Whitepaper V3

# A Future Currency With OTOCASH

**WWW.OTOCASH.IO**
**Version 3**

## Table Of Contents

## Abstract

The purpose of this White Paper is to present OTOCASH, the technology, business model and OTO coin to potential coin holders.

OTOCASH (OTO) is Cryptocurrency Based Scrypt-PoS, OTOCASH coins will be used on the OTOCASH PAYMENT SYSTEM platform that allows buyers to use their OTO coin to pay private or merchant sellers. We provide safety and convenience with KYC for every consumer or trader and offer the best consumer-protection.

Today's world, making transactions through the existing financial system is subject to high charges. Nearly 90% of today's available financial system charges a major cost of 2% fees and appears very costly to consumers. To solve this problem, OTOCASH will create an innovative payment platform that will charge you free when using OTO coin. The advancement of this blockchain technology enables it to be realized using our advanced formula.

When you make payments and transactions to any seller or anyone in the world through cryptocurrency, you will always face doubts and concerns to be deceived; No one wants to be a victim of fraud. For that, we are building something that will prevent users from being exposed to any kind of deceit.

By creating efficient and secure platform to all consumers around the world, it is convincing that future affairs will go smoothly and OTOCASH will become a platform that can be tailored to various forms of transactions and payments.

## INTRODUCTION

In today's crypto currency community, a general understanding suggests that Proof-of-Stake has yet to prove its security, economic value, and overall energy efficiency over time. OTOCASH was originally created as an attempt to prove that the concept of Scrypt-Proof-Of-Stake is valid; asserting that it is a real world applications in the future of crypto currencies.

Proof-of-stake (PoS) aims to replace the means of reaching consensus in distributed system; instead of completing the Proof-of-Work, the node which generates a block that has to provide a proof of access to a certain amount of coins before being accepted by the network. Generating a block involves sending coins to oneself, which proves the ownership. The required amount of coins (also called target) is determined by the network through the same difficult adjustment process similar to PoW which guarantee an approximate, constant block time. As in PoW, the block generation process will be rewarded through transaction fees and a supply model specified by the underlying protocol; which can also be seen as interest rate by common definition. The initial distribution of the currency is usually obtained through a period of PoW mining.

Cryptocurrency uses the original PoS based protocol based on the project development described above. It is clear that PoS is better than PoW as a method used to establish consensus on the network, and to enhance network security. The Age of Coin in the generation of OTOCASH block protocol is based on the age of the coin which is a factor that will increase the weight of unspent coins linearly over time; the proof that has to be provided together with a new block and must meet the following requirements

$$\text{proofhash} < \underbrace{\text{coins} \cdot \text{age}}_{\text{coin age}} \cdot \text{target}$$

Eq.1

The proof hash corresponds to the hash of an obfuscation sum that depends on a stake modifier, the unspent output, and the current time.

With this system, it is possible for an attacker to save up enough coin age to become the node with the highest weight on the network. If the attack were to be malicious, the attacker can then fork the blockchain and perform a double-spend. After this is done, a second double-spend would require the attacker to save up coin age again, as the stake resets when the block was generated.

It is worth mentioning that this situation is highly improbable and that the incentive is questionable (saving enough coin age to be the highest weight on the network would either take a lot of time or a lot of coins, and thus money, to make this happen. Next to that, performing such an attack would probably devalue the system itself so it wouldn't be profitable to do the attack in the long run.

Another problem with coin age are greedy honest nodes. These are nodes that have no malice but they keep their coins off the network and only stake every once in awhile to get their stake reward. The current system actually encourages rough behaviour towards these nodes by maintaining their node offline until it accumulates enough coin age to get there within a short period of time and then shut down the node again .

**Blockchain Precomputation and Long Range Attacks**

At the time of this writing, there is no known solution for secure timestamping in a largely distributed network. Rules of the current block timestamp give an attacker a degree of freedom in selecting the proof hash described in Eq. 1 and therefore increase the probability of a successful attempt to fork from several blocks in the past.

In addition, the current stake modifier does not obfuscate enough hash function to prevent the attacker from precomputing future proofs. Therefore, someone who attempts to attack the network in a malicious way will be able to calculate the future interval for future proof of completion, which allows the individual to produce several consecutive blocks and perform malicious attacks that may harm the network.

**Block Timestamp Rules**

Appropriate changes have been made at the time of the block to work more efficiently with PoS. Expected block time is raised from original 60 seconds to match the granularity. Note that it is assumed that the nodes has an external source of time, and if the internal time of a node deviates too much from the general consensus, then there is a high probability that the blocks generated by this node will get orphaned.The proposed changes below outline the modifications to the block timestamp rules.

| OTOCASH | PoS |
|---|---|
| Past limit: | time of last block |
| Future limit: | +30 seconds |
| Granularity: | 60 seconds |
| Expected block time: | 140 seconds |

## OTOCASH CHAIN PROTOCOL BENEFITS

### Open Source Software

OTOCASH is an open source software project released under the MIT/X11 license which gives you the power to run, modify, and copy the software and to distribute, at your option, modified copies of the software. The software is released in a transparent process that allows for independent verification of binaries and their corresponding source code.

### Blockchain

OTOCASH blockchain is capable of handling higher transaction volume. Due to more frequent block generation, the network supports more transactions without a need to modify the software in the future. As a result, receiver get faster confirmation times, while still having ability to wait for more confirmations when selling bigger ticket items.

### Wallet Encryption

Wallet encryption allows you to secure your wallet, so that you can view transactions and your account balance, but are required to enter your password before spending OTOs. This provides protection from wallet-stealing viruses and trojans as well as a sanity check before sending payments.

### Mining And Reward

Based on Proof-of-Stake. No more power hungry mining hardware.Users who keep their wallet open to secure the network via staking will get from 0.0001 OTO rewards per block (varies according to network weight).

# Coin Details

## COIN IDENTITY

Coin Name: OTOCASH
Coin Symbol: OTO
Asset Type: COIN

## BLOCKCHAIN

Algorithm: Scrypt-PoS
Coin Decimals: 8
Genesis Date: March 01, 2018
Supply Type: Mineable By Staking
Block Reward: 0.0001 OTO
Average Block Time: 140 Seconds
Spend Confirmation: 1/10

## SUPPLY

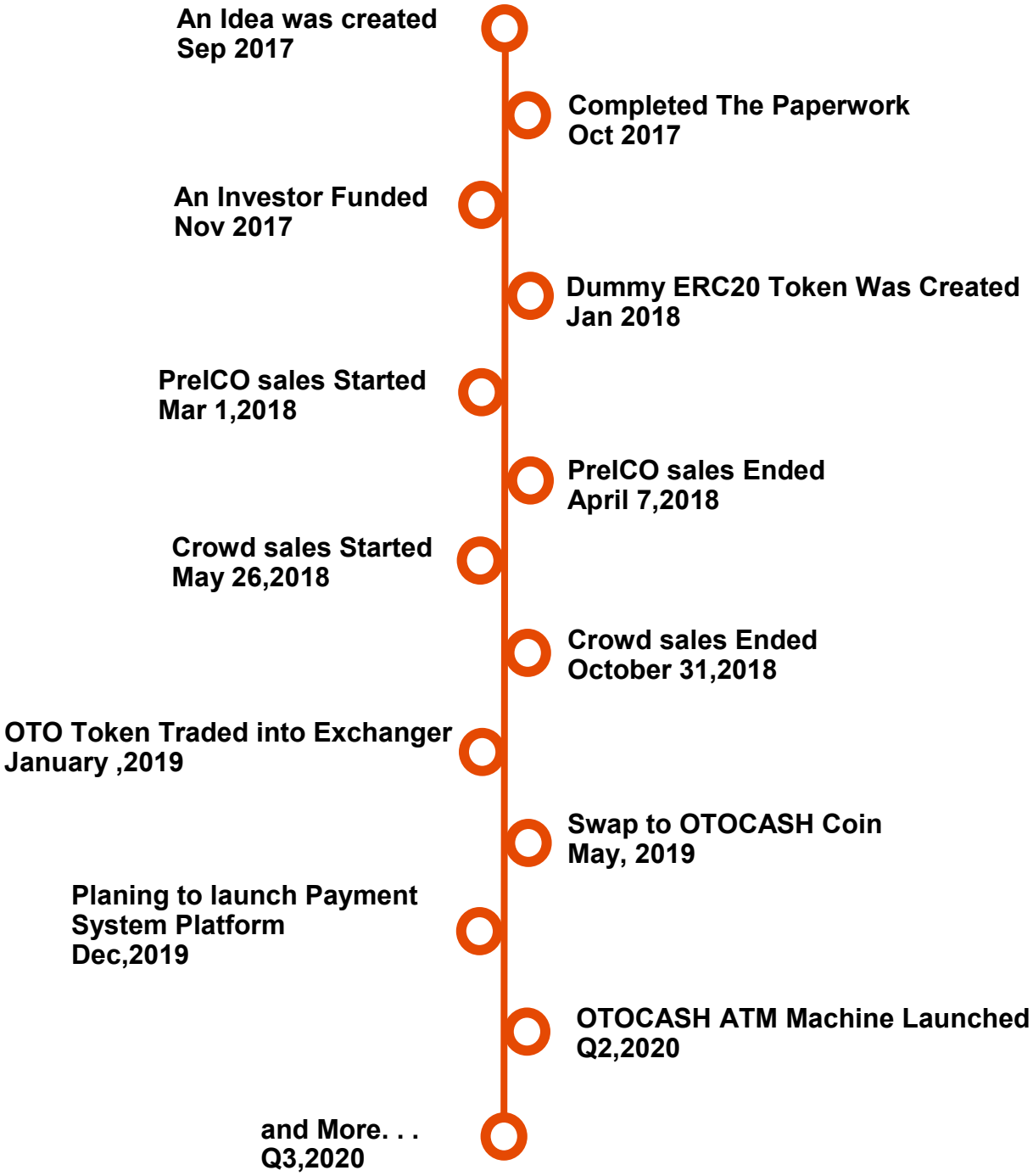
Premine: 38254582 OTO
Company Reserve: 5000000 OTO
Company Members: 2500000 OTO

## ICO

ICO Sold: 30754582 OTO
ICO Date: March 30,2018 – November 30, 2018
ICO Price: 0.00004 BTC – 0.00006 BTC With Bonus 10% – 60%

## ROADMAP

Our Road Map is a real workaround that we can give a real situation about OTOCASH timeline.



## Top Management Team

OTOCASH Enterprise runs operations by hiring contractors for most development work. Here are the top management details of OTOCASH Project.

Mr. Khairul Anuar

*Founder / CEO*

Mr. Azad Ashraf

*CFO*

### COMPANY CONTACT


**OTO CASH ENTERPRISE ( Reg No. IP0493634-K )**

**Register Certificate** [*See Documentation*]

**www.otocash.io**

**contact@otocash.io**


Note: All Programs and coin developed as specified in this Whitepaper and anything contained in the www.otocash.io website is not conducted by our parent companies and www.otocash.io do not use any license issued to companies under the OTOCASH GROUP. The website www.otocash.io is operated by OTO CASH Enterprise.