# INSTACASH

The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. But since then, it has evolved into something greater. By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin, the tech community is now finding other potential uses for the technology.

Cryptocurrencies have emerged as the latest brave market in the trading world. These trading markets are relatively young and thus full exploitation has not yet been achieved.The fact that some coins like Bitcoin can rise by 10% in a single day signifies the need for other stable coins to join the market. The tender age cryptocurrency in the trading world has prevented the established trading houses and only
left the young companies to invest. Some years back, the market capitalization for cryptocurrency stood at $80 bn and still growing. This further signifies the availability of opportunities for young traders to venture in the market and make profit.

Bitcoin “pioneer of cryptocurrencies” has shown currency can exist outside of the current financial system. It is technologically resistant to counterfeiting via blockchain technology. However, this by itself is not inherently strong enough to spark a technological payments revolution. Rather, bitcoin is exciting and motivating entrepreneurs to build a better mousetrap.

## ABOUT INSTACASH

InstaCash is an open source crypto-currency focused on fast private transactions with low transaction fees & environmental footprint. It utilizes a custom Proof of Stake protocol for securing its network and uses an innovative variable seesaw reward mechanism that dynamically balances 90% of its block reward size between master-nodes and staking nodes and 10% dedicated for budget proposals. The goal of InstaCash is to achieve a decentralized sustainable cryp-to currency with near instant full-time private transactions, fair governance and community intelligence.

## MAIN FEATURES

⚡ Anonymized transactions using the Zerocoin Protocol.

⚡ Fast transactions featuring guaranteed zero confirmation transactions, we call it SwiftX.

⚡ Decentralized blockchain voting providing for consensus based advancement of the current Masternode technology used to secure the network and provide the above features, each Masternode is secured with a collateral of 10K ICH.

⚡ Wallet Built-in Block Explorer and Wallet Repair Tool.

⚡ Integrated BIP38, Multisignature and MultiSend Functions.

POS 3.0.

⚡ Low Transaction Fee.

⚡ Auto Synchronization with Addnodes.

⚡ Smart Contracts [soon].

⚡ Low inflation.

⚡ Long-Term Development & Support.

## TECH SPECS

Name **InstaCash**

Ticker **ICH**

Algo **Quark**

Blocktime **30 sec**

Maturity **100 blocks**

Diff retargeting **Every block**

Total supply **~100,000,000 after 18+ years**

Premine **0.5%**

Masternode Collateral **10000 ICH**

Minimum Staking Age **1 hour**

Port **46200**

RPC Port **46201**

P2P Port **9050**

## POW REWARDS

since start: 100

since block 10 001: 10

Last PoW Block: 100 000

## POS REWARDS

since block 100 001: 5

## MASTERNODE REWARDS

since block 10 001: 25%

since block 100 001: 75%

## POW

The first is the question of mining. Mining is the process by which individuals dedicate computational resources to solving difficult mathematical problems. Upon solving the aforementioned, a new block is found on the blockchain and with it newly pending transactions are confirmed and cleared through. This process is known as Proof of Work (or PoW) as it forces the miner to prove that they have done the necessary work to verify the block, and the first miner to find a new block is compensated for their efforts.

This introduces an element of economic competition between miners and prevents the network from being attacked as attacks become too costly and thus, economically unviable. Consider this process as rolling a die in a casino and needing to roll below a

certain number, and the first roller who rolls below said number wins the prize, except that the die does not have 6 facets, but rather an extremely large number of them. Unfortunately, the Bitcoin protocol has introduced a mining algorithm that allows for ASICs (Application-Specific Integrated Circuit) - devices that can create a very large number of hashes per second (or in our example, roll a die much quicker than other rollers). This has created an unfair status quo whereby those who can afford to purchase ASIC devices have a clear upper hand and those who cannot are effectively excluded from participating in the network.

Since every bitcoin protocol enhancement needs to be approved with a 95% majority of miners, the top X% of miners who own 95% of the mining power can either accept or veto any suggestion that is brought before the community. This effectively overrules the democratic nature that a decentralized network should be characterized by and creates a disproportionate centralization of decision-making power. In order to prevent such an occurrence, ICH utilizes an advanced and fair hashing algorithm known as Quark.

## QUARK

Quark is well known for being a lightweight algorithm that can be mined with very modest hardware devices. This ensures that anyone can participate in the ICH mining, whether they own a smartphone or a super computer. It further utilizes multiple algorithms, namely Blake, Groestl, Blue midnight wish, Jh, SHA-3 and Skein, which makes the development of a dedicated ASIC device specifically designed to produce a large number of hashes per second virtually impossible as it must work with 6 radically different functions. This property is known as ASIC-resistance, and with it, we seek to eliminate any barrier to entry for the average ICH end user in terms of network governance and promote absolute decentralization and democracy.  Quark is super secure and uses a different hashing algorithm with 9 rounds of hashing from 6 unique hashing functions (blake, groestl, blue midnight wish, jh, SHA-3, skein). 3 rounds deliver a random hashing function. Even though most believe the SHA2 is sufficient at present, technology is always changing and improving. Just one of Quark's algos, SHA-3, was developed after SHA-2 in case it was somehow comprised in the future. The multiple hash gives a further layer of security against unknowns that will enter the market down the road.

## MASTERNODE

As we have mentioned the term masternodes in this document and have provided several hints as to its nature, we would like to now offer a more meaningful overview. Masternode are dedicated hardware nodes that sit on worldwide servers connected to the ICH network, each maintaining an exact replica of the entire ICH blockchain and providing enhanced services to the network. As masternodes are essentially continuously-connected nodes that are hosted on dedicated servers, their function is to provide a host of services and guarantee their availability to customers of the ICH network. To increase the degree of distribution and thus network security, each masternode is required to have its own IP address, to ensure they are hosted on as many servers as possible and guarantee network resilience and redundancy. Within the context of the ICH network and as each standard node and thin client Masternodes must lock in a large number of coins (exactly 10,000 ICH as collateral; this is a flexible collateral as it can be withdrawn and moved at any point in time, however, upon doing so, the masternode immediately goes offline) as well as incur hosting costs, they are compensated for their costs and efforts in terms of both a portion of all block rewards and fees for the advanced services outlined above.