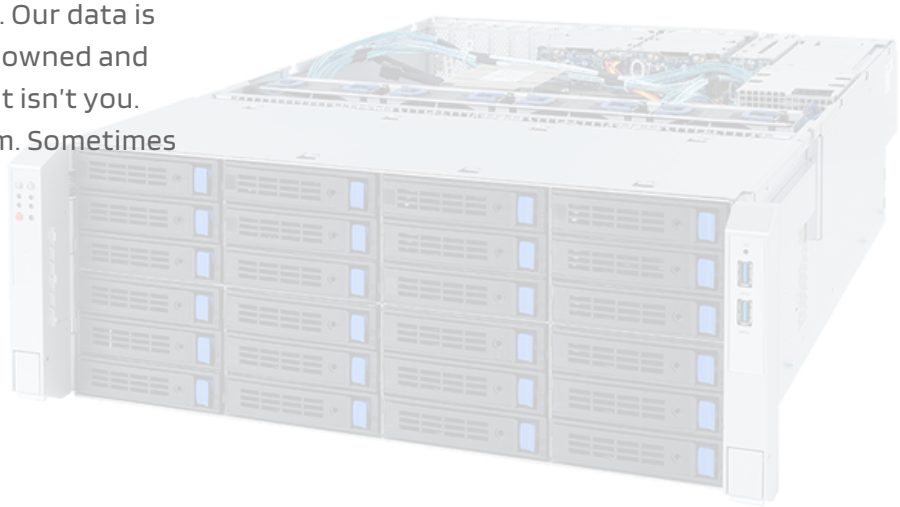
- Physical media. Think HDDs to share films with friends or USB thumb drives for small file storage.

- Centralized cloud storage. Our data is hosted on a central cloud owned and operated by someone that isn't you. Your data belongs to them. Sometimes it isn't even safe.

On the other hand, decentralized cloud storage is where data is stored on a decentralized network across multiple locations by users or groups who are incentivized to join, store, and keep data accessible.

The servers used are hosted by people, rather than a single company. Anyone is free to join, they are kept honest due to smart contracts, and they are incentivized to participate by getting coins as rewards

Thanks to the integrated technology on Revo, it will also be possible to create private instances and customized shared storage pools.



There are several reasons for the advent of decentralized storage over centralized cloud storage.

- Data breaches: Just about all the major players have had data breaches in the last few years.
- Data outages: Dreaded DDoS attacks can leave you and millions of others without data.
- Rising storage costs: This means high bandwidth transmission costs, as well as increased data security costs as centralized storage, is easier to attack.
- Lack of ownership: Your personal private data is not owned only by you.
- Censorship and monitoring: While there are some benefits associated with this, many people disagree with censorship and surveillance especially if it approaches Orwellian levels.

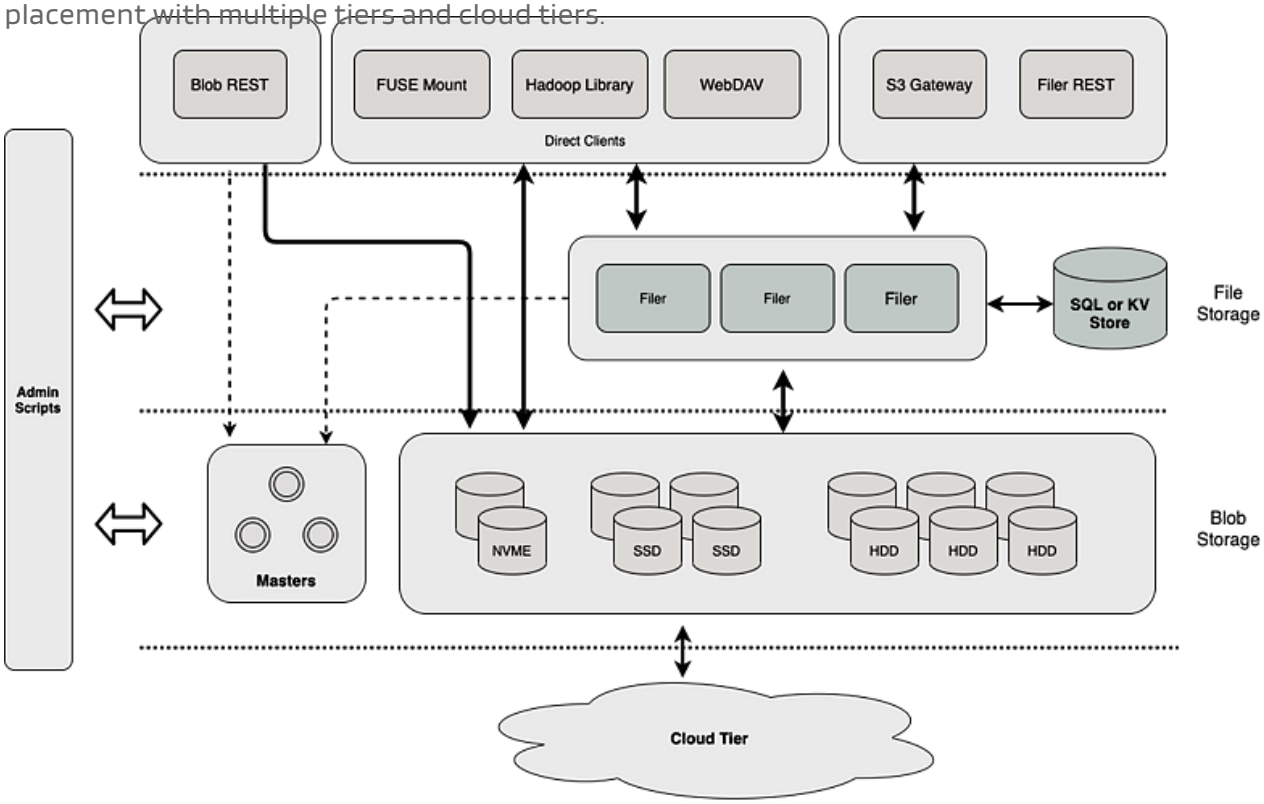
Furthermore, with the industry expected to reach 101 $billion+ by 2023, there is a significant need for these problems to be solved. We, like many others, believe decentralized cloud storage can do that.

Decentralized storage means the files are stored on multiple computers (called nodes) on a decentralized network. Like with conventional cloud storage, when you need a file, you can request it and receive the file. Requesting your file works similarly to BitTorrent and other P2P clients where you download fragments of that file from participants in the network until you have the full file.

But that doesn't mean those holding your files can read them. Instead, decentralized storage automatically encrypts files and only you hold the encryption key, guaranteeing your files can only be read by you. Furthermore, through a process of sharding, no single person holding your files has the entirety of it, thus adding an extra layer of security and protection.
Unlike centralized cloud storage which keeps data in a central point based on a location that might not be near you (resulting in users competing for bandwidth), the nature of decentralized storage means data distribution and retrieval is handled by nearby peers regardless of physical location. This results in higher transfer speeds due to utilizing local network bandwidth.

2.9.1 Model technology

The software behind Revo's virtual datacenter system is SeaweedFS a completely open source project developed by Chrislusf. It's a distributed storage system for blobs, objects, files, and data. A data warehouse with predictable low latency with O(1) disk seek, and flexible data
placement with multiple tiers and cloud tiers.



SeaweedFS is built into multiple layers.

- Blob Storage consists of master , volume servers, and cloud tier.
- File Storage consists of the Blob Storage and filer servers.
- Object Storage consists of the File Storage and S3 servers.
- Data warehouse consists of the File Storage and Hadoop compatible libraries, used by HDFS, Hadoop, Spark, Flink, Presto, HBase, etc.
- FUSE Mount consists of the File Storage mounted to the user space on clients, used in common FUSE mount, Kubernetes persistent volume, etc.

SeaweedFS is:

- A fast key to file mapping with O(1) disk seek.
- A customizable tiered storage placing data on demand.
- An elastic storage system that offloads less active data to cloud.
- A scalable file system to replace HDFS.
- A high-performance in-house S3 compatible object store.

The advantages of SeaweedFS include:

High data and service availability:

- No single point of failure
- Supports Active-Active asynchronous replication
- Supports Erasure Coding
- Supports file checksum
- Supports rack and data center aware replication
- Supports metadata backup and replication

Optimized for performance:

- Optimized for lots of small files. Each file overhead is 40 bytes. SeaweedFS Architecture 3 Always O(1) disk read, even for Erasure-Coded data
- Linear scalable. No HDFS name node bottleneck
- Clients access data directly on volume servers
- File servers are accessed for meta data
- Place data by requirements to custom disk types, e.g., NVME, SSD, HDD

Simple operations Just add volume servers to increase capacity.

Volume Server

The volume servers stores a bunch of volumes. Each volume defaults to 30GB. The disk space can be pre-allocated. All the writes are append only. The volumes are compacted periodically. So there is not much disk space wasted.

Each volume can contain lots of files. Each file is indexed by its offset in a separate volume index. So each file read request will just read the in-memory volume index for the offset and size, and then read the volume file with a single disk seek.

Volumes can have different replication settings. Each write to a volume will be replicated to its peers with strong consistency. If any replica fails to write, the whole request fails. Volumes also have different TTL settings. The TTL volumes are not compacted, but just purged as a whole if all the entries in a volume past the TTL.

Volumes can be tagged as different disk types, such as SSD, HDD, or actually any tags, such as NVME, fastHDD, slowHDD. The data is placed according to the write request requirement. The admin scripts can move the data to other tiers.

Master Server

The master servers track volume locations on all of the volume servers. This information is dynamically collected as soft states and never persisted. This info is provided to clients as a DNS to locate each volume.

Plan on Revo integration

The SeaweedFS integration plan into Revo sees the object storage mode as the primary focus. To guarantee a complete decentralization and autonomous management via smart contract, the aforementioned distributed DNS system will take care of being the connection point between master servers and volume servers.

The nodes that want to contribute to the storage network will be able to participate in it by initially creating a network identifier (in our case a decentralized domain), with which they will choose whether to become a master server or a volume server.

However, there are minimum requirements depending on the type of node chosen. It is very important that both types of nodes have good network connectivity via cable and that they are able to withstand a few hours even in the event of a blackout, therefore a UPS is seen as necessary.

It will be essential to have a static and public IP address with NAT 1: 1 for the correct routing of data packets.

New startup flags will be implemented directly in the revo daemon code:

--storage-enable= true / false
This command allows you to enable the storage functionality on your Revo node. This command is launched to allow the daemon to install and configure all the libraries necessary for the proper functioning of the storage system

--storage-upgrade
Command required for storage software LTS update (Long Term Support)

--storage-issue-new= master / volume
Startup command that starts the wizard that allows the miner to create a unique identifier based on the type of storage mode chosen. At the end of the procedure, a storage.conf file will be created in the .revo folder (or% AppData% / Roaming / Revo on windows) containing the complete configuration for storage mode.

--storage-mode= master / volume
Start command that specifies how the daemon will be run.

--storage-path= path
Needed to specify which directory to allocate to storage mode.

--storage-bind= public IP: PORT
Command to customize interface and the public network port

In addition to these basic commands, specific functions will be implemented where each individual user can personalize the amount of space (in gigabytes) to be made available, the amount of volumes to be pre-generated, etc.

2.9.2 Public and Personal storage pools

Basically, the storage mode on Revo is created specifically for a type of public and shared use which allows it, through a complex reward mechanism, to make storage space available for everyone. Thanks to the intrinsic functionality of SeaweedFS, it will also be possible to start the storage daemon in offline mode, and create storage pools and data sharing locally, taking full advantage of all of the native features of SeaweedFS

2.9.3 Reward system

The reward system for the storage mode is entirely managed by smart contract code. Thanks to the work done in unison by the volume server and master server, the owners will receive tokens as remuneration for the service based on:

- uptime
- amount of allocated storage space
- long-term conservation
- data transferred / served
- network reliability

The task of the master servers will also be to redirect data backup requests to the closest nodes (with lower latency), to ensure content redundancy and network reliability.

2.9.4 Objective

This type of distributed management allows the creation of a public environment with a precise system of virtually unlimited space, capable of handling and sharing any type of file, in an encrypted and redundant manner. The files will therefore be accessible at any time and from anywhere in the world making it censor free.

3. Governance

On Chain Governance Protocol (OGP)

The word Governance is usually used when speaking of a small circle of actors who have the task of managing the operation of a system or organization in its entirety. However, it does not necessarily have to mean centralization.

As a decentralized public chain, Revo Blockchain regards blockchain governance as an important aspect of achieving sustainable development. The governance model of Revo includes two main aspects.

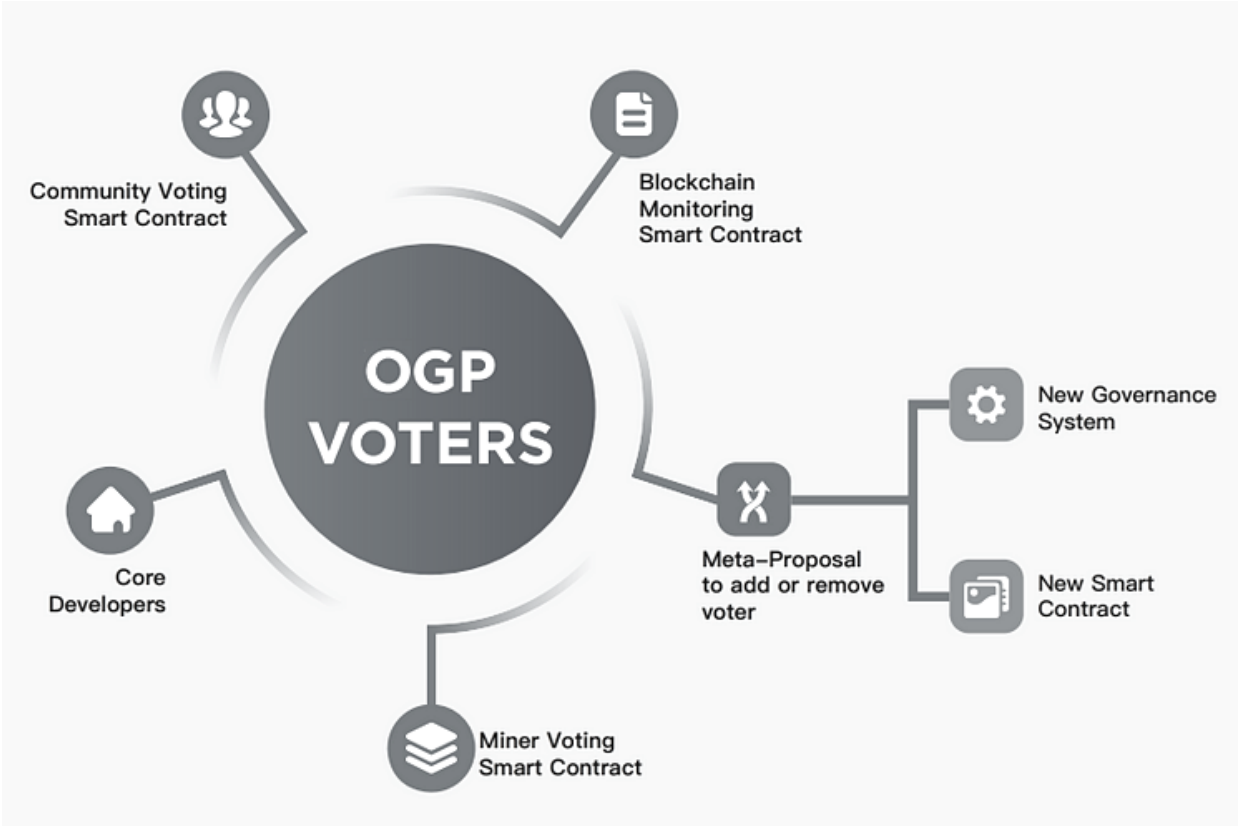
One is on-chain governance which uses OGP, the other is off-chain governance, which is established in code. These values are considered default values

Through the introduction of OGP and the establishment of the Revo Foundation, the blockchain applies both human governance and code governance to the public chain, thereby realizing the decentralization of blockchain governance and effective governance decision-making.

The core character of OGP is that in addition to allowing RVO holders to participate in the voting and negotiation of the upgrade and iteration of the blockchain network itself, it also introduces a way for other participants in the ecosystem, including developers, community member representatives, miners, and other multi-party participants to propose and vote for on-chain governance proposals.

3.1 On chain shared Governance Protocol

OGP manages the parameters of the blockchain network through smart contracts embedded in the genesis blocks and clarifies the governance seats and proportion of governance participants for each party. Any participant can initiate a proposal, and the type of proposal includes the increase of management or governance seats, deletion, modification of common network parameters, etc. Participants with governance seats vote on the proposal, decide whether the proposal is approved, and execute the approved proposals through smart contracts.



The on-chain governance mechanism on the OGP is efficient and automatic.

It can realize the automatic upgrade and continuous update iteration of the Revo blockchain consensus through real-time effective decision-making and execution mechanisms.

At the same time, the on-chain governance process is public and transparent, and the process is easy to audit and traceback, which helps to ensure the fairness of the entire governance process and improves decision-making efficiency without worrying about the technical and social impact of a soft and hard forks on the network system.

3.2 Democratic Actors

As introduced above, the OGP smart contract protocol is a common consensus mechanism that is composed of a well-defined number of actors. For obvious reasons, the first actor is the owner of the contract (in our case the Revo Foundation) who has the right to add and identify a new actor.

In addition to the Foundation, other main types of actors are:

- Core Developers
- Other Foundations
- Schools - Universities
- Institutions
- Research centers
- Community representatives
- Key Partners

Each actor is identified with its own specific address and carries with it well-defined characteristics. For example, a malevolent actor can also be inhibited, through a common vote by the community. Depending on the type of actor, the voting power changes: an entity such as the Revo Foundation, a core developer or a university, will have more authority when voting for a proposal. At the same time, however, this authority is counterbalanced by the voting power of the members of the community: this guarantees fairness in any case.

3.3 Consensus proposal

To propose a change to a consensus rule, it is necessary to draw up a smart contract (based on an already defined model) in which the new rules that the proponent wants to change are written. First of all, this smart contract must be filled in and published in the blockchain from the proposer's address (this avoids hijacking during the forwarding of the proposal to a malicious smart contract not written by the proposer himself). The proposer will attach the address of the smart contract just published to the transaction that will propose the change of consensus to the OGP smart contract.

The OGP will automatically initiate a vote which, once the quorum of 51% is reached, will close successfully. If the outcome is positive, the consent parameters will automatically change for the entire network at the next block, otherwise the proposal will be rejected.

At the moment, the consensus parameters that can be changed following a joint vote are the following:

- blockGasLimit (How much gas is allowed at maximum to be spent inside a single block)
- blockSize (The upper size limit, in bytes, for a single block)
- gasSchedule (EVM gas pricelist - regulates all smart contract operations prices)
- minGasPrice (Minimum allowed units of gas for broadcasting a contract transaction)

3.4 Scalability

The OGP is a shared method of ensuring the scalability of the Revo protocol. If the blockchain network were under stress for any reason or simply there was a need to scale to increase the performance of the consensus mechanism, the community could do so, at any time.

3.5 Attack mitigation

Another aspect to take into consideration is the possibility for the community to mitigate a possible attack on the primary blockchain.
Let's take, for example, an attacker who wants to enlarge the blocks by filling them with spam transactions through smart contracts (perhaps to prevent the execution of transactions by other users). Once identified and analyzed, through the OGP it would be possible to increase the cost in terms of gas for a specific type of operation, depleting the attacker's RVOs and effectively ending the attack. Later another proposal would return the parameters to their previous values.

4.Economic model

There is no PoS without PoW

As we understood, the block validation protocol on Revo is the PoS (Proof Of Stake), if we want to force it we could further simplify (by making a comparison with Bitcoin) that the quantity of coins of the validator node are like the miner's hashrate. The more coins owned (and therefore of valid UTXOs), the higher the possibility of being selected by the network to create a new block. But if you need coins to validate the blocks, what happens to the genesis (block 0)?

What few people know is that each PoS coin has a small epoch (usually between 1000 and 5000 blocks) during which the initial coins are generated with a mechanism identical to Bitcoin's Proof Of Work. It is extremely important that at the end of this period the UTXOs generated are mature and valid for the change of consensus to PoS.

Generating few coins, and consequently few valid UTXOs, would be very risky in terms of security. Few UTXOs expose the network to a risk of blocking: if there are not enough mature transactions for staking, the blockchain would stop (Nothing at stake error) and there would be no alternative solution other than starting again from scratch.

On the other hand, generating too many UTXOs could lead to too high an increase in staking difficulty, significantly slowing down the performance of the blockchain itself.

Revo, during its premine phase, will generate approx 100,000,000 new RVOs, divided into 20,000 UTXOs in 5,000 blocks before fully switching to PoS consensus.

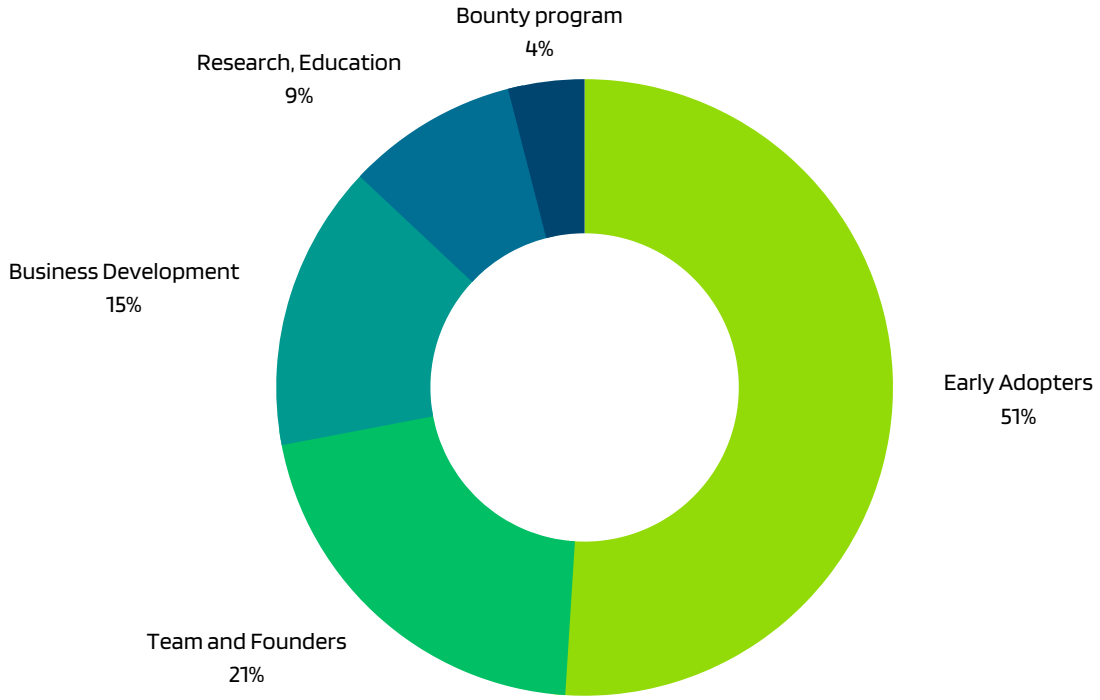
This initial supply of 105 million RVOs is distributed with the aim of growing the community around Revo and promoting the decentralization of the system.

Of the initially created coins, 51%, or 53,550 million RVOs, will be allocated for validators and early node adopters in a single locked smart contract that will regulate free airdrop distribution. All allocation will be distributed to node adopters. Revenue from the physical and virtual node sales from RevolutionChain Italy funds the constitution of the Revo Foundation, including system development, marketing, financial and legal consulting.

24%, or 25,2 million RVOs, will be used for commercial and community development, academic research, education, and market expansion. Of this, 15% will be used for business development, including expansion of industry-related applications, supporting DApp (Distributed Application) development, business expenses (legal, compliance, accounting, consulting), marketing and public relations, and token swaps. The remaining 9% will be used to support academic research, developer education, promotion of Revo blockchain technology, and cooperation with the open-source community.

21%, or 22,05 million RVOs, will be allocated to the Founding Team, and Development Teams that will follow Revo blockchain development before (and after) it's source code release.

4%, or 4,2 million RVOs, will be allocated for bounty programs and community initiatives.



4.1 Initial RVO distribuition

Although not being able to talk about actual values and numbers (Revo is in early stage and does not yet exist on any exchange), the decision to deploy an initial set of nodes was not taken lightly or for commercial reasons. When you participate in an online airdrop, 99% of the time you redeem something that often doesn't even interest you, and like you, tens of thousands of other users. There is no contribution to the intrinsic value of the project by the claimers, who, after a future listing, will look forward to cashing out.

For the Revo network, on the other hand, whoever receives the coins will do so solely and exclusively for merit, tangibly supporting the network, its security and redundancy itself. This differentiates between a solid and a bad community (which is the thing we care about most at the moment).

Self Funding

Revo, the Development Team and the Foundation finance the work on the blockchain thanks to the services they build in the ecosystem. The distribution of RVOs is not linked to an ICO (Initial Coin Offering) nor to an IPO (Initial Public Offering). None of Revo's related counterparties will intend to undertake a public sale of RVO coins. Revo coin act as gas (RVO) and it's used to run the DApps (Decentralized Applications) that will be distributed on the platform. Selling physical and virtual Revo validators is our way to fund our project.

So how do you become a validator?
It is important to underline that Revo is not a permissioned blockchain, but a full permissionless one. The validators can at any time transfer RVO to other subjects, who independently (thanks to the open source code) have the immediate possibility to compile a wallet and become new validators. The model that has been established is seen as necessary for technical and operational issues which provide for the free transfer of RVO through a KYC (Know Your Customer) process.

Early Adopters can purchase a physical validator node and become eligible to receive a quantity of coins with which to participate in the PoS with a free airdrop. The quantity is chosen randomly and automatically between 1500 and 5000 coins by the same distribution smart contract). The code that governs the distribution system is open source and completely transparent.

Virtual VS Physical nodes

The physical nodes have been designed and structured to favor the decentralization of REVO in support of the ecosystem network:
they are created to be plug & play and with reduced power consumption, which can be positioned anywhere without the need for particular network or space requirements.
The connection to the network can take place via cable or WiFi.

Virtualized nodes, on the other hand, work in the same way and are managed entirely by our IT department directly in our Revo Datacenter. The difference between the two options is essentially entirely linked to expandability. The physical devices are in fact already prepared for the expansion of disk space, which can then be shared in support of the network (see Decentralized Storage).

Furthermore, the physical device has a one-off cost, while the virtualized node, at the end of the 18 months, is renewed on a monthly basis like a simple VPS server hosting plan.

More information regarding the purchase of validator nodes can be found at **revo.network**

4.1.1 Early Adopters

We can consider as Early Adopters all those who contributed to the initial start-up of Revo technology. Companies that have decided to develop on Revo in the initial stages, users who have purchased a validator node, etc.

This set of entities are the backbone of the Revo community, those who make the correct functioning of the blockchain ecosystem possible in its entirety, starting from the network nodes to the services present on the chain. For this reason 51% of the entire premine was dedicated to them.

Giving the amount allocated (53,550 million of RVOs), the plan is to distribute coins to a number between 34,000 and 10,200 decentralized validators.

There is also a small number of users, companies and partners who have actively contributed in the alpha and beta stages of Revo: they'll receive an extra bonus of 21 RVO for each validated block on the latest Alphanet chain at the prior condition that they switched to an official mainnet node.

4.1.2 Airdrop and KYC

While Revo is free and distributable software, to have validated access to the airdrop a physical or virtual node must initially be purchased from one of our trusted partners. This is because in order to send RVO coins and act as validators, for a first step it is necessary to complete the KYC process towards Revo. When users receive coins they get full control over them thanks to a wallet private key (which has to be kept in a safe place).

Please note that in any case Revo Team or Associated Companies will ever sell coins to Early Adopters. RVO coins are **GIFTED** to user as an incentive to keep the Revo Blockchain Network online.
You will be able to use REVO to take advantage of various features and utilities, such as distributed storage and enterprise products, create tokens, smart contracts and much more. When you purchase a node, you actually buy a fully functioning hardware/virtual vm system that has warranty, technical support and granted future updates.

Airdrop enrollment works by submitting the access token individual code to Revo from the node interface

4.2 Supply Schedule

Even if Revo was born as service chain, here in the headquarters we have decided to entrust the Revo blockchain with a completely different supply schedule from what has already been seen. We love playing with numbers. To honor Bitcoin, the blockchain from which we take the accounting model, we have marked the number 21. (Bitcoin has a max supply of 21,000,000 BTC)

The next link is made with the Fibonacci series, replacing the generic halving model, which is used by all other cryptocurrencies. The Fibonacci sequence is composed of a series of numbers, where the next number is given by the addition of the two numbers before it.

0, 1, 1, 2, 3, 5, 8, 13, 21 ...

One of the fascinating things about the Fibonacci sequence is the direct link to the Golden Ratio. The golden ratio or golden mean, represented by the Greek letter phi (ϕ), is an irrational number that approximately equals 1.618. The golden ratio results when the ratio of two numbers is the same as the ratio of their sum to the larger of the two numbers. When we take two successive numbers (one after the other) of the Fibonacci series, their ratio tends to approach ϕ.

This also aims to symbolize that Revo, over the years, wants to achieve perfection.

Revo has a time between blocks of about 30 seconds. This means that, theoretically-mathematically, two blocks are created every minute, every hour 120. Every day 2880 and every year around 1 million.

Consequently, according to the fibonacci series, the reward for each block changes every 1,1,2,3,5,8,13,21 years. Similarly, the reward of each block will start from 21 until it reaches zero, always following the Fibonacci series.

Blocks				Fibonacci			
from	to	Year	Changes	Block Reward	New RVO	Total RVO	Approx RVO/year
1	5000	2022	0	21000	105.000.000,00	105.000.000,00	n/a
5001	1000000	2023	0	21	20.895.000,00	125.895.000,00	20.895.000,00
1000001	2000000	2024	1	13	13.000.000,00	138.895.000,00	13.000.000,00
2000001	4000000	2026	2	8	16.000.000,00	154.895.000,00	8000000,00
4000001	7000000	2029	3	5	15.000.000,00	169.895.000,00	5000000,00
7000001	12000000	2034	4	3	15.000.000,00	184.895.000,00	3000000,00
12000001	20000000	2042	5	2	16.000.000,00	200.895.000,00	2000000,00
20000001	33000000	2055	6	1	13.000.000,00	213.895.000,00	1000000,00
33000001	>	2076	7	0	0,00	213.895.000,00	0

To ensure a very high distribution and ecosystem centralization, the amount of preminated coins linked to Team and Founders, Business Development, Research, Education and Bounty will not be used for staking.

Given also the objective of avoiding any type of initial centralization of the Revo blockchain, only a small part of the Business Development allocation can be used by the Development Team to keep the blockchain active in the early stages (See avoiding nothing at stake error).

An important fact is that the Early Adopters allocation (both Beta / Alpha and Early) will not be available forever. The possibility of claiming the RVOs for these allocations is identified in 1 year for the first bracket, and in 2 years for the second. Any leftovers will inevitably be blocked and sent to a transparent burn address.

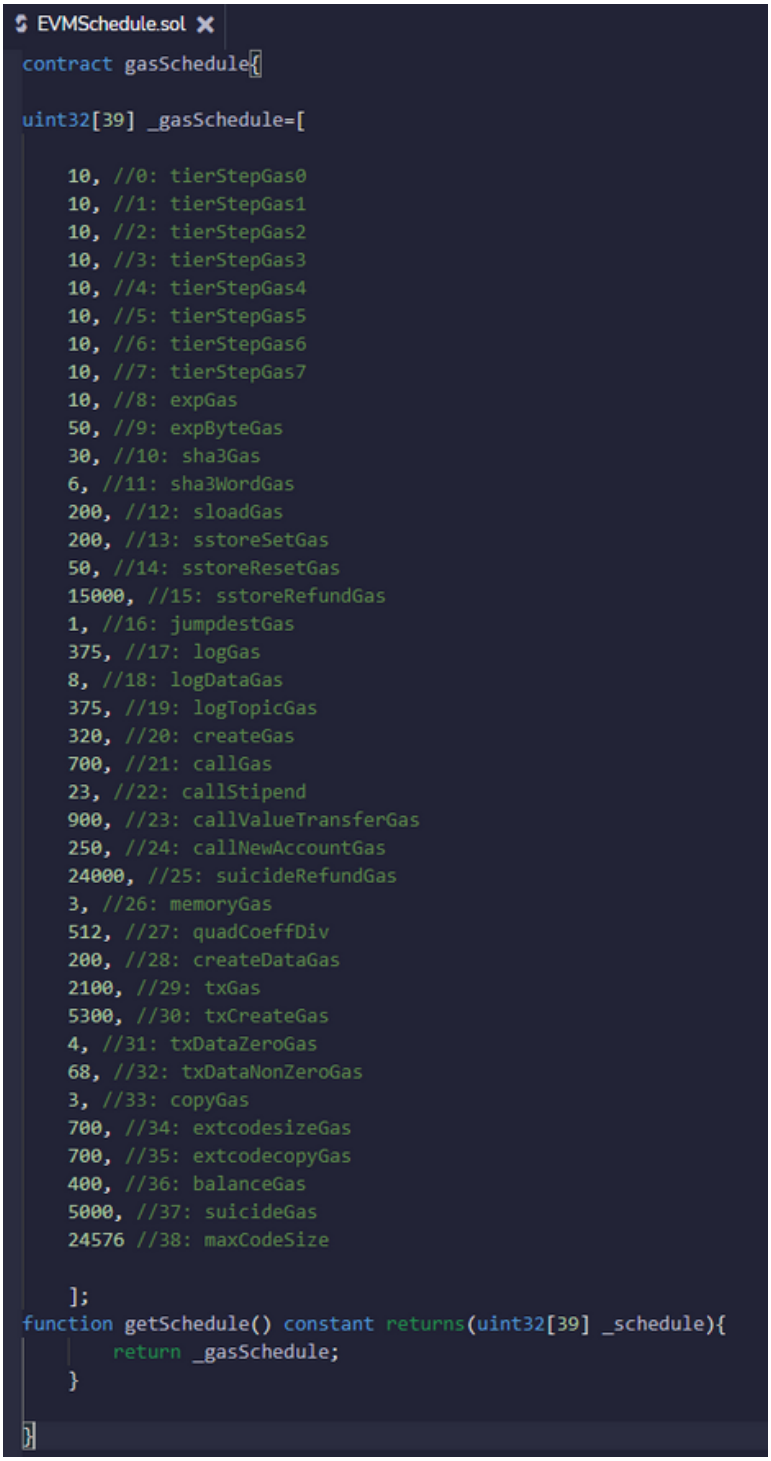
Even if taken for granted, given the above scheme, the new RVOs will over time exceed what was initially pre-allocated for the initial premine.

4.3 EVM Schedule

A blockchain like Revo needs to allow the Companies and the Community that use it an efficient and inexpensive way to send Smart Contract transactions. For this reason the EVM schedule (i.e. the one that in less technical terms is compared to a real gas pricelist for contract operations) starts with very low costs (For this reason, to avoid spam attacks and for the establishment of the Foundation, Revo starts such as Closed Mainnet).

This will allow not only the DApps that have now been forced to stop operations due to costs to return fully operational, but also to bring to light the connection with the SideChains: blockchains dedicated to Enterprise use (Triton blockchain upgrade).

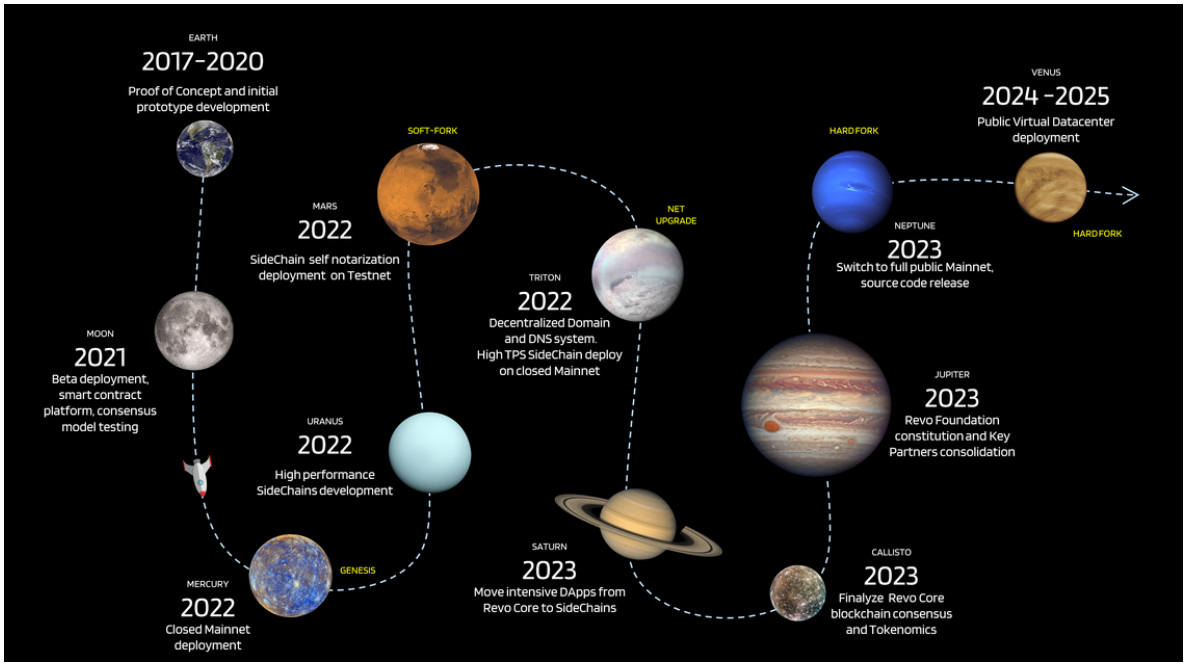
At the end of this update, the EVM schedule will be re-adjusted to allow progress towards the Neptune upgrade, which will see the complete release of the Revo source code to the public.



5. Roadmap

There is still a long way to go

Notwithstanding that the dates visible in this roadmap are indicative, and for obvious reasons they will never reflect the exact reality, Revo will follow a very tortuous development path, which we have tried to summarize in a few points below.



EARTH
Phase in which Revo was conceived, during which the first feasibility, functional and prototyping studies began.

MOON
Launch of betachain and alphachain, creation of ecosystem and Smart Contract platform, consensus and model testing.

MERCURY
Launch of the Closed Mainnet.

URANUS
High performance SideChains development, self-notarization system for secondary blockchains.

MARS
SideChain units deployment on Testnet.

TRITON
Initialization of the decentralized domain system (DDS) and deployment of High TPS SideChain on the closed mainnet.

SATURN
Moving DApps from Revo Core to SideChains.

CALLISTO
Finalize Revo Core, consensus rules and tokenomics in preparation for the public release of the sources.

JUPITER
Establishment of the Revo Foundation and consolidation of the Key Partners.

NEPTUNE
Full switch to public mainnet with full source code release.

VENUS
Public integration of the distributed storage system (Virtual Datacenter)

future development

6. Revo Foundation

Soul of ecosystem development

The Revo project was started by a group of developers in 2017.
As has been extensively discussed in previous chapters, revo has been designed to be geared towards industrial applications, supply chain traceability, notarization, etc.With this in mind, the first part of its life will be dedicated to strengthening the decentralization of the network, the distribution of revo initial supply and the creation of a set of applications that will then allow an autonomous life in the subsequent phases.

For this reason, revo will initially be distributed as compiled code, and to some extent controlled by the development team.

However, this is in no way meant to be a long term goal.

Revo is a public, open, distributed and transparent blockchain.On this basis, the creation of the Revo Foundation is planned.The Revo Foundation will be a non-profit organization dedicated to supporting and maintaining Revo and its related technologies. It is not a lucrative Company, nor a traditional non-profit one.

Its role won't be to control or lead Revo, and it won't be the only organization funding the critical development of Revo-related technologies.

WIP

The Foundation will be a keystone of the ecosystem and will take care of free training initiatives, events and seminars. It will also have the role of encouraging, proposing and helping innovative startups and projects considered interesting for the ecosystem to complete them or / and finance them.

Moreover the establishment of the foundation will be a fundamental milestone for revo, as it will be complimentary to the release of the source code.

The establishment of the Revo Foundation is one of the objectives that RevolutionChain sets itself for 2023/2024 and it will in fact be one of the fundamental points for the expansion of the project, in conjunction with the Neptune update. For this reason, this chapter is still work in progress.

6. Sustainability

The importance of a clean ecosystem

As we all know, the most famous and widespread energy-intensive blockchains such as Bitcoin, Ethereum, Litecoin are supported by a PoW (Proof of Work) validation protocol. Taking Bitcoin for example, we can imagine the activity that miners do as simply generating random hashes at maximum speed to satisfy a certain type of criteria. This process is carried out by dedicated machines (ASIC, FPGA or GPU) consuming huge amounts of energy. These criteria are dictated by the blockchain taking into consideration values such as the current generation difficulty and the time interval of the previous blocks.

In general, the validation protocol of a blockchain keeps time by adjusting the mining difficulty from time to time based on the speed with which the previous blocks were created. Consequently, it is understood that as the competition between miners increases, the difficulty increases and if the difficulty increases, the energy needed to generate new blocks increases.

On the contrary, Revo, thanks to its PoS (Proof of Stake) protocol, regulates the validation of blocks through an almost entirely energy free system that we can compare to a lottery.

In Revo, any coin holder is in fact a validator, any UTXO greater than 100 coins (upon reaching maturity), is considered a lottery ticket. The internal protocol, called "Staker", does nothing but constantly cycle through the UTXOs present in the wallet of the validator and, by calculating the hash based on the current timestamp of the node, check if it satisfies the aforementioned criteria of difficulty and blocktime.

This understandably leads to an almost total reduction (99.99%) of the electricity consumption necessary to validate blocks of transactions. The fact that the entire Revo software eco-system is able to operate at full speed validating blocks and transactions on a device like the Raspberry Pi Zero consuming 80mA / h (0.4 Watts) helps us understand how much Revo is an almost completely zero impact blockchain. .

Revo has, among its aims, to be an accessible blockchain to develop supply chain traceability systems. The blockchain has positioned itself as a revolutionary element on the side of environmental sustainability (for example, guaranteeing the origin and transparency on the certified organic food supply chains).

Using an energy-intensive blockchain to track organic or zero-kilometer products would be an oxymoron: this is why Revo will be the solution.

External references

1. A.M Antonopoulos. Mastering bitcoins, 2014.
2. I. Bentov, A. Gabizon, and A. Mizrahi. Cryptocurrencies Without Proof of Work, pages 142–157. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016. 3.
A. Biryukov and D. Khovratovich. Equihash: Asymmetric proof-of-work based on the generalized birthday problem. Proceedings of NDSSˆaˇA´Z16, 21–24 February 2016, San Diego, CA, USA. ISBN 1-891562-41-X, 2016.
4. B. Bisping, P.D. Brodmann, T. Jungnickel, C. Rickmann, H. Seidler, A. St¨uber, A. Wilhelm-Weidner, K. Peters, and U. Nestmann. Mechanical verification of a constructive proof for flp. In International Conference on Interactive Theorem Proving, pages 107–122. Springer, 2016.
5. Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. Proof-of-personhood: Redemocratizing permissionless cryptocurrencies. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pages 23–26. IEEE, 2017.
6. O. Bussmann. The Future of Finance: FinTech, Tech Disruption, and Orchestrating Innovation, pages 473–486. Springer International Publishing, Cham, 2017.
7. C. Cachin. Architecture of the hyperledger blockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016.
8. Krishnendu Chatterjee, Amir Kafshdar Goharshady, and Arash Pourdamghani. Hybrid mining: exploiting blockchain's computational power for distributed problem solving. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pages 374–381. ACM, 2019.
9. K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the internet of things. IEEE Access, 4:2292–2303, 2016.
10. Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin G¨un Sirer, et al. On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security, pages 106–125. Springer, 2016.
11. P. Dai, N. Mahi, J. Earls, and A. Norta. Smart-contract value-transfer protocols on a distributed mobile application platform. URL: https://qtum. org/uploads/files/cf6d69348ca50dd985b60425ccf282f3. pdf, 2017.
12. Daniel Ferreira, Jin Li, and Radoslawa Nikolowa. Corporate capture of blockchain governance. Available at SSRN 3320437, 2019.
13. Johannes G¨obel and Anthony E Krzesinski. Increased block size and bitcoin blockchain dynamics. In 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), pages 1–6. IEEE, 2017.
14. A. Kiayias, I. Konstantinou, A. Russell, B. David, and R. Oliynykov. A provably secure proof-of-stake blockchain protocol, 2016.

15. Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC
conference on computer and communications security, pages 254–269. ACM, 2016.
16. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012):28, 2008.
17. A. Ouaddah, A.A. Elkalam, and A.A. Ouahman. Towards a Novel PrivacyPreserving Access Control Model Based on Blockchain Technology in IoT,
pages 523–533. Springer International Publishing, Cham, 2017.
18. Fahad Saleh. Blockchain without waste: Proof-of-stake. Available at SSRN 3183935, 2019.
19. P. Serguei. A probabilistic analysis of the nxt forging algorithm. Ledger, 1:69–83, 2016.
20. Voshmgir Shermin. Disrupting governance with blockchains and smart contracts. Strategic Change, 26(5):499–509, 2017.
21. P Vasin. Blackcoin's proof-of-stake protocol v2, 2014.
22. M. Vukolí c. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In International Workshop on Open Problems in Network Security,
pages 112–125. Springer, 2015.
23. M. Vukolí c. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication,
pages 112–125. Springer International Publishing, Cham,
2016.
24. Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. A survey on consensus
mechanisms and mining strategy management in blockchain networks. IEEE Access, 7:22328–22370, 2019.
25. G. Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014.
26. Xiwei Xu, Ingo Weber, and Mark Staples. Architecture for blockchain applications. Springer, 2019.
27. Matthew A Zook and Joe Blankenship. New spaces of disruption? the failures of bitcoin and the rhetorical power of algorithmic governance. Geoforum,
96:248–255, 2018.
28. The top-five enterprise blockchain priorities for 2022 - Blog - DigitalAsset.com
29. SeaweedFS - Github.com 2022
30. Bitcoin Whitepaper - 2022
31. Qtum Whitepaper - 2022
32. Zcash Whitepaper - 2022

WHITEPAPER

Initial Release

Feb 2023

Written by
RevolutionChain Italy

revo.network