# BITTORIUM

BITTORIUM

Whitepaper v1
by Naeem Azad

**27/09/2018**

# ABSTRACT

Bittorium was created on 1st September 2018 by Naeem Azad.

The idea behind Bittorium was to create a Cryptocurrency for all, including low fees and maintaining the aspect of decentralisation disallowing political issues to cause a deficit in exchange rates. Privacy and the ability to spend on items we really want has become scarce in present times, with Bittorium users will not face this issue.

Bittorium is based on the foundation of Cryptonote technology.

The Cryptonote technology base allows users to transact with Bittorium anywhere in the world with low network fees and speed without compromising on privacy. We chose this algorithm and base due to its stability and its ability to add future features, also to allow miners to be rewarded for assisting in maintaining a healthy and secure network with PoW (Proof Of Work).

# 1. INTRODUCTION

The initial stage of Cryptocurrency has passed and increasing numbers of people are gathering knowledge on blockchain technology.

One successful example of what can be achieved is Bitcoin, it started with an idea and expanded to become a well known crypto peer to peer asset. Over the years a plethora of different types of Cryptocurrencies appeared but still not one has succeeded in mass adoption. Bittorium aims to target this to become a global payment method and introduce BTOR Pay, this will be a payment method at point of sale using contactless functionality.

# 2. USE CASES

We are in a digital age where people are relying on digital fiat currency (bank cards) to allow them to spend. The issue with fiat currency being it is controlled by political issues thus increasing prices and exchange rates. Blockchain technology is advancing daily and can solve these issues as only the people that use the Cryptocurrency decide on the value. With Bittorium users can transact anywhere in the world without high fees and a politically influenced exchange rate.

Bittorium is a project and does not represent an asset in any shape or form, we seek to become a global payment method and allow users to transact anywhere in the world with instant global access.

# 3. TECHNOLOGY

Bittorium is based on Cryptonote technology and has been forked from Pinkstarcoin, we amended the code and will continue to add to the project implementing new features. Bittorium uses Cryptonight Lite Variant 1 algorithm to allow users to interact private and securely.

Anyone can mine Bittorium to receive rewards (308 BTOR, decreasing over the next 30 years) to help build a powerful and fast network.

Bittorium will implement masternodes during development to build upon our plans.

## What are the Specifications?

Name: **Bittorium**

Ticker: **BTOR**

Max Supply: **180,000,000**

Decimals: **2**

Block Time: **240 seconds**

Algorithm: **Cryptonight Lite Variant 1**

# 4. WHAT IS CRYPTONOTE?

## Anonymous Payments:

Implemented ring signature technology allows the signing of payments on behalf of its users. This proves the payment was signed by its users but is indistinguishable.

## Unlinkable Transactions:

Using a variation of the Deffie-Hellman exchange protocol this releases multiple unique one-time addresses derived from the senders single public key.

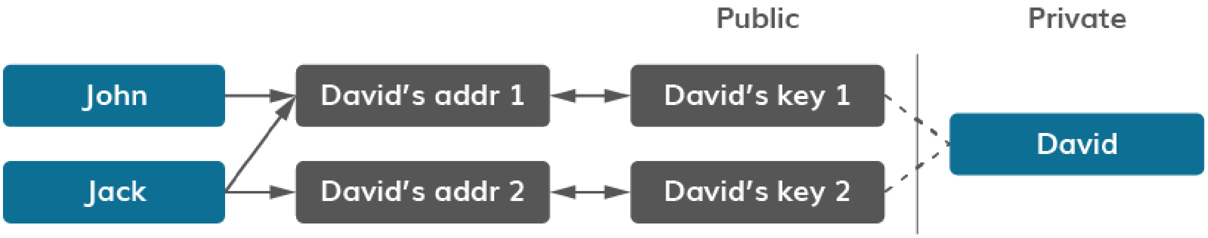

*Fig. 1. Traditional Bitcoin keys/ transactions model*

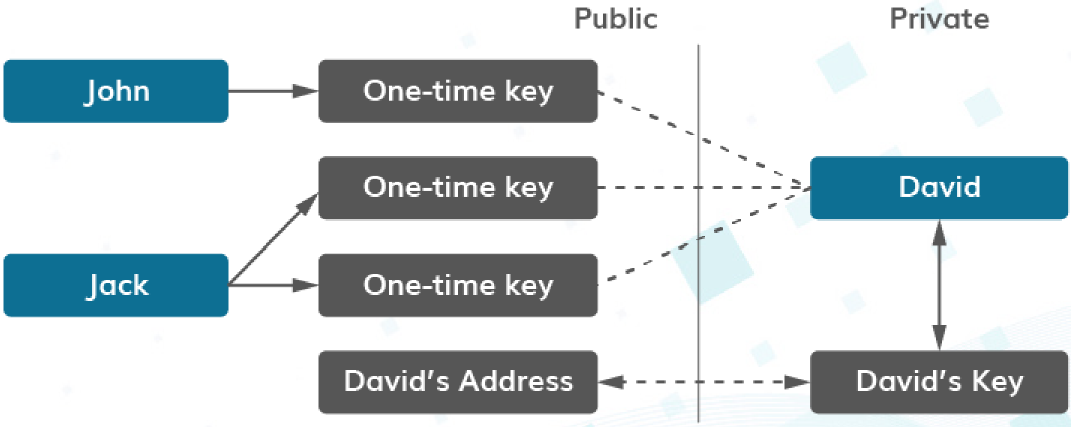

*Fig. 2. CryptoNote keys/transactions model.*

## Egalitarian Proof Of Work:

The primary goal is to close the gap between CPU (majority) and GPU/FPGA/ASIC (minority) miners. This allows users to mine from home using ordinary computers.

## Adaptive Parameters:

Cryptonote has no hard coded constants; the parameters are re-calculated based on the previous state of the network. This allows a dynamic and adaptive network.

## Double-Spending Proof:

Every signature contains a fingerprint key image of the secret key. This implies that given only the key image it is impossible to restore the corresponding secret key.

## Blockchain Analysis Resistance:

Non-repeating one-time addresses and mixed keys in ring signatures make the whole blockchain resistant to analysis. With every transaction this resistance grows.

# 5. BTOR PAY

Over the years spending has become easier as new features have been implemented to allow fiat currency to be spent. Contactless has become a typical way of transacting but raises concerns to security and privacy. With BTOR Pay, we aim to build on the concept of contactless but allow users data to stay private but also to transact more securely.

Users will be able to use BTOR Pay on smartphones and smartwatches to make payments with ease but maintaining the aspect of privacy and security.

Smartphones have become a vital part in peoples lives and BTOR Pay will be an application that can be loaded on to these. People that have no access to smartphones can also interact with BTOR Pay users with QR codes or using one of our wallets.

Payment terminals will be modified to allow Bittorium to be used, this is easily achieved through building relationships with major businesses to allow Bittorium to be accepted as a method of payment.

BTOR PAY

# 6. CONCLUSION

Bittorium is an ongoing project that has an aim to become a global currency to allow users to transact without privacy issues or speed concerns. Allowing usage to anyone in the world and tackle the need to exchange or pay more due to political tensions.

Bittorium will implement masternodes to add to the health of the network and to allow usage anywhere without the issue of storage capacity.

BTOR Pay will be used to spend on anything users like without the issue of privacy. All this will lead to the mass adoption of Cryptocurrency.