Frozen Network

FAST.SECURE.RARE

A scalable, high-performance, low-cost, decentralized encryption currency and block chain

V.2.0

DISCLAIMER

Nothing herein constitutes an offer to sell, or the solicitation of an offer to buy, any tokens, nor shall there be any offer, solicitation, or sale of Frozen Network Tokens. You should carefully read and consider fully the information contained herein this white paper and any subsequent updates. Every potential token contributor will be required to undergo an onboarding registration process. This includes a Know Your Customer (KYC) identity verification and proof of address documentation. Please make sure to consult with your appropriate legal and investment advisors before contributing to our token sale. This white paper describes our current vision for the Frozen Network platform. While we intend to attempt to realize this vision, please recognize that it is dependent on quite a number of factors and subject to quite a number of risks. It is entirely possible that the Frozen Network platform will never be widely implemented or adopted,or that only a portion of our vision will be realized. We do not guarantee, represent, or warrant any of the statements in this white paper, because they are based on our current beliefs, expectations, and assumptions, about which there can be no assurance, due to various anticipated and/or unanticipated events that may or may

not occur. Please know that we plan to work hard in seeking to achieve our vision but that you cannot rely on any of it coming true. Blockchain, cryptocurrencies, and other aspects of our technology and markets are in their infancy and will be subject to many challenges, competition, and a rapidly changing environment. We will try to update our community as we grow and evolve, but undertake no obligation to do so.

1. Introduction

Cryptocurrency and smart contracts are changing the world economy. From a currency perspective, what was previously impossible in most of the world – transferring money globally in an instant – is now not only possible, it's safe, fast, easy and almost frictionless.

Smart contracts are also rapidly changing the way business is done. A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.

The potential uses of cryptocurrency and smart contracts via the blockchain are revolutionary and have the potential to disrupt almost every industry and institution imaginable. But, there are problems in making this vision a reality. The largest and most immediate problems are blockchain in its current form is not scalable, lacks real decentralization, and is using absurd amounts of energy that is not sustainable. We intend to fix those problems with immediacy!

1.1. Executive Summary

Frozen Network, a standalone blockchain, is a next generation smart contract platform. It’s built upon an improved Ethereum codebase that solves the scaling problem with immediacy. We currently have a working TestNet showing in excess of 1300 transactions per second ongoing with stability and has been running as high as 2400 transactions per second.

Right now Ethereum can only process 13 transactions per second and as such their network is at capacity, yet it’s the industry standard. There are other players coming into the space trying to build new blockchains to solve this scalability issue but that won’t solve the Ethereum scaling problem. Next, many of these new blockchain solutions are 12-24 months out. Over 90% of the smart contracts are Ethereum based and they need an immediate solution. And, that’s where Frozen Network comes in.

We will not only solve the Ethereum scaling problem with immediacy, but anyone currently using Ethereum will be able to seamlessly transfer to our network without making any code changes to get:

1. 10x more decentralization

2. 100x increase in speed
3. 1000x improvement in energy consumption

Let’ s take these one by one and break them down because this is a tremendously difficult problem to solve and it’ s a controversial one. If it was easy you wouldn’ t be reading this white paper. Let’ s start with decentralization because that’ s probably one of the most controversial topics today.

The promise of a truly decentralized network and the currently reality are two dramatically different things. At the time of this writing 4 companies in China account for 70-80% of all the mining activity for all the major coins/tokens including Ethereum. That is about as far from true decentralization as you can get, yet the purists still want to argue its merits. We obviously disagree and further acknowledge that true decentralization in its purest form is not possible today without making some sacrifices to get as close as possible.

So, then what is the next best solution and how do we solve this decentralization problem? Our solution is to take a step back towards the

middle, or in this case towards centralization, to take a leap forward in creating the most decentralized solution possible. Sometimes you have to take a step or two back to make a leap forward.

We are doing this by changing the consensus algorithm from Proof of Work (POW) to Proof of Reputation (POR). POR is an upgraded, stronger, and more secure form of Proof of Authority (POA). In POA the transactions and blocks are validated by approved accounts known as validators. POA has typically been used in private networks and most recently a few companies that have adopted it to use individuals as the validators whose identities are publicly disclosed and at stake.

In exchange for staking their identities they are rewarded and monetarily incentivized to process transactions. With the individual’s identities disclosed this is meant to disincentivize them from being bad actors because it would damage their reputation. We don’t think this goes far enough because as the value of the network grows the incentive to cheat will become larger and larger.

This is why we’ve come up with POR which uses companies as

validators not individuals. A company with a reputation has a lot more to lose than an individual and is a much stronger deterrent to be a bad actor because the risk is much larger. A company caught cheating would not only be risking its reputation. It would be risking its entire market cap and the reputation of the officers and shareholders of the company. It would have significantly more to lose than any one individual.

Taking it a step further we plan to use 50 companies in 50 different countries as the validators to force decentralization. By spreading the validators across 50 different companies with reputations at stake it should create almost perfect decentralization and make the network very difficult to be compromised. Furthermore, by spreading the nodes geographically no one government, like the US or China, can come in and take over the network. These two considerations should deter any 51% attacks.

How will the validators be chosen? Initially, Frozen Network will choose the validators and then the selection process will be turned over to the network. What kind of companies will they be?

Think, Venture backed startups with a burn rate, VC partners, angel investors, and new product or service. By using these types of companies or larger there is a huge incentive maintain network integrity to protect their market cap and professional integrity. Next, how do we move from 13 transactions a second to 1300+ tps? We are solving this partially by moving to POR and by dealing with the large amounts of data in ways that allow for much faster speeds. Again, this is not an easy issue to solve. The data storage issue alone at 1300 transactions per second produces 0.7 gigabytes a data an hour. It should be noted that any offchain solutions such as Plasma or Raiden will be able to work on top of Frozen Network to make it even faster.

Lastly, by switching to POR we will be able to dramatically decrease the energy utilization needed to process the blocks. The network effect will be somewhere between 1000 to 10,000x greener in terms of energy utilization. We have a world class dev team is lead by Travis Reeder the former founder of Iron.io. We also have Iron ’ s former Director of Engineering Romana Kononov. While at Iron they pioneered Serverless Cloud Computing to over 1 million transactions per second.

Moving forward we plan to launch the next generation of smart contracts. We think smart contracts should be “smart” with the ability to be changed, altered, paused, and/or terminated over time as conditions and/or agreements change. Just like in the real world.

Our MainNet will launch at the end of May 2019 Followed by smart contract upgrades and further network speed increases by the end of 2019.In 2020 we plan to upgrade our network to excess of 13,000 tps or 1000x the speed of Ethereum.

1.2 Previous Work

1.2.1. Proof-of-Work Algorithm. Proof-of-Work (PoW)is a consensus algorithm that is commonly used in cryptocurrencies. PoW was originally invented as a means to combat spam; if you make it computationally expensive to send email then spamming would be cost prohibitive while still being almost free for a normal user to send email. The same concept is used in cryptocurrencies to prevent malicious actions by making it prohibitively expensive to modify the blockchain.

In cryptocurrency networks, “miners” are special nodes that perform the PoW calculation on a set of transactions plus the hash of the previous block to generate the next block in the blockchain. Since the block contains the hash of the previous block, changing a historical block would require regenerating all of the subsequent blocks. Regenerating all the hashes would be computationally intensive and would require a lot of energy- and energy isn’ t free. It would also be time consuming. The process of proving work and generating blocks is called ”mining”.

Miners are rewarded for this work with newly minted coins adding to the total supply.Although PoW has helped move us towards secure distributed ledger system, it suffers from poor performance, a lack of decentralization, and excessive energy consumption.

1.2.2. **Proof-of-Stake Algorithm.** Proof-of-Stake (PoS) is another consensus algorithm which pseudo-randomly chooses validators based on their stake in the network. The idea is that those with the most coins in circulation have the most to lose so they are positioned to work in the interest of the network. This approach avoids the cost of computing hashes, however, it makes assumptions about the interests of its members

being in line with the network.

Validators within the PoS network are anonymous users who are identified only by their wallet address. This pro-vides no additional accountability over PoW for bad actors who can amass significant wealth on the network. Second, transaction fees will go to those who already have the most money within the network and large wealth requirements exclude poorer coinholders from validation. Finally, while PoS reduces energy consumption its goal is not oriented towards high performance. Initial targets for Ethereum’s Casper implementation are only 100 TPS.

1.2.3. Proof-of-Authority Algorithm. Proof-of-Authority is a new consensus algorithm where a trusted set individuals provide all transaction processing. This trust allows transaction processing speed to improve significantly by skipping the PoW hash computation. A few networks exist but they currently only focus on private networks or do not focus on performance as a goal. Many also do not have compatibility with the Ethereum network.

One public network relies the US state-level Notary Public system to

verify the identity of 12 individuals who will act as validators on the network. Candidates requesting validator status submit proof of physical address, bank account, social network, and mobile phone to verify their real-world identity. While PoA removes the the computational burden of mining,trusting individuals for transaction processing breaks down at scale for several reasons.

First, there is a disparity between the net worth of the network versus the market cap of the network. This is what the PoS system attempts to solve. Assuming an average net worth of an individual in the United States is $68,828, the total net worth of the validators is $825,936:

$12 * \$68,828 = \$825,936$

Even if the number of validators increased by an order of magnitude, the total net worth of the validators is a tiny fraction of the $6.8T in transactions processed by Visa, Inc. every year.This disparity introduces a strong incentive for bribery.

Second, validators must post their physical address publicly which opens the potential for intimidation or physical threats. A terrorist organization or rogue state can mount an attack on a large scale financial system by

controlling half of these validators.Finally, most individuals lack the experience and infrastructure to run a secure transaction processing system. This significantly increases the network’s exposure to malicious hacking.

2. Implementation

2.1. Authorized Signers

Authorized signers are trusted nodes that create blocks, sign them, and distribute them to other nodes. Similar to miners in a Proof-of-Work (PoW) system in that they create blocks and sign them but without the mining cost.

A list of authorized signers will be maintained on the blockchain. Only authorized nodes can sign blocks and all blocks are verified that this is true by checking the signer is in the authorized list. The signing algorithm is essentially the same signature algorithm as PoW but with a different set of headers. PoW-specific headers will be removed and additional headers added to enable voting.

Given N authorized signers, a signer may only sign a block every (N/2) +1. This ensures that someone would need to control > 50% of signers to perform a malicious attack .

2.2. Signer Verification

Companies which operate authorized signer nodes will go through a verification process to ensure their identity is correct. These validation steps will be automated through the use of smart contracts on the blockchain.

The PoA implementation provides point-in-time signer & voting state that we can build upon to provide full transparency to end users. Combined with the verification data stored within smart contracts, users can what companies are running which nodes at any given point.

2.3. Checkpoints

A checkpoint is a signed snapshot of the current state of the entire blockchain at a particular block number. It will contain all non-zero account balances and smart contract states. Once a checkpoint is generated, all the previous blocks and data can be removed.

When a new node is started, it will download a recent checkpoint, then continue retrieving blocks and state from that point on. This will save

hours, if not days, getting in sync. This means a node can be up and running in minutes.

Frozen Network will provide a publicly-available, read-only API to retrieve any historical block so anyone can look up data by keys. This will be open-source so anyone can run this to keep a full history. We encourage it for further verification and accountability. This will make it easier to build third party services such as block explorers.

2.4. Performance and Optimizations

2.4.1. Speed and Volume of Transactions. By using trusted nodes, transactions can be verified very quickly and the volume of transactions the network can handle increases by orders of magnitude. Similar to systems we use every day that can handle high volumes, like a Google search or Visa payments, those systems can handle high load only because they trust the servers and the network they are running on.

Other factors such as block size and gas limits are artificially low because of the computation power required by PoW. By trusting the consensus nodes we can increase the volume of the network by 100x more than

Ethereum can currently handle. Trusted consensus is used outside cryptocurrencies in systems such as etcd which can reach 141,578 transaction per second on a 3-node cluster using modest hardware.

Improving throughput is critical as the growth rate of Ethereum is skyrocketing to an unsustainable rate. Ethereum runs at 13 tx/second right now;we are targeting 1,300 tx/second at mainnet launch.The two major parameters we can tweak are block size (gas limit) and block times. Due to the fact that we have a relatively small set of signers (vs the number of miners in PoW) with known capabilities, we are able to increase the block size drastically and reduce the block times. This alone greatly increases the number of transactions per second. As stated above, the reason you can’ t increase block size in PoW is that it makes the hashing algorithm too hard and too expensive. Frozen Network does not have that limitation.

2.4.2. Energy Consumption. Using a trusted network of authoritative nodes means that there will be no mining. No mining means there will be no battle between computers to win blocks and therefore no wasted energy. Nodes will only require a small fraction of this energy to process

transactions, run smart contracts, and verify blocks.

Ethereum’s estimated energy consumption at the time of this writing is 14 TWh and rising.Assuming 450W power usage per server, our 50-node cluster will only use 197.1 MWh or 0.001% of the energy of the Ethereum network.

2.4.3. Networking. Signers will communicate directly with each other. This means that the node who just finished signing will send the just signed block to other signers in the authorized signers list before sending to a replication node. This ensures the authorized signers get the information they need as fast as possible while offloading blockchain and API queries for the rest of the network to dedicated replica nodes.

The replication layer exists for non-signer nodes (everyone else) to request blocks and query the state using a read-only API. Because the replication layer is read-only, we can horizontal scale to meet the needs of a global scale set of users. Figure 6 shows an example of this 3-tier network strategy.

2.4.4. Storage. The storage requirements to store the entire blockchain is quite large – Ethereum size is hundreds of gigabytes and it's growing rapidly. It can take hours or days to synchronize to a new node which makes it impractical for the average user that just wants to send a transaction. There are newer modes you can run to reduce the size such as fast and light mode, which reduce the size drastically and that is a good step in the right direction.

Since Frozen Network will be handling 100x more transaction volume, storage becomes much bigger – potentially 100x bigger. As of this writing, Ethereum transactions average 174 bytes and 700,000 transactions occur per day which produce 120.4MB of block data per day or 43.9GB per year. Increasing throughput by 2 orders of magnitude will generate 4.4TB of block data per year. Propagating this across all 23,000 nodes in the Ethereum network would require 101 petabytes.

By limiting the set of nodes operating on the dataset we reduce the network traffic and storage requirements. Checkpointing allows nodes to only store the small fraction of the total blockchain that is required for current processing. Current cloud pricing of $0.022 USD per GB/month

makes storing a copy of the blockchain history only $1,161.60 USD per year of block data.

2.4.5. The Future. Beyond our initial goals described above, we have a plan to upgrade the smart contract system to make it easier and less error prone. Software almost always contains bugs that are unknown at the time of release and developers need a way to fix those bugs.

Ethereum does not allow you to upgrade your contracts and that results in $100’ s of millions of value being stolen. We intend to make writing smart contracts easier to write and easier to deploy, as well as making them safer to prevent the massive amounts of theft that is happening. Smart contracts need to be more like the real world, where they can be amended,paused, and/or terminated.

We are also adding standardized rulesets to contracts to define how and when contracts can be modified. We expect this will help the adoption of smart contracts by the broader business community by using familiar contract terms. For example, a co-op organization may require a quorum of members to change a contract while other organizations may require

all participants in a contract to agree to a change. Frozen Network will continue to default contracts to be immutable by default for compatibility with Ethereum. Frozen Network will also add additional security features such as whitelists to protect access to contracts to minimize attack risk.

3. Road Map