IceChain

High-Throughput Transactional System

Version 0.1A

WHITEPAPER

icechain.io

CONTENTS

ICECHAIN.IO

1. DISCLAIMER

This white paper is meant to be understood as offering an outline of what we hope to create and does not in any way represent, nor should it be construed as, any type of advice. This includes financial or tax related advice and you should know that you should contact your own tax advisors before you decide to go ahead with IceChain. IceChain, all employees of same and all affiliates are not responsible to you in any way for any loss that you incur on the IceChain platform without any limit.

This white paper is supplied to provide generalized information and the information contained herein should not be looked at as being comprehensive in nature or the final specifics of the IceChain platform. All ideas contained in this paper can change before the platform comes to fruition. All third-party information should be verified independently. This white paper is not an offer to sell IceChain coins.

By virtue of having accessed this white paper you agree and understand that you should not rely on this whitepaper as the final determination in whether to purchase and ICH and that if you do it will be in full compliance with your own local laws, all other laws and any further regulatory requirement that might exist. You understand that there is no guarantee as to a set value for the ICH token or any related liquidity. You understand that all IceChain employees, affiliates and owners, are not responsible for the value that becomes attached to the ICH coin at any point in the future. This also includes the ability to transfer the coin or market availability.
The ability to purchase any ICH coin will be regulated in the first instance by your own local jurisdiction and the regulations which exist for same in your country. If you are a resident of any jurisdiction that bans participation in the crypto market you must not purchase ICH tokens, which includes but is not limited to Canada, the United States, China, South Korea or New Zealand.

Risks should be carefully considered and weighted by you prior to buying any ICH. Any statement which is made by any IceChain employee or any of its affiliates, are to be considered as future projections and should not be considered a definite. The purchase of ICH tokens will have separate terms and conditions which will govern that area that will contain all facts relating to buying ICH. You understand that there are many factors that might influence the token and platform in the future and that many are outside of the platform's control, such as changes in regulation. This would include any issue that might have an impact on the IceChain development.

You may not copy this white paper or share it without permission from IceChain. If you need a translation of this white paper, please write to us by email and we will endeavour to provide an accurate translation in your chosen language.

2. EXECUTIVE SUMMARY

Given the rise in use of decentralized blockchains, there has been a number of new coins created to where now there are many coins to choose from, instead of the 'traditional' choices of Bitcoin or Ethereum. Due to this growth in the digital currency market, there is a necessity to include a higher level of distributed ledger technology, which is able to handle the high volumes without lag.

IceChain has created a system which can handle large amount of transactions. IceChain is an innovative digital platform that is scalable and which provides secure, decentralized technology. This guarantees the high level of security, leveraging permissionless mining and transactions secured by at least 50% hash power at one time sent to the head chain to prevent double spending. The platform can also issue cross transactions and be confirmed in a few minutes. The number of cross transactions at any one time will act to increase the response speed.

3. INTRO

Since Bitcoin first arrived on the global stage, the area of blockchain has advanced quite considerably. Ethereum was the second generation and allows for blockchains to run smart contracts. The industry has moved on yet again, to be a proof of stake style platform which is a step up from the proof of work technology.

Under the IceChain platform there will be an ability to issue block rewards and use less hash power overall. Block rewards will be issued on a proportionate basis which will decrease the overall energy needed for mining and make the platform economically efficient. This builds on from where the last generation of digital currency platforms left off and will allow IceChain to have a dominant level in the industry. In the future, the old way of transacting will become obsolete as customers will choose the service which allows them to facilitate their transactions at the cheapest cost in the fastest time with the highest level of security. The scaling is a major problem for traditional blockchains at present. Under the IceChain system, this will be eliminated and the platform will have the ability to scale as appropriate to allow for any number of users to make transactions at the same time.

4. ICECHAIN

Through using the newest technology including using shards, IceChain will be able to scale as need and also be able to handle any amount of distribution. Using this model, IceChain will be able to offer high-throughput blockchain users are already looking for; something safe, fast and cheap (if not free) to transact on. Since the platform will run on a distributable network, it will allow the ICH coin to integrate into common purchase transactions, offering a decentralized and fast service.

5. ICECHAIN TECH

The design principles which form the basis of the IceChain network are that the platform is able to scale as needed while not compromising on any level of security and without costing users more in transaction fee. Security, scalability and decentralization are at the core of the IceChain model. Cross shard transactions will be able to be created in a seamless manner which will give a high level of quality within the experience to users. All this, on an ecosystem that will be driven by incentives and able to support a wide variety of alternative platforms to provide users the ability to use one account for all their transactions. Security will be maintained at the same high level regardless of how large the platform scales.

The contemporary functioning of blockchain technology offers two basic functions in every block found in a chain. There is the ledger that includes the current ledger, and the confirmation that is required to approve the transactions from within the ledger and go on to mine blocks in order to reach the desired difficult levels that creates the proof of work. A ledger has the main benefit of offering a large area where data can be stored which would include the ledger being up to date and continuously making notations of all new transactions when they happen. Included in this would be the source, execution code, destination and amount of the transaction. Only a finite amount of information is capable of being saved into any single block, which is what causes the longer time waits in the blockchain. Transactional results will create confirmations in the ledger prior to the block being mined in order to reach the necessary proof of work. It is this system that creates a belief in safety that another user could not attach the system by fork mining, since to do so would cost the user far too much money and as such not be a viable plan. More hash power is needed for the computation than for the rest of the tasks needed to complete the process.

With this in mind, IceChain operates under a type of 'divide and conquer' approach that will separate the above functions over two separate layers. This will allow for a high level of scalability while the security levels are appropriately maintained throughout the scaling. By using an elastic sharding layer, smaller shards in the blockchain can be listed in the layers.

This means that as the shard numbers increase, the processing ability also increases, creating an increased systems capacity through concurrent operations of both layers. The IceChain network has a head chain which will act to confirm the blocks in the chain without processing any of the transactions and have such a high level of difficulty that people will not try to revert a transaction as it would not be a gain. Additional shards can be supported on the platform that is capable of independently processing different transaction subsets.

6. ICECHAIN POSITIONING

The design put forward by IceChain allows for a new approach in the blockchain market, considering the single and multiple blockchain system relationship. When the entire head chain reaches 100% hash power, the IceChain network will reposition itself as a single blockchain, therein morphing as required, when necessary. This is possible due to not having any shards of mining, and multiple pools of weaker miners working together, and adding many minor blocks together allow for the head chain size to be infinite. If the head chain hash power becomes 0% the IceChain system will independently operate in a multiple blockchain system since each IceChain shard is an independent blockchain operating together in a multiple blockchain system. This also allows for the highest level of decentralization.

The IceChain network will have a much higher level of decentralization than other existing blockchain systems, with an equally higher level of security. This is a benefit of allocating only 50% hash power on the head chain and integrating sharding technology that facilitates an increase in capacity in relation to the number of transactions being processed. This is helpful in allowing scalability on the network any time that it is needed without the need to compromise on efficiency and time. It also creates higher than average decentralization levels as compared to normal blockchains, and offers better security through maintaining half of the hash power within the head chain.

Main Features on the IceChain Network:

❯ IceChain maintains a horizontal scalability option, running each node as a full node which creates the same security against attacks as what a traditional blockchain offers.
❯ IceChain network was designed from the outset with this scalability feature in mind, so it will run smoothly and will offer high throughput.
❯ The IceChain network is safe and well protected by 50% hash power distribution.

7. SHARDING

Sharding happens with data is partitioned from a larger database to several smaller databases. The commonly used sharding method for centralized systems is for meeting scalability. As an example, cross-shard transactions are supported on IceChain and the platform uses the technology to meet their scalability requirements. When this type of sharding is not planned for at the outset, however, there is an issue in maintaining the same level of security that previously existed. Without planning for scalable security at the outset, the system becomes weaker and more prone to risks when multiple transactions hit the platform at the same time.

Sharding challenges include scalability and cross sharding, or security issues like single shard takeovers. There can be a trade-off for older platforms that did not plan for security scalability, in order to successfully create a blockchain. Where there is a need for a larger storage capacity there can be seen to exist transaction speeds that are slower than average. IceChain planned to overcome this issue from the outset, and as such can be assured that it will not transpire on this platform as it has on older platforms.

8. SCALABILITY

Blockchain can be scaled in different ways, including through the use of multiple blockchain, sharding or through a lightning network.

In a lightning network, it would be ineffective for a random user to try and reach a sporadic target; transactions are tracked with lightning channels that are not as transparent as they could be. This is because they are tracked inside the channel instead of within the main blockchain. Third party sites are also a normal requirement in this method, such as PayPal, in off-chain solutions like this. There are enough centralized payment methods at present that it does not seem feasible to create another. Scaling is completed by multiple blockchains by splitting transactions between several different blockchains. This acts to a create less demand for transactions and also creates less hash power to power each blockchain. In this type of system, a person could gain enough hash power to create a double spend attack. Trading off security for scalability is not a viable option, and multiple blockchains act to limit performance ability for cross chain transactions. Cross chain transactions require users to maintain addresses on each network, which is a further security issue, and there are key concerns relating to private key management across multiple platforms.

9. DECENTRALIZATION

Necessary expenses are reduced through a decentralized trading and storage, giving everyday people the chance to gain from technology just like a business or large group would. Decentralization also creates the security for the entire blockchain that is inherent in a good blockchain platform. When smaller mining pools link together to create mining pools, proportional block share rewards can be enjoyed by any miner, in the same time frame that a larger mining pool would gain. Centralization is benefitted by this design of blockchain which is a risk to the decentralized proof of work format blockchain that is envisioned.

Collaborative mining style formations create difficult algorithms which are effectively hard enough to share the hash power across the miners equally, which allows for the system to be evenly spread. This is controlled through the head chain and by ensuring that at least 50% of the overall hash power is spread across the entirety of the network. This acts to prevent any type of double spend attack or attack by a malicious miner.

10. SECURITY FEATURES

If security issues are prioritized through a decentralized ledger, vulnerabilities on the transactional platform can be secured and eliminated. In order to keep every node in sync, a peer to peer blockchain has the requirement of needing to be updated regularly. In a proof of work based blockchain there will be 51% of the total hash power needed for completion f the double spend or in order to reverse any transaction. To create an attack like this requires the platform to be less decentralized than what is possible in the IceChain network. When a blockchain is appropriately decentralized it will create a situation that it would not be economically efficient for a person to attempt a double spend attack.

The IceChain network has both a head blockchain, and several minor blockchains, that all operate on different levels of difficulty and with different levels of incentive. Miners can then choose which blockchain is best for them considering their desired hash power. This creates an open market economics model that allows the blockchain to act as a goods seller, i.e. the block rewards, and makes the miner a buyer. This benefits all parties and allows all to pursue their own interests.

All IceChain system transactions are protected through the operation of a consensus algorithm across the head and shard networks, while a proof of work system will be operating across the head chain. At the same time a head chain first proof of work algorithm is running within the shard networks. This type of proof of work system operates in the main blockchain networks as well, such as Bitcoin and Ethereum, that have the first proof of work additional head chain as a unique shard network platform compared to IceChain.

IceChain is operated by determining which one of two shards will be allowed to survive through having a node compare the corresponding chains and only allowing the longer one to survive. This type of system would be much more difficult to attack since it would require manipulating at least 51% of the overall hash power to survive.

On the IceChain platform there are 10 minor blockchains that operate in the network system with a total head blockchain target of no longer than 180 seconds in duration and block target durations of 10 seconds. This will facilitate the system being able to operate and around 10x the level of any single shard, therein creating an even mining. Trying to run super full nodes ends up being higher priced when there is a high level of throughput in the blockchain. If 1M TPS is given on each transaction of 300 bytes a requirement would be created for over 2.4GBps of network bandwidth, which most users could not achieve. Traffic would also create a pull on the central processing unit, storage, memory and overall network capability, which is not conducive to blockchain values nor any good for maintaining decentralization.

The IceChain network will tackle this issue through the implementation of several 'trust' nodes that will cluster in order to run like a super full node. Each node will only be able to validate a small subset of the chain and the grouping of subsets that cover the head chain. If one node crashes it will not be an emergency because the other nodes will still be running and continuing to validate blocks by the ability of any two nodes being able to cluster. Miner incentives will encourage cluster formation that will have the result of encouraging miners to work together.

HEAD CHAIN   SHARDS
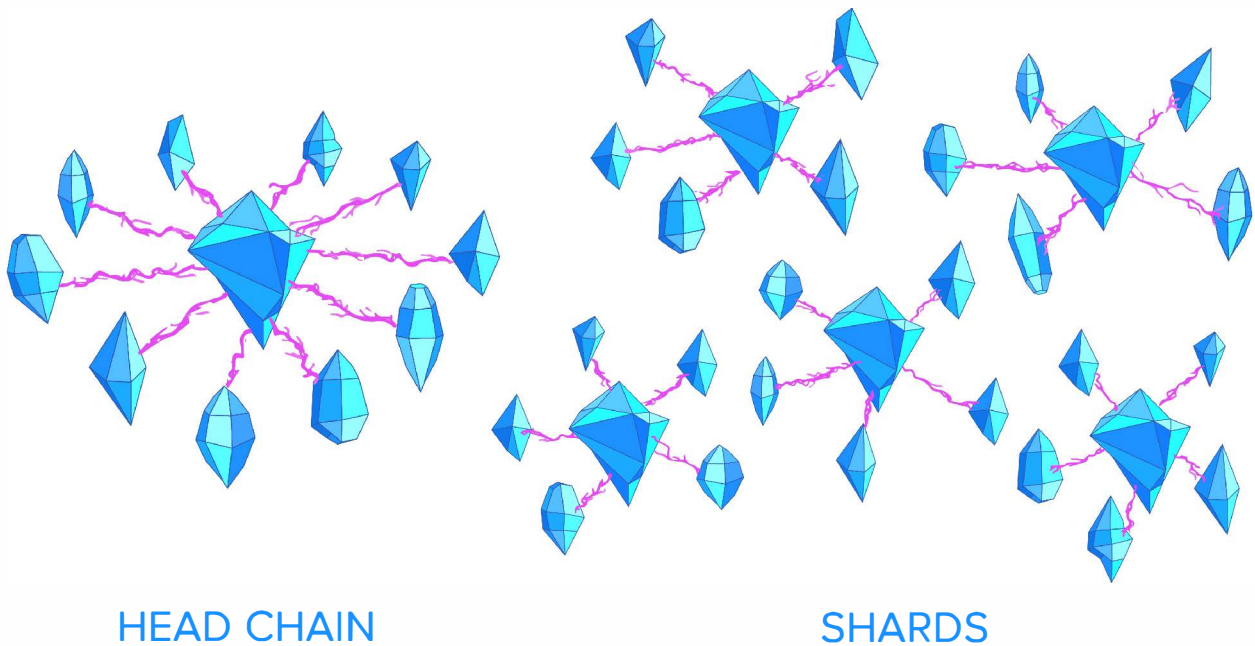
Solving random block information will be conducted over a high number of blocks that will be intensive on memory use and create an inefficiency in downloading random blocks. A transaction will be classed as either being a cross-shard transaction that has their input and output addresses contained on different shards, or will be in-shard transactions. The in-shard transactions have less difficulty since the shard stores all the information together, and a requirement to synchronize cross shard transactions as they increase in amount. The cross shard transactions will be supported by allowing any user to be able to issue a cross shard transaction at any point in time, that will have a minutes confirmation and be able to scale linearly as shards increase in numbers.

With the IceChain solution a user will not have to make several accounts across all the different shards in order to manage their cross-shard transactions since only one account will be needed for account management to complete a smart contract. Smart wallets will facilitate cross-shard and in-shard transactions in a seamless manner, allowing the user to have in-shard transactions.

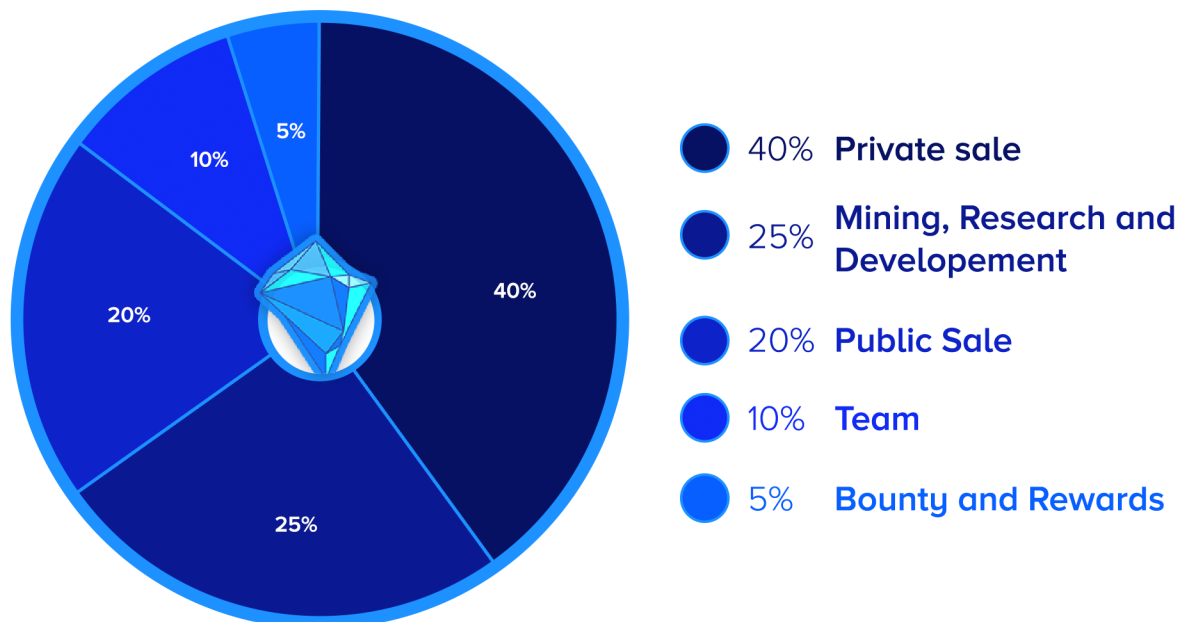## 11. CROSS CHAIN TRANSACTIONS

In the IceChain design a cross-shard transaction becomes manageable by token conversion and transaction performance. A sub-chain will be on offer to the other chain, that can make a cross-chain a cross-shard. Smart contracts will be made possible through the EVM as it is the most popular choice at present. Off chain transactions will be accommodated for whenever a transaction must have access to information that is off the blockchain. Smart contract data will be sharded when needed and remain specific in nature. The overall account management is made easy by the ability to have one account having access to any shard and users will be able to run a primary account containing the user address in a default shard, or by running a secondary account that manages every address of the user in a shard. The primary option will be the most popular account chosen and will only be moved temporarily to another address in a second account if necessary. The remaining balance in the secondary account will be moved back to the main account. The overall process will be easy and the shards will be able to automatically detect what a user's primary account is, with seamless running that will go unnoticed by the user.

12. ICH TOKEN

IceChain will use the ICH token. It has been designed to be the main token for the IceChain network. The ICH will issue at the outset as ERC-20 tokens on the Ethereum network and will then migrate to the IceChain own network. The ICH token will be the native token for IceChain network. ICH cannot be thought of as being any type of shareholding in IceChain nor in any aspect of any of IceChain's affiliates. There is no inherent ownership rights with the exception of having an express right to use them as the means to interact on the IceChain network. One area of focus for the IceChain network will be the gaming and fintech industries, to provide a trustworthy and solid exchange medium.

The IceChain network is mobile oriented and the infrastructure is supported with DApps. There will be on-site developer tools offered on IceChain to allow for the creation of different Android/iOS enabled environments. Developers on the IceChain platform will be ale to create and run small online projects. The network will also allow for business owners of small to medium size enterprise to be able to add more efficiency in authentication through using block chain for high volume transactions. The use of sharding blockchain technology will have an unlimited number of uses in the internet of things (IoT) and will undoubtably bring new users to the IceChain network.

13. TOKEN DISTRIBUTION

40%	**Private sale**	
25%	**Mining, Research and Developement**	
20%	**Public Sale**	
10%	**Team**	
5%	**Bounty and Rewards**	

14. ROADMAP

December 2017
Current Blockchains Analysis

January 2018
Scalability Problem Research

March 2018
IceChain Development

May 2018
Draft Programming Tasks

August 2018
WhitePaper Release

September 2018
Private Sale

October 2018
Token Distribution

January 2019
Testnet v0.1

April 2019
Testnet v0.1 (with smart contract support)

June 2019
IceChain Alliance

July 2019
Making the Source Code Public

August 2019
Mainnet v0.1

October 2019
Wallet Release

December 2019
Android & iOS App Release