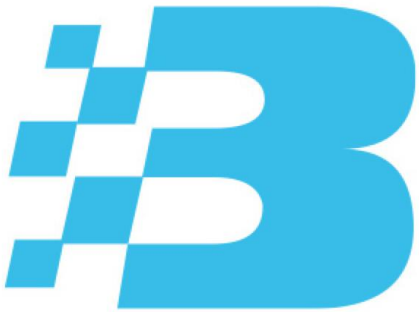


UB.com
UnitedBitcoin

White Paper

Silicon Valley
12 December 2017

Last updated
10 May 2018

Table of Contents

Part One: Abstract

(UB coin = UBTC)

As an excellent representative of digital currencies, Bitcoin brings irreversible transaction implementation and decentralized consensus to the world. Bitcoin's price reflects its value as a disruptive technology, a store of value, and a medium of exchange. Even with the advent of numerous altcoins, Bitcoin has remained dominant in the space and has found increased legitimacy in the eyes of traditional markets through futures trading.

Bitcoin is the best example of applied blockchain technology. It was started and initially adopted by technology enthusiasts and is now spreading around the world.

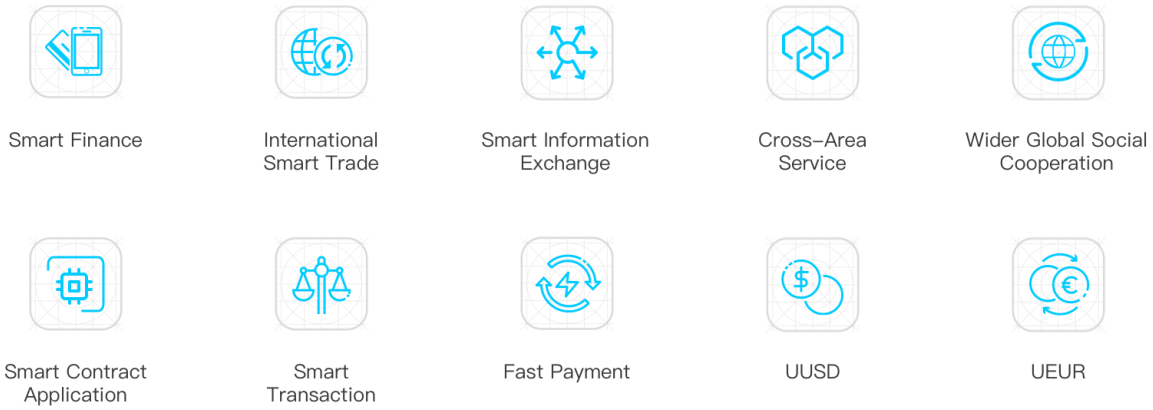
Bitcoin functions as a currency. However, Bitcoin's value was initially extremely low. Consequently, people did not take the necessary security precautions. While technically these Bitcoins haven't gone anywhere, in practice they lower the circulating supply of Bitcoin. Without private keys these coins are locked away, unable to be reclaimed.

While this is deflationary and has driven Bitcoin's price up, it is not enough to aid further development. Its high price, high transaction costs and low quantity of available Bitcoin will limit its growth.

The mission of UB is to find a purpose for lost Bitcoin and inactive wallets, and create a stable cryptocurrency system (UB Stable Coin) through an association of joint credit and smart contracts.

UB will use the pressure-tested mechanics of Bitcoin, while it upgrades areas to accommodate for larger social demands. These improvements will be an increase in block size to 8mb, the addition of smart contract support based on UVM, and Segregated Witness (SegWit) implementation.

Business vision:



Part Two: Operating Model

UB forked away from the Bitcoin network, and immediately improved its protocol in the new network. All active Bitcoin addresses received corresponding balances on UB's chain.

Balances of inactive addresses were collected and are being used to serve the active community and grow the ecosystem.

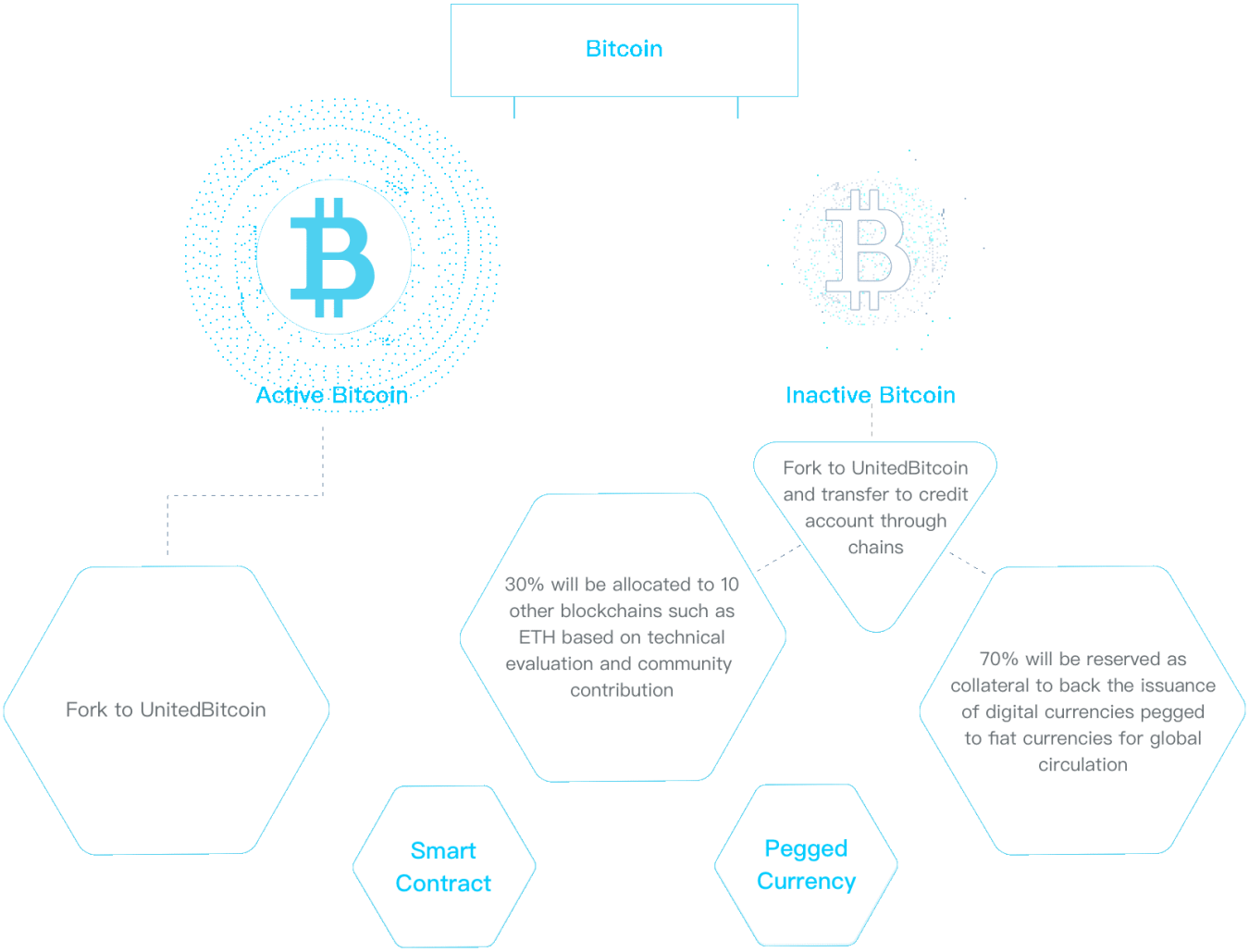
30% of the inactive balances have been used to grow the eco-system which includes distribution to other technologically influential communities in the cryptocurrencies space to further increase the influence and adoption of UB. This redistribution finished on 12 May 2018

70% of the inactive balances have been reserved as collateral to issue UB Stable Coin (https://ubpay.io/) pegged to chosen fiat currencies, similar to a gold standard. However, unlike a gold standard where the mint ratio (the fixed exchange rate between gold and dollar value) tends to overvalue gold, the UB standard is designed to keep the reserve UBTC value over-collateralized against the value of the issued pegged coins. The ratio is targeted to be around 3:1 (i.e. for every UBTC reserved, we can only issue UB Stable Coin up to 33.3% of one coin's market value). If the market price of UBTC increases, then it provides more value capacity to issue more stable coins, but no new stable coins will necessarily be issued; if the market price of UBTC decreases such that the value of UB Stable Coin breaches 33.3% value of the reserved UBTC, then this initiates the Stable Coin to be bought back until the 33.3% safe line is satisfied. This is similar to how the Federal Reserve interacts with the US Dollar Liquidity Fund.

The UB Stable Coin backed by UBTC reserves is intended for use in global trade or large-scale projects which may result in a greatly enhanced ease of use and popularity of UB's systems.

UB is set to become a global savings union of joint credit. The new smart contract function will also provide infinite possibilities to UB.

Differentiation between active and inactive bitcoins:



Part Three: Technical Solutions

While Bitcoin is by far the most secure and most dominant cryptocurrency right now, it also has some imperfections, mainly because it was the first.

3.1 UTXO Data Model

Over the last nine years, the UTXO data model used in Bitcoin has proven to be a dependable way to create a stable and reliable digital currency. The most important function of a currency is to be a medium-of-exchange and the UTXO model does this wonderfully. Inheriting this through the fork is of utmost importance to UB.

3.2 SHA256 PoW Mining Model

UB keeps the mining algorithm of Bitcoin. Although energy consumption is a concern with PoW (proof of work), it has a very solid track record and has demonstrated itself to be very secure. A hybrid consensus model where mining will be partially based on PoW and partially on PoS (proof of stake) is being explored.

3.3 Total Quantity and Block Time

UB is a fork of Bitcoin and inherited its block time, halving time and total number of Bitcoin's cap (21 million). Following an upgrade of the network at block 506,400 the following adjustments were made;

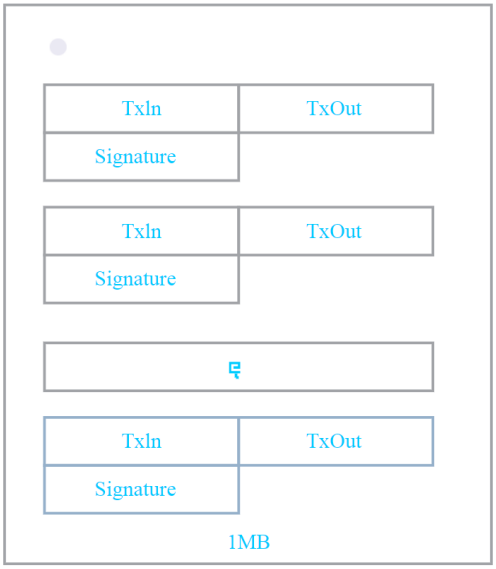
1. Targeted block speed adjusted to 1 minute
2. Difficulty adjustment cycle was adjusted to 10 blocks
3. Bock reward was adjusted to 1 UBTC
4. Reward lock up period adjusted to 7,200 blocks

The total resulting supply cap is 20,166,000

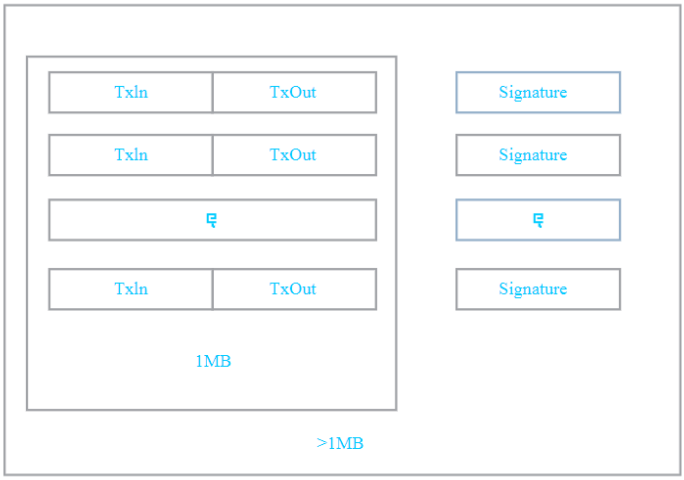
3.4 Segregated Witness / SegWit

SegWit is the data structure improvement that puts digital signatures of TX_IN and TX_OUT outside the transaction. This solves the problem of transaction extensibility and eases the problem of block size limits; enhancing on-chain scalability.

Before implementation of SegWit, the structure of the blockchain is as follows:



After implementation of SegWit, the structure of the blockchain is as follows:



3.5 On-Chain Scalability

Bitcoin's current maximum number of transactions per second is around 7tps. This does not accommodate the network's needs at times, and therefore cannot begin to handle the needs of global transaction volume.

The implementation of SegWit, mentioned earlier, alleviates some of this, but only to a limited extent. Increasing the block size will result in a greater alleviation and provide significant room to grow, however this requires a hard fork.

Increasing the block size increases network requirements. However, considering that most nodes are run by mining pools or companies and the feedback we have received from miners regarding this, we conclude this isn't too much of a constraint and 8MB is an adequate value.

3.6 Replay Protection

Because UB is a fork of Bitcoin, we must ensure that transactions on one chain cannot be replayed on another chain. UB implements replay protection by introducing new transaction signatures. New SigHash types will also improve the overall security of the network.

3.7 Asset Activation

After the fork, all active addresses on the Bitcoin network received equivalent balances on the UB network. Inactive addresses are addresses without activity since block height 494,000 (11 November 2017) and as a result did not automatically receive UBTC during Phase 1 of the asset allocation procedure.

Full details of the allocation procedure can be found on our website https://www.ub.com/project/get

3.8 Smart Contracts

UB's smart contracts allow users to write customized behaviors and use them in the blockchain, rather than having to do several (manual) predefined operations. By using smart contracts, users can easily configure complex transaction logic, as well as execute complex financial contracts. At the same time, users can extend functionality, add restrictions or add dynamic controls, without modifying or upgrading the blockchain.

Smart contracts allow users to register customized contract bytecode in the blockchain and invoke transactions in UB's chain. The bytecode is executed in a Turing-complete virtual machine for blockchain.

Developers can write smart contracts using a programming language with friendly syntax (C#, Java, LUA or Kotlin), which is then compiled into contract bytecode and stored in the blockchain.

Each node of UB synchronizes the blockchain and invokes a virtual machine to perform and verify the relevant contract bytecode.

3.8.1 Types of Contract Transactions

The ScriptPubKey lock script area of the transaction can increase the contract related operators to trigger registration of the contract, invoke the contract, upgrade the contract, and/or cancel the contract.

Transactions with these operators will trigger the smart contract virtual machine to perform the associated contract bytecode.

The operator of the registration of the contract will execute the contract bytecode to register on the chain as a new smart contract, and once successful a new smart contract address will be assigned.

The operator that invokes the contract on the chain, executes the corresponding bytecode, and generates certain execution results, such as transfer or contract status changes.

The operator that upgrades a contract can assign a unique name to an un-upgraded and unwritten contract on the blockchain and mark the contract as un-cancellable. This smart contract is invoked by the user or other contract by the contract name.

The operator that cancels a contract can mark an un-upgraded and unwritten contract on the user-created blockchain as cancelled. The cancelled contract will not disappear from the blockchain, but cannot be called again, only the relevant historical data can be queried.

3.8.2 Contract Virtual Machine

The contract virtual machine is designed to be Turing-complete. The contract virtual machine has a high performance, is scalable and can interact with the UB blockchain. It can run smart contracts and return the results.

The contract virtual machine of UB has the characteristics of definitiveness, and the same results can be found at any time after the transaction of a contract is recorded on the blockchain, which can be verified and confirmed.

Developers can use a variety of high-level programming languages for smart contract development, and compile and generate contract bytecode to be stored in UB's blockchain.

After weighing different options, UB has decided to adopt a UVM virtual machine, which is based on improvements of LUA, and subsequently supports simulated languages similar to C#, Java and Kotlin. The UVM is one of the most efficient virtual machines and its underlying language has been used for years in practical applications.

In terms of security, the UVM will remove some functionality such as external IO. In terms of stability, the UVM ensures graceful termination and continual executions.

3.8.3 Mechanism of Gas

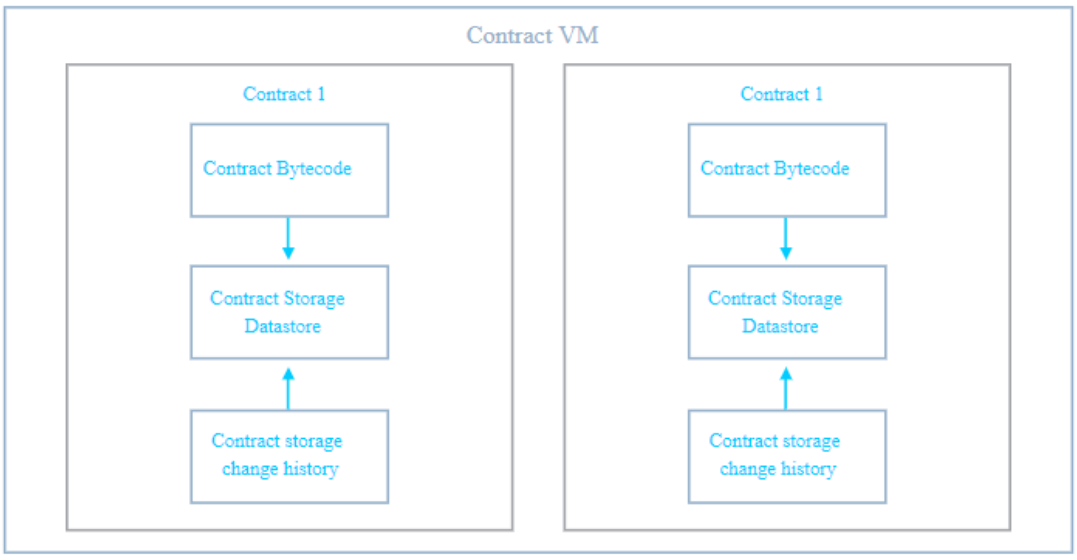
The implementation of smart contracts requires gas, which is the economic cost of implementing smart contracts. Gas in UB's Chain uses UBTC as system base coins. The gas mechanism increases the economic disincentive of attacking the blockchain ensuring stability.

Different contract calls require a different amount of gas, depending on the number of contract bytecode instructions and the types of instructions in the execution process.

3.8.4 Contract State Storage

Each smart contract has an isolated storage area for housekeeping, and to record the status data of the smart contract. When the contract is executed, it can modify or query the storage of the contract. Changes to the storage can only be submitted to the blockchain if execution succeeds. When retroversion of a block of blockchain occurs, the storage of the contract needs to revert back to its previous state, based on the history of the storage.

The functions of the smart contract virtual machine are as follows:



3.8.5 Contract Books

Each smart contract has a contract address, and the contract address can possess blockchain assets and receive transfers. During contract execution, transactions arising from a contract transfer to another address, following the execution of a contract call, are known as result transactions. The result transaction's ScriptPubKey lock script region contains scripts from contract transfers to other addresses. The assets of the contract address are transferred out of contract execution and consensus, without the need for a private key to sign the behavior of the contract address asset.

Part Four: Timeline

11th December 2017	Phase 1 distribution
12th December 2017	UB launch in Silicon Valley
15th December 2017	Ambassador program announced
22nd December 2017	Full node reward program announcement
29th December 2017	Open Letter to UBTC community (including Phase 2 process)
3rd January 2018	Phase 2 distribution announcement
4th January 2018	Final block height to end Phase 2 is 502,315.
13th January 2018	Phase 2 grace period announcement
14th January 2018	Roadshow in Shanghai
15th January 2018	Documentary, episode 1 released
19th January 2018	Documentary, episode 2 released
22nd January 2018	Distribution community airdrop distribution announcement
24th January 2018	Phase 2 distribution begins
30th January 2018	Documentary, episode 3 released
1st February 2018	First HSR & QTUM snapshot at UTC 12pm
11th February 2018	First ETH & LTC snapshot at UTC 12pm
14th February 2018	Phase 2 grace period ends
15th February 2018	Phase 2 grace period distribution
21st February 2018	First INK snapshot at UTC 12pm
1st March 2018	Second HSR & QTUM snapshot at UTC 12pm
11th March 2018	Second ETH & LTC snapshot at UTC 12pm
15th March 2018	Phase 2 distribution ends
21st March 2018	Second INK snapshot at UTC 12pm
1st April 2018	Final HSR & QTUM snapshot at UTC 12pm
3rd April 2018	UBPay & Stablecoin launch
9th April 2018	Meet up in Hong Kong
10th April 2018	Network upgrade
11th April 2018	Final ETH & LTC snapshot at UTC 12pm
18th April 2018	Launch of Smart Contracts on UB TestNet
21st April 2018	Final INK snapshot at UTC 12pm
14th – 16th May 2018	UB at Consensus conference in New York

Coming Soon

- Smart contract support
- Hybrid consensus

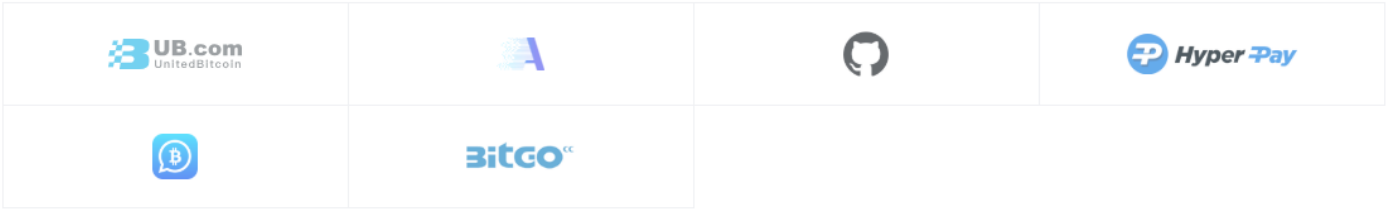
Part Five: Ecosystem

5.1 Exchanges

UBTC can be traded at a number of exchanges, including:

5.2 Wallets & Full Nodes

UnitedBitcoin provides a number of wallets including a CLI full node, QT-wallet and light wallet based on Electrum. Next an increasing number of third party wallets support UBTC.



5.3 Block Explorers

Next to the block explorer provided by UnitedBitcoin, Bitbank provides a block explorer for the UB blockchain.

5.4 Pools

Pool mining is supported by several mining pools, including: