Bitcoin Vault Whitepaper

Eyal Avramovich, Kacper Wiśniewski, Piotr Kozłowski, Radek Popiel et Anon

Whitepaper v1.0

Abstract

In 2009 an anonymous individual or team of anonymous developers created the first peer-to-peer network based on the blockchain technology that allowed users to transfer funds between anonymized hash addresses. Bitcoin revolution had begun. It resulted in a series of forks of the original concept.

One of them has led to the concept of Bitcoin Vault.

Our aim as developers was to upgrade the existing blockchain with unique features that would give users more control and raise their safety level with the way wallets addresses are managed, private and public keys are stored, and assets are transferred between individuals. We wanted to create a coin that would offer all the advantages of Bitcoin with additional features for users to have maximum control of their assets in an easy and convenient way without compromising the flexibility that cryptocurrencies offer.

With immutability of the blockchain as the key feature behind distributed ledgers, we saw not only advantages but also – from our own experiences – dangers related to lost, misplaced or stolen funds. With several changes into the code and the way how private and public keys are used in the blockchain ecosystem we came up with an idea of making irreversible transactions reversible without compromising the immutability of the blockchain.

Contents

Introduction

Bitcoin Vault (BTCV) was launched in 2019 as an alpha chain. It was development heavily between December 2019 and November 2020, which saw the release of the key feature enabling reversible transactions on the blockchain

Bitcoin Vault is the world's first cryptocurrency that allows users to cancel transactions after they are posted to the blockchain. This revolutionary approach is possible with a customized blockchain protocol which confirms payments within 144 blocks (or around 24 hours). This feature protects users from losing their funds in case of common key thefts, user mistakes or errors and bugs.

Bitcoin Vault is a hard fork of Bitcoin Royale, adding one private key to the process, bringing the total to three. Since launching in late 2019, we have expanded the technical and market foundations in line with an ambitious roadmap extending to 2022 and beyond.

Problem Statement

According to CipherTrace's Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report, in the first five months of 2020, crypto thefts, hacks, and frauds totaled $1.36 billion.

Cryptocurrency exchanges need to recover user funds that were mistakenly sent to the wrong addresses on daily basis. This costs them both time and money and do not guarantee that user funds will be recovered.

There are no reliable sources on how many crypto assets, coins, tokes are being transferred every day to well-known scam addresses, hackers or are being lost due to Man-In-The-Middle types of attacks.

We believe that a significant portion of the above could be avoided if the user had the possibility to simply cancel and reverse outgoing transactions as soon as he realizes that he made a mistake, assets have been stolen, or someone gained unauthorized access to the cryptocurrency wallet.

Mission & Vision

BTCV was developed to provide an extra level of security based on a 3-Key Security Solution which allows users to reverse certain types of transactions on the blockchain. It features all the convenience of Bitcoin while adding important features allowing user transparency and freedom. Bitcoin Vault is our answer to issues faced by the crypto community over the last decade which mainly are:

1. Unauthorized access to wallets due to either hacks or accessing user private keys,
2. Human mistakes with sending crypto assets to the wrong wallet addresses or other kind of mistakes related to mistyping transfer amounts or mixing transfer amount with gas amount,
3. Errors, bugs and other issues related to the cryptocurrency software.

BTCV development is focused on security and safety features, user convenience and user experience as we also believe that those are the key challenges that prevent significant portion of society to become part of global crypto community.

BTCV approach

Cryptocurrencies gave users freedom and responsibility over how they store, manage and transfer funds across P2P networks. In this white paper, we assume that every cryptocurrency user should be familiar with the concept of private and public key and know how to safely store and secure keys. Based on this assumption, we have developed a new approach to key management and its usage for various types of transactions.

3-Keys Security Solution

Bitcoin Vault developed a 3-Key Security Solution which requires users to generate three Elliptic Curve Digital Signature Algorithm (ECDSA) keys – one is stored automatically within the app and the other two need to be managed by the user. The current setup in Bitcoin Vault allows users to cancel initiated transaction and reverse it to an existing or a new wallet address.

Solution supports three ECDSA key with different roles in the ecosystem:

- Standard Transaction Key is generated automatically and works in the background. It is required to initiate all transactions, and to recover a wallet in case of a hack or technical issue.
- Cancel Transaction Key allows users to perform Cancel transactions within approximately 24 hours, after 144 blocks are generated.
- Fast Transaction Key gives users the possibility to make Secure Fast transactions and transfer BTCV in a matter of minutes.

Bitcoin Vault Ecosystem

Bitcoin Vault's ecosystem includes three apps that were created in-house solely for the purpose of storing and managing BTCV. Together, they form a powerful tool that guarantees a higher standard in security, transparency and freedom.

Gold Wallet

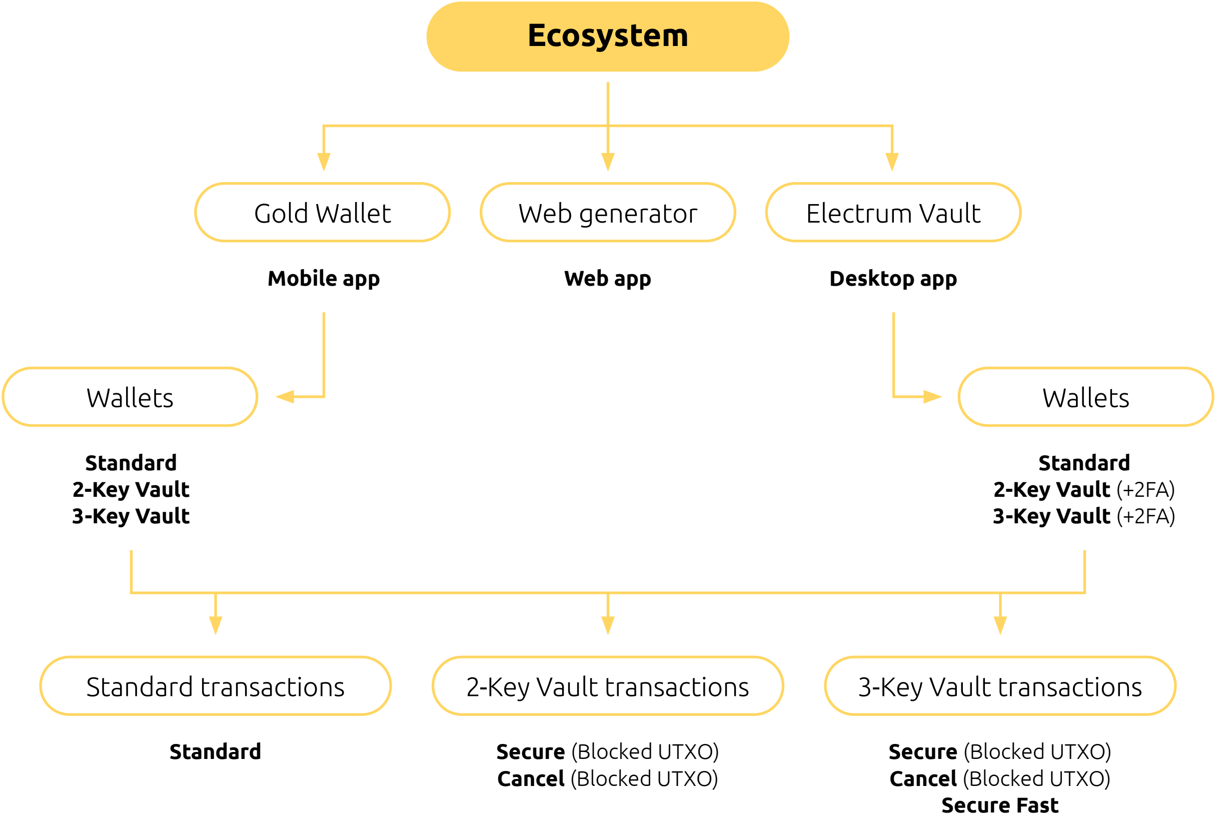
Gold Wallet is an app for mobile devices designed to store, send and receive BTCV. It allows users to create three types of wallets and perform various types of transactions, including Secure Fast, Secure and Cancel Transaction. Gold Wallet can also be used as an authenticator for the two-factor authentication (2FA) for the Electrum Vault desktop app.

Key Generator

Key Generator is a web-based app that generates individual public and private keys necessary to set up wallets and perform transactions. It uses only local resources, which means the key generation process, as well as the keys themselves, never leave the user's device. They are not stored anywhere and cannot be accessed online. The keys are stored offline, providing the utmost level of safety.

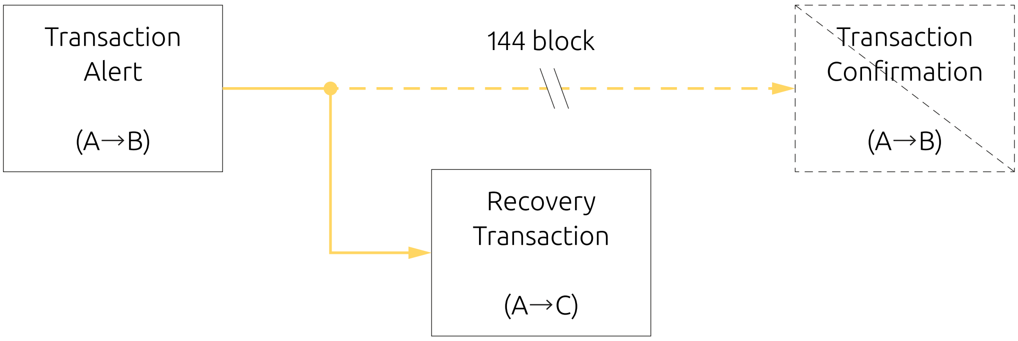
Electrum Vault

Electrum Vault is a desktop app based on an open-source Electrum Wallet. It has all the features of Gold Wallet, which means it can be used to store, send and receive BTCV, create wallets and perform transactions, including Secure Fast, Secure and Cancel Transaction.

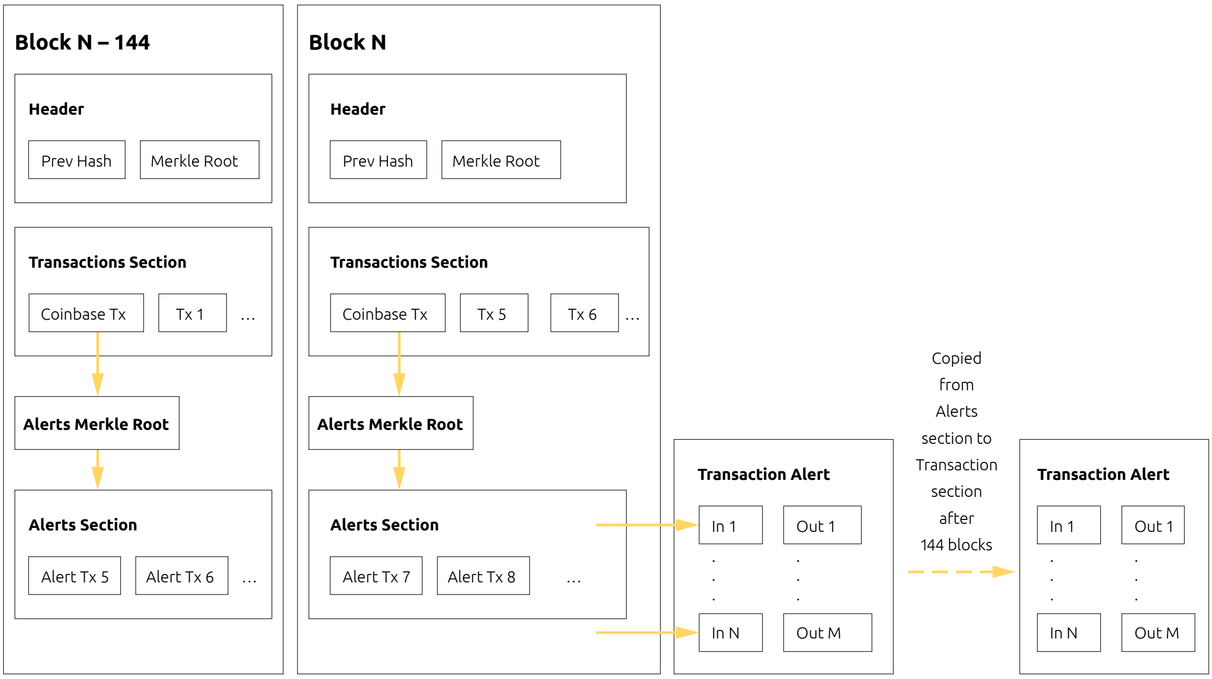


Technical overview

Locking script, default delay of 144 blocks, on-chain alert transactions:



BTCV Block structure with alert section (how it is stored, what happens when transaction change status from alert to confirmed, how miners verify when transaction change status)



Transactions Alerts changes the life-cycle of UTXOs.

In the standard version, UTXO has two states: unspent and spent (which basically means it's removed). A new version of Bitcoin Vault introduces a new state – confirmed. This changes the way UTXOs are stored in the database. From now on, the "confirmed" state is the time when UTXO is removed from the database and state spent locks the UTXO and stores the information about the block height it was spent in. This way, the system waits for the Transaction Alert to be confirmed before removing UTXO.

This is a necessary approach because, until confirmation is received, Transaction Alert might be recovered with Recovery Transaction (it uses only locked UTXO as inputs). The best way to alter the life-cycle of UTXO in the application would be to store information about the height they were spent at – spent height. This new information will determine in what state UTXO is:

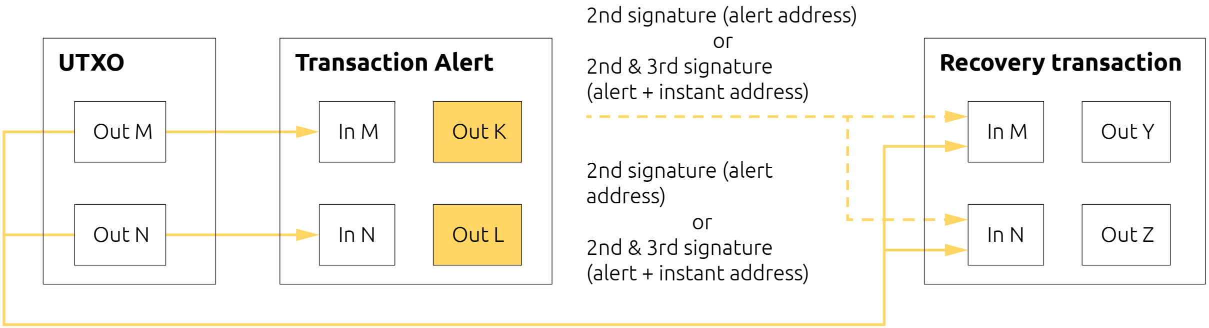
- 0 when unspent,
- >0 when spent.

Additionally, the same information should be considered in Undo structure. The Undo list stores the information of previous states of UTXOs at different heights and utilizes such information when the chain reorganization occurs.

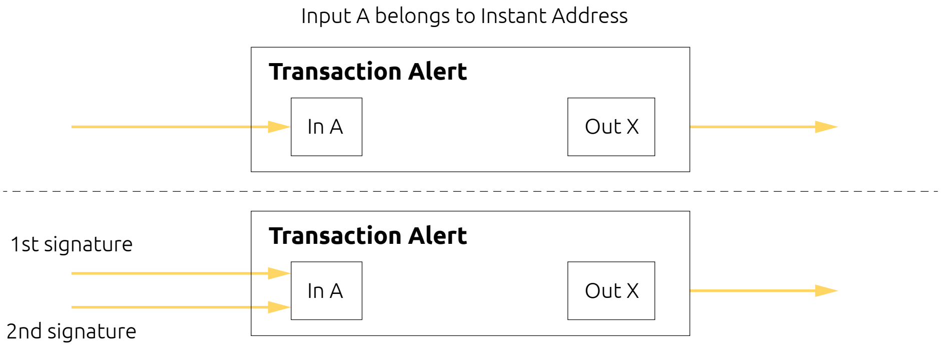
New UTXO states and transaction types have also an impact on balances visible to the users. UTXO that are in the spent state should be counted as a new balance that will be visible in the confirmed balance.

It cannot be counted as unconfirmed balance because that balance is related to unmined and spendable transactions. The idea is to create balances that are un-spendable but informative:

- alerts outgoing – counted out of UTXOs in the spent state, that are locked by Transactions Alerts,
- alerts incoming – counted out of UTXOs that are going to be available after Transactions Alerts confirmation.



How Fast Transaction works (explanation of by-pass of 24 h delay, what makes it possible – multi signatures):



Proof-of-Work

Bitcoin Vault is a Proof-of-Work coin based on the Bitcoin Royale open source code. With the hardfork performed on November 17, 2020, a merged mining with Bitcoin (BTCV) was implemented.

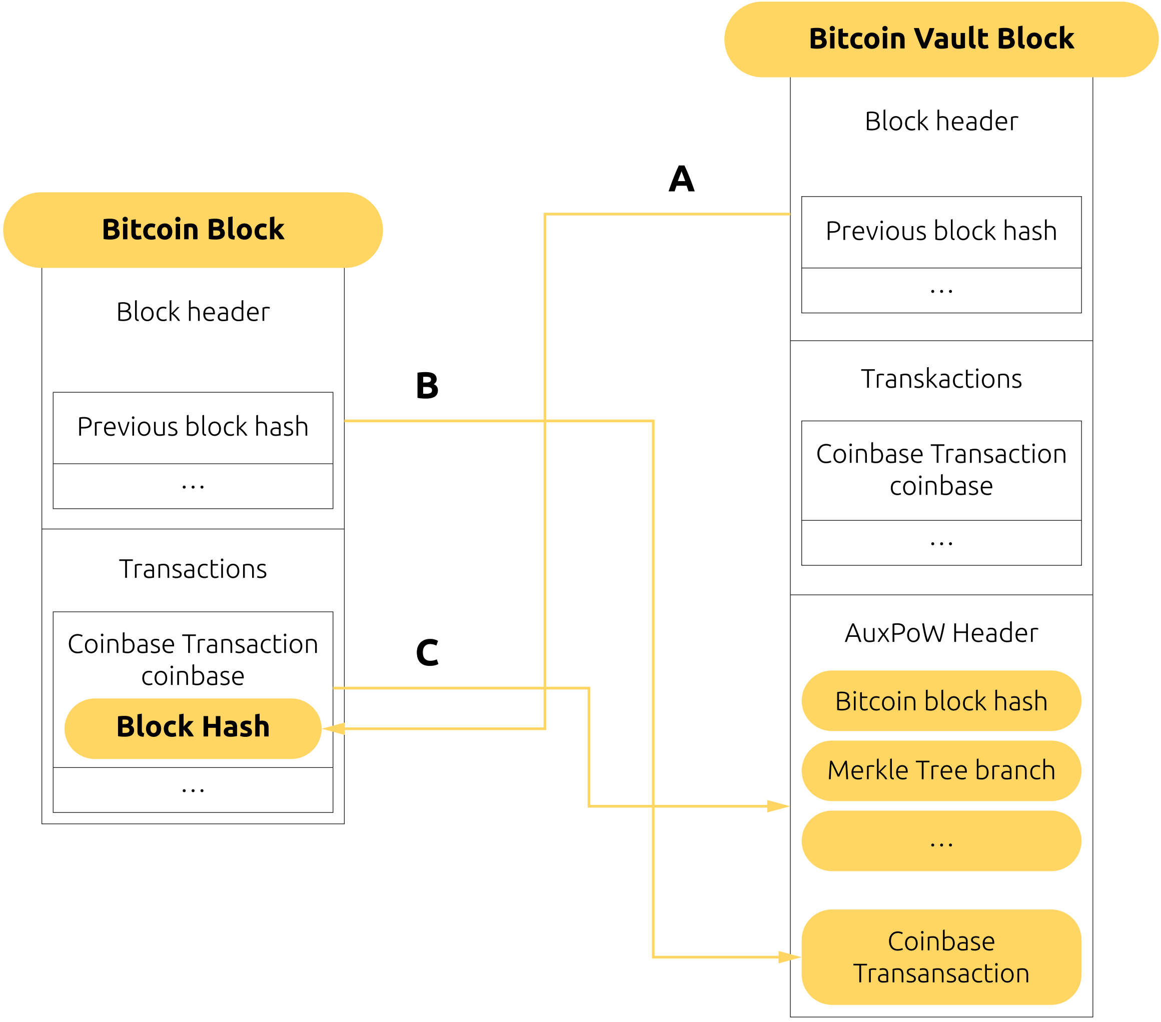
Merged Mining

Along with major update of BTCV protocol at block number 58,420, Bitcoin Vault was also adjusted to accept merged mining. Merged mining, also known as Auxiliary Proof-of-Work, is a process where miners are simultaneously searching for PoW for at least two separate cryptocurrencies with the same computational power. However, to build such a relationship between blockchains – parent and auxiliary – it is easiest when the auxiliary chain is prepared for the change.

In Bitcoin Vault, merged mining was implemented with Bitcoin, since both cryptocurrencies use the SHA-256 hash function. In this case, BTC is the parent chain and BTCV the auxiliary chain.

As a result, Bitcoin's (parent) proof-of-work solutions can be used to validate Bitcoin Vault (auxiliary chain) as an auxiliary proof-of-work (AuxPoW) consensus mechanism.

Technical explanation with graphic example of block structure and relationship between BTC and BTCV blocks:



With the implementation of merged mining to the protocol, BTCV miners are incentivized by a possibility to get two block rewards from both BTC and BTCV blockchains. An additional incentive is that thanks to the additional hashing power added to the network by piggybacking of the Bitcoin network with a higher hash rate, the network security is increased.

Block Rewards

Bitcoin Vault has a total supply of 21 million coins and an estimated time of mining a block of 10 minutes.

The Bitcoin Vault block reward was designed to eliminate certain issues arising at early stages of cryptocurrency development. Two main problems were identified:

The initial period to gain new participants is too short to reach the right number of community members necessary for the sustainable development of the project.

Block rewards after the initial period decrease drastically. This could lead to discourage miners from further participating in the mining process and result in significant drops in hash power.

In order to prevent such threats, Bitcoin Vault proposed the following solutions:

- To extend period with higher block rewards to 46 months.
- Divide this period into nine shorter sub-periods, every six months, with a more gradual block reward reduction.

This allows the team behind the project to have enough time for development. The community has a chance to grow to significant numbers, miners are incentivized to participate in the network from the early days for a longer period, and there is enough time for the number of coins to catch up with Bitcoin while not causing drastic block rewards reduction.

During that period, block rewards reduction is scheduled in the following way:

Date	BTCV Reward Reduction	Sub-Period Number	Block Reward	Sub-Period Time	Sub-Period Blocks
May 2020	175 to 150	1	175	6 months	29850
November 2020	150 to 125	2	150	6 months	26600
May 2021	125 to 100	3	125	6 months	26600
November 2021	100 to 75	4	100	6 months	26600
May 2022	75 to 50	5	75	6 months	26600
November 2022	50 to 25	6	50	6 months	26600
May 2023	25 to 12.5	7	25	6 months	26600
November 2023	12.5 to 6.25	8	12.5	6 months	26600
May 2024	6.25 to 3.125	9	6.25	6 months	26600

As a result, 19,687,500 coins are going to be distributed during this period, catching up and meeting the number of Bitcoins by its 4th halving (estimated in March 11, 2024). After that, the BTCV block reward will follow Bitcoin's halving schedule.

Development of Bitcoin Vault

Stages of BTCV development:

May 2019 – December 2019	Pre-Alpha
December 2019 – September 2020	Alpha
September 2020 – November 2020	Beta
November 2020	Mainnet

Mainnet

Mainnet was successfully launched on November 17, 2020 with block height number 58,420.

Roadmap

On December 2020 BTCV Development Team launched new roadmap covering years 2021-2022. Further BTCV development was divided into six workstreams:

Workstream no. 1 – Development upgrades

Development workstream relates to all blockchain upgrades that will be added to Bitcoin Vault. The main goal of this workstream is to participate in Dapp ecosystem around Ethereum 2.0 with Wrapped BTCV (wBTCV) until the end of 2021.

- Q1 2021
  - wBTCV ERC-20 token – analytics & tokenomics behind wBTCV
- Q2 2021
  - Ledger integration
- Q3 2021
  - wBTCV ERC-20 token beta tests phase
- Q4 2021
  - wBTCV launch
  - Start of integration with DeFI ecosystem
- Q1 2022
  - Full integration with DeFI ecosystem
  - Dapps development
- Q2 2022+
  - Dapps development

Workstream no. 2 – Security upgrades

Bitcoin Vault has an internal team of blockchain security experts. Mainnet blockchain integrity has been verified numerous times and in 2021 our main goal will be to strengthen the code and identify any bugs and holes left also with the support of external partners. After internal and external penetration tests, we will run an open bounty program for developers and work closely with the 'white hat' community.

- Q1 2021
  - Full code audit (internal & external)
- Q2 2021
  - Penetration tests (internal)
- Q3 2021
  - Penetration tests (external)
- Q4 2021
  - Security audit CIS/20
  - Cloud Security Matrix
- 2022+
  - Further security improvements & audits
  - Hackathons
  - Bounty program

Workstream no. 3 – User experience upgrades

User experience is one of the most important factors behind usage and adoption of the product. Our aim is to further develop and upgrade applications and tailor them to the needs of a variety of users based on the feedback from the community.

- Q1 &Q2 2021
  - GoldWallet mobile app UX improvements
  - Electric Vault mobile app easy mode and expert mode switch
- Q3 2021
  - GoldWallet user notifications
- Q4 2021
  - GoldWallet integration with 3rd party apps
- 2022+
  - Further UX improvements

Workstream no. 4 – Products

Along with IT development, we are strongly focusing on market adoption with new products in the pipeline. In 2021, we want to launch staking products with support of BTCV partners and connect BTCV ecosystem to FIAT currencies.

- Q1 2021
  - New staking products via 3rd parties
  - New trading products

- Q2 2021
  - New payment gateways
  - FIAT integrations
- Q3 2021
  - Data analysis platform (Big Data)
- Q4 2021
  - wBTCV token related products
- 2022+
  - New 3Keys functionalities
  - dApps products

Workstream no. 5 – Marketing activities

In 2021, we plan to launch a global awareness and engagement campaign aimed at current and future users of BTCV as well as the whole crypto community around the world. We will be seeking new partnerships that would strengthen security of BTCV blockchain as well as allow BTCV to be ahead of quantum research.

- Q1 2021
  - New website launch
- Q2 & Q3 2021
  - Global awareness & engagement campaign
- Q4 2021
  - Strategic security partnership
- 2022+
  - Strategic scientific partnership

Workstream no. 6 – Other upgrades

With some additional upgrades to the BTCV ecosystem, we want to connect and engage with our community and offer new options for hodlers through new a airdrop mechanism that will be fully launched in early Q2 2021. Our long-term focus will be also around quantum computing and its potential to influence cryptography of blockchain.

- Q1 2021
  - Development & launch of the new airdrops mechanism
  - Airdrops wallet lock
- Q2 2021
  - Airdrops platform / app
- Q3 2021
  - Blockchain analysis platform
- Q4 2021+
  - Quantum research
  - Scientific partnership grant program

Quantum Computing & DLT – Our Vision

As the most blockchain developers we are genuinely interested in the progress of quantum technologies. Researchers and developers working on distributed ledger technologies (DLTs) like blockchain depend on public-key cryptography and hash functions which are essential to all blockchain solutions.

Bitcoin Vault blockchain is secured by powerful cryptographic algorithms such as ECDSA and SHA-256, also used in Bitcoin as well as many other cryptocurrencies. The currently-used encryption algorithms are powerful enough for traditional computational methods.

Quantum computing threat

In theory, exponentially improving computing power with quantum technology can lead to the point when cracking a public key to calculate private key hash or breaking the SHA-256 algorithm to obtain the required one-time hash value block on the blockchain may be possible. According to many experts in the field, we are still years of research from developing stable quantum computers. Even then, those computers would need to be properly coded for the purpose of cracking certain cryptographic algorithms.

Quantum computing opportunity

Instead of focusing on the threats, we would like to focus on the opportunities.

Again, in theory, when quantum computers are able to reach enough stability to perform reliable calculations, it would be possible to use them to improve cryptographic algorithms. This is the opportunity we see for the future of blockchain.

For the present day, we can consider different approaches to achieve the goal of a quantum-proof coin, ie.:

- lattice-based cryptosystems,
- multivariate-based public-key cryptosystems,
- super-singular elliptic-curve isogenies cryptosystems,
- hash-based digital signature cryptosystems
- hybrid solutions like the ones tested by Google (CECPQ1 and CECPQ2)
- and some others.

To find a proper anti-quantum solution and prepare the BTCV coin for a post-quantum era, our development team needs to do more research in terms of necessary on-key compression techniques and on the use of certain types of codes and coding techniques.

Nevertheless, nowadays, there are no post-quantum blockchain algorithms that provide small key size, short signature/hash sizes, fast execution, low computational complexity, and low energy consumption, all at the same time. These factors are especially critical for resource-constrained embedded devices like the ones used in the Internet of Things.

Over the next 3 to 5 years, us BTCV developers will focus on reaching operational readiness in quantum resistance through new partnerships, especially with experts from various businesses, start-ups and technical universities.

Bitcoin Vault Founder

Bitcoin Vault was founded by Eyal Avramovich, CEO of Minebest, one of the world-leading operators of crypto mining facilities located in Asia and Europe.

More information about Minebest can be found here: https://minebest.com/

More information about the team behind Bitcoin Vault can be found on the official website: https://bitcoinvault.global/

Related works

We would like to give credit to the creators of Bitcoin Royale for the concept idea that led to the development of Bitcoin Vault.

Bitcoin Royale whitepaper: https://bitcoinroyale.org/bitcoinroyale.pdf

BTCV Sources:

Additional information about the project can be found:

https://bitcoinvault.global/
https://twitter.com/vaultbitcoin
https://medium.com/bitcoin-vault-btcv
https://t.me/Bitcoin_Vault
https://www.facebook.com/bitcoinvaultofficial
https://www.instagram.com/bitcoinvaultofficial
https://www.youtube.com/c/BitcoinVault

References

1. Bitcoin Whitepaper, Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf
2. Bitcoin Royale: Peer-to-Peer No-Theft Electronic Gold, Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
3. Cryptocurrency Anti-Money Laundering and Crime Report, Spring 2020, https://ciphertrace.com/cryptocurrency-anti-money-laundering-and-crime-report-spring-2020/
4. The Chainalysis 2020 Crypto Crime Report, https://go.chainalysis.com/2020-Crypto-Crime-Report.html
5. Bitcoin, crypto-coins, and global anti-money laundering governance, Malcolm Campbell-Verduyn, https://www.researchgate.net/publication/322596368_Bitcoin_crypto-coins_and_global_anti-money_laundering_governance
6. Namecoin project, https://www.namecoin.org/
7. Bitcoin Wiki, Merged Mining Specifications, https://en.bitcoin.it/wiki/Merged_mining_specification

8. Adam Back, Hashcash – A Denial of Service Counter-Measure, http://www.hashcash.org/papers/hashcash.pdf
9. Phil Daian, Rafael Pass, Elaine Shi; Snow White: Robustly Reconfigurable Consensus and Applications, https://eprint.iacr.org/2016/919.pdf
10. Wrapped Tokens A multi-institutional framework for tokenizing any asset https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf
11. Smart Contract Extensibility with Wrapped Tokens https://yos.io/2019/07/13/smart-contract-extensibility-wrapped-tokens/#:~:text=Wrapped%20Tokens%20is%20a%20design,two%20versions%20at%20any%20time.
12. Aleksei Pupyshev, Ilya Sapranidi, Elshan Dzhafarov, Shamil Khalilov, Ilya Teterin, Graviton: interchain swaps and wrapped tokens liquidity incentivisation solution, https://arxiv.org/ftp/arxiv/papers/2009/2009.05540.pdf