Bitcoin Cash Private

contents

Subject Page Number

ABSTRACT

Bitcoin Cash Private (BCHP) is a fork of Bitcoin Cash based on a fully private Blockchain framework. It allows for private transactions, with the development of zkSNARKs and the smart contract capabilities alongside a revolutionary DAO engine.

The fork will take place on the 5th of August. We plan to list on popular cryptocurrency exchanges (Pre-Fork and Post-Fork) some of these will include Etherdelta, Forkdelta, Token Store, Coinexchange and a mystery exchange. Taking the form of an ERC-20 token during the airdrop 8,000,000 tokens will be distributed to people submitting their details to a google form, and a further 21,000,000 tokens will be given to BCH holders.

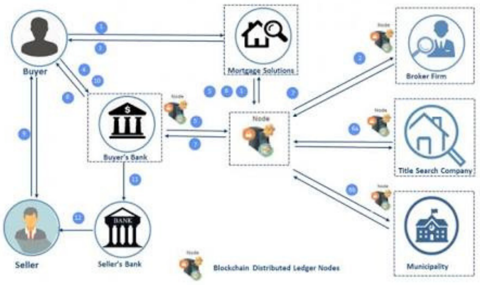
The fork will take place for 3 major purposes – to improve transaction speed and scalability, to increase the amount of privacy and security available to users, and to embed the useful smart contract functionality which is often limited to Ethereum, along with some useful new features. It is the firm belief of the BCHP team that privacy must be protected and improved, and that smart contracts are the next frontier in the world of online transactions. Bitcoin Cash and other existing tokens like Bitcoin and Zcash are currently failing at combining all of these features into one useful format.

By combining the unmatched potential for trustless transactions provided by zkSNARKs with increased block sizes and significantly reduced block times, alongside the implementation of smart contracting capabilities, it is believed the Bitcoin Cash Private will position itself as the cryptocurrency to lead the blockchain ecosystem to the next phase of burgeoning evolution.

Introduction

This paper will address some topics and ideas that may be unfamiliar to those without a solid grounding in blockchain and cryptocurrency technology, so it is instructive to first of all establish a few definitions before going further. These are some terms that need to be explored in order to understand the operational framework and utility of the Bitcoin Cash Private.

Blockchain: A blockchain, according to the standard definition is a network that is decentralized and distributed across all its nodes so that the network cannot be compromised by any single node. In plain English, what that means is that a chain of little bits of data called ‘blocks’ being created, updated and stored across several different locations in real-time is called a ‘blockchain’.



The major difference between blockchain networks and regular centralized networks is that blockchains do not have a “server” or a “headquarters” where isolated information exists in a silo. Blockchains instead make use of the entire network of nodes as their storage and processing capacity, and each node has a copy of the blockchain which is constantly in communication with the others, verifying transactions and comparing information to make sure the data across all of them is exactly the same. If any single node has data that does not match with that on the rest of the blockchain network, it is immediately isolated as a compromised node and the network automatically excludes it and keeps on functioning.

What this means to the uninitiated is that the blockchains are very secure, possessing no single location that can be hacked or compromised in any way, and not permitting any variation in data across network nodes. Data stored on a blockchain is thus practically immutable and unchangeable, which makes it ideal for recording sensitive data like transaction records and medical records. A graphical illustration of the Blockchain process is provided below:

Cryptocurrency: A cryptocurrency is a representation of a digital asset, and it is also sometimes referred to as a token or a coin. Cryptocurrencies contain no information that can be used to personally identify their users, and as such they have gained popularity around the world for a variety of reasons as ‘anonymous currency’.

A vast number of cryptocurrencies exist currently, ranging from the ubiquitous Bitcoin (BTC) and Ethereum (ETH) to a basket of currencies including Ripple (XRP), Monero (XMR), Tron (TRX) and for the purposes of this paper, the cryptocurrency that will be focused on is Bitcoin Cash Private (BCHP), which is a fork of Bitcoin Cash.

Flat Currency: A flat currency is the money most people are familiar with, I.e money that is issued and backed by a government institution and usually regulated by a central banking institution. Unlike cryptocurrencies, flat currencies (even when stored electronically) contain identifying information and are stored in centralized silos rather than across a decentralized networks

Fork: A fork is a situation that occurs when a cryptocurrency splits in two. It may either be a soft fork or a hard fork. In the case of a soft fork, the cryptocurrency’s code is changed and users adopt the changed token on the same blockchain. In other words, users adopt an update and continue making use of the token as normal, abandoning the old version. In theory, a split has still occurred (bear in mind that any kind of data stored on a blockchain including cryptocurrency code cannot be edited, hence an update to the code must take the form of a completely new a separate code). In the case if a hard fork however, the new cryptocurrency is not intended to replace the old one, but to split off into a separate blockchain and exist concurrently alongside it. Some popular examples of cryptocurrency hard forks include the split of Bitcoin into Bitcoin Cash, and the split of Ethereum into Ethereum Classic. Bitcoin Cash Private is a hard fork of Bitcoin Cash, which has a number of advantages over Bitcoin Cash.

Smart Contract: A smart contract is a method of exchanging value between two or more parties using the blockchain as a tool for validation and escrow. It is a program containing a set of instructions which guide online transactions and exchanges of value. Smart contracts use the blockchain as a validator and escrow solution, cutting out the need or the middleman and exponentially increasing the fidelity of transactions.

Using a smart contract, a seller and a buyer involved in a peer-to-peer transaction do not need to have a middleman interceding between them to ensure that the right exchange is made at the right time.

Rather, a set of conditions, instructions and parameters is coded into a safe wallet under the care of the smart contract protocol. Once the buyer confirms that they have received the requested value from the seller and it is acceptable to them, the smart contract automatically releases the payment to the seller.

DAO: Provided by the Azurite Network, a Decentralized Autonomous Organization (DAO), also known as a Decentralized Autonomous Corporation (DAC) is one of whose sole purpose for existence is essentially to execute a number of smart contracts. The technology underpinning the smart contract is deployed in conjunction with a financial transaction record on the blockchain, so that a large number of recurring transactions can take place automatically and with minimal investment in hardware. In other words, this is a fully automated organisation that has the capacity to run with practically zero human input.

zkSNARKs: This is a relatively new security protocol within the blockchain ecosystem that is slowly gaining popularity among so-called ‘security tokens’ such as Zcash. The zkSNARKs framework is built on a variant of zero-knowledge cryptography, which is a field that deals with data security using encryption that is practically impossible to break because it does not function as a regular ‘lock and key’ system. With zSNARKs, entitles conducting a transaction with each other on the blockchain who need to verify certain information about each other can do so without actually revealing that information. For example, in case of a purchase transaction where the buyer is required to show evidence of their possession of the required cryptocurrency amount, probably by means of their secret token wallet key, it is possible to verify the necessary information without the buyer revealing the secret key to another party. This security framework is potentially the next innovation in the blockchain ecosystem as users continue to explore improved individual security and personal privacy. BCHP combines all the features of BCH and adds the security layer of zkSNARKs, which makes this token one of the most secure cryptocurrencies in existence.

Now that these terms have been defined, it is time to delve into the world of Bitcoin Cash Private and examine what it does and why.

Features

BCHP will be one of the first blockchains to allow smart contracts with complete transaction privacy. The integration of the cutting-edge DAO Management Engine (DAOME) also makes it very easy for regular users to create a DAO or execute smart contracts on the BCHP blockchain.

SPEED

In the world of online payments, cryptocurrencies are still a long way behind fiat providers, and a key reason for this is the yawning difference that exists between them in terms of speed of transaction processing. Where PayPal handles roughly 193 transactions per second, and Visa manages 1667 transactions per second, Ethereum manages to process only about 20 transactions per second, while Bitcoin lags further behind with 7 per second. Bitcoin Cash Private is a substantial upgrade on these fairly dismal figures, which makes BCHP among the fastest coins in the market.

PRIVACY

Due to the utilization of the revolutionary zkSNARKs technology, BCHP is able to provide private transactions that are similar to those in Monero, Zclassic and other privacy coins. zSNARKs (Zero-Knowledge succinct Non-Interactive Argument of Knowledge) is a security framework that enables a party in a transaction to show that they have certain authentic information, such as a secret key to a crypto wallet, without actually revealing the information. In other words, it is a verification tool that makes it possible for parties in a blockchain transaction to ‘trust’ each other without actually ‘trusting’ each other. It is a very useful way of setting up trust-less frameworks for transactions without any sensitive information being revealed by either party.

SCALABILITY

It has been established that the principal impediment to the growth of cryptocurrency payments has been poor block times, but what has not been mentioned is that a large part of the reason for the long lag is relatively tiny block sizes available. BTC for example, has a block size of just 1MB in order to keep the Bitcoin blockchain free of spam transactions. In theory, this has lead to a situation where performing transaction hashes in order to put transactions into the Bitcoin blockchain has become an extremely difficult and time-consuming process. The current situation benefits no one except miners whose fees are directly proportional to the difficulty of hashing. BCHP solves this problem by utilizing a significantly increased block size, which is carefully calculated to ease the difficulty of hashing without creating a centralization risk or discouraging miners, which could potentially reduce the blockchain's hash rate. Bitcoin Cash Private is capable of doing over 30TPS, which is 7.5 times more than bitcoin.

SMART CONTRACTS

Building on the excellent concept of the Ethereum smart contract, BCHP will be one of the first blockchains to allow smart contracts with complete transaction privacy. In other words, BCHP users will be able to carry out transactions which are completely private and free from scrutiny, which Ethereum does not currently permit. Furthermore, Azurite Network will be designing and managing the DAO. This means that BCHP is uniquely poised to become the preferred platform for secure transactions that are fully private and anonymous.

Details

PRE-FORK (TOKEN)

MAX SUPPLY: 8,000,000

TOKEN SYMBOL: BCHP

DECIMALS: 18

CONTRACT ADDRESS: 0x83e8Ec3C405Eb0861C55f865294dEfa00F504068

POST-FORK (COIN)

MAX SUPPLY: 29,000,000

COIN SYMBOL: BCHP

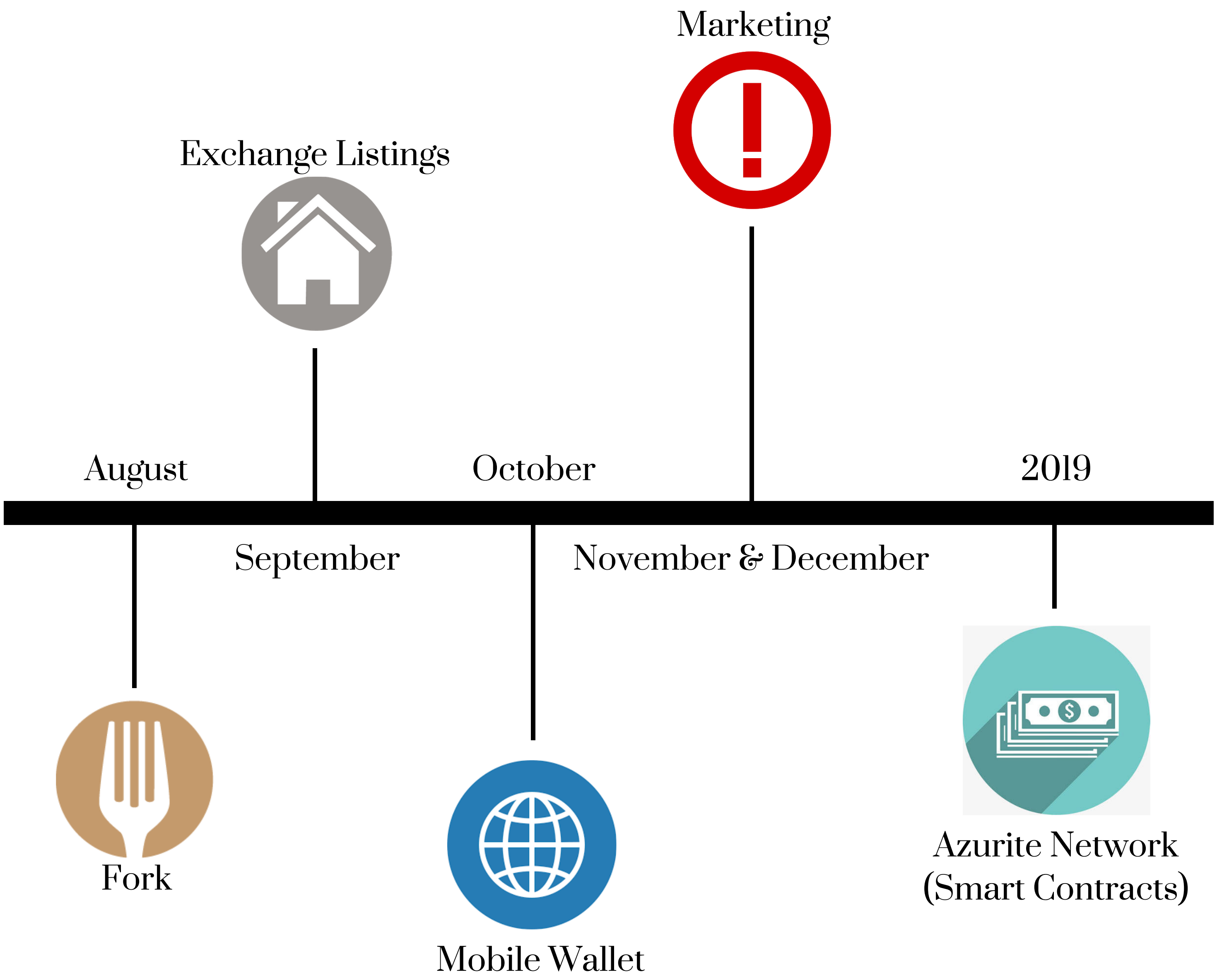
BLOCK TIMES & REWARD: Same as BCH

PRIVACY TECH: zkSNARK

HASHING ALGORITHM: EQUIHASH

Roadmap

There is also a plan to develop mobile wallets capable of integrating with Android and iOS devices. Work on these has already begun and the results will be communicated in due course.



August

Fork

Exchange Listings

September

October

Mobile Wallet

Marketing

November & December

2019

Azurite Network (Smart Contracts)

Team

Chris Philips / Project Lead

Chris leads the team as well as working to implement smart contracts into Bitcoin Cash Private and forking the Bitcoin Cash blockchain. Chris is… the silent type, but is very persuasive when he needs to be.

"Inanenova" / Lead Blockchain Developer

Nova is adjusting and implementing zero knowledge proofs (zkSNARKs) and the direction of Azurite Network which will provide our DAO (Smart Contracts), this requires him to lead a team of developers.

“Sharkfish” / Community Manager

“Sharkfish” works as the community manager and at Bitcoin Cash Private, he has chosen to use a pseudonym. Works with us remotely.

Aubrey Ling / Web and Graphic Design Developer

Aubrey’s a pretty damn good graphic designer, she created and now maintains our website. She enjoys traveling and has been to over 12 countries.

Mark “Snoopy” Davis / Marketing Lead

Mark specializes in the marketing aspect of Bitcoin Cash Private, helping with the growth of the community. Known for his cool head under tough situations.

Robert Fellows / Software Engineer

Robert is out in house software engineer, developing our mobile applications and future payment platform. Wishes to make his mark in the world of cryptocurrency.

conclusion

Bitcoin Cash Private is a uniquely useful cryptocurrency solution that solves the 4 basic problems that exist with Bitcoin and other cryptocurrencies.

- It delivers a block time that matches Bitcoin Cash, with speeds of up to 7.5 times that of BTC and 2 times that of ETH. In so doing, it not only improves on the operational efficiency of Bitcoin, but it also moves the cryptocurrency ecosystem closer toward the goal of being able to offer similar transaction speeds and reliability as that offered by conventional fiat transaction processors.

- It solves the scalability problem of Bitcoin by increasing the block sizes within a carefully calculated tradeoff with security needs. This enables transactions to be hashed at a much quicker rate, increasing the capacity of the bitcoin blockchain to handle transactions without opening the platform up to the risk of centralization or reduced hash rate due to disincenvtized miners.

- Using the revolutionary zkSNARKs framework, BCHP ensures that a greater level of transaction security and privacy is achieved than is possible with BCH. Under this framework, a party in a transaction is able to provide proof of their possession of a certain credential such as a secret key without actually revealing the credential, which has enormous positive implications for any

- BCHP makes use of Azurite Network's planned smart contract capability, making it possible for the first time to make use of smart contracts with a privatized coin.

Disclaimer

The Bitcoin Cash Private service and the Bitcoin Cash Private platform are provided strictly on an “ as available” and “as is” basis. No assurances or representations of any type, direct or otherwise, are made regarding the operation of the service or content, information, materials, or products displayed on the website.

No express or implied representations or warranties regarding the Bitcoin Cash Private service and website, or the products or services provided therein are made. Therefore, any implied warranties of Bitcoin Cash Private merchantability, fitness for a particular purpose, and non-infringement are expressly disclaimed and excluded. In addition, we make no representation that the operation of our service will be uninterrupted or error free, and we will not be liable for the consequences of any interruptions or errors be they direct, secondary, related, penal, or consequential.

BCHP should not be treated as an investment. There is no guarantee that the BCHP you purchase will increase in value and/or provide any return.

Bitcoin Cash Private does not confer exclusive ownership or arbitrary right to control. Possession of BCHP tokens does not grant the holder exclusive ownership or sole equity in the Bitcoin Cash Private platform as a whole. No one individual has exclusive rights or power over the decentralized Bitcoin Cash Private platform.

The purchaser’s BCHP can only be accessed with private keys held by the purchaser’. The loss of the private key will result in the loss of BCHP. To prevent such a situation, it is strongly advised that the holder should safely store private keys in one or more backup locations that are geographically separated from the working location, and are accessible in the event of an emergency.

As they grow in popularity and application, Blockchain technologies have also become subject to regulatory attention and action by the government and financial industry organizations around the world. Although not likely, the functioning of the Bitcoin Cash Private platform and BCHP tokens could be impacted by any regulatory inquiries or actions, including but not limited to restrictions on the use or possession of digital tokens like BCHP, which could impede or limit the development of the Bitcoin Cash Private platform.

The purchaser's BCHP can only be accessed with private keys held by the purchaser'. The loss of the private key will result in the loss of BCHP. To prevent such a situation, it is strongly advised that the holder should safely store private keys in one or more backup locations that are geographically separated from the working location, and are accessible in the event of an emergency.

As they grow in popularity and application, Blockchain technologies have also become subject to regulatory attention and action by the government and financial industry organizations around the world. Although not likely, the functioning of the Bitcoin Cash Private platform and BCHP tokens could be impacted by any regulatory inquiries or actions, including but not limited to restrictions on the use or possession of digital tokens like BCHP, which could impede or limit the development of the Bitcoin Cash Private platform.

It is possible that the Bitcoin Cash Private platform will not be used by large numbers or individuals, and that there will be limited public interest in the creation and development of the distributed applications. Such a lack of interest could impact the development of the Bitcoin Cash Private platform and therefore potential uses or value of BCHP.

The Bitcoin Cash Private platform is presently under development and may undergo significant changes before its full release. Any expectations regarding the form and the functionality of BCHP or the Bitcoin Cash Private platform held by the purchaser may not be met upon release, for any number of reasons including a change in the design and implementation plans and execution of the Bitcoin Cash Private platform.

Hackers or other groups or organizations may attempt to interfere with the Bitcoin Cash Private platform and/or website, or the availability of BCHP in any number of ways, team members may operate under pseudonyms to protect their identities.