Bitcoin Vault: Peer-to-Peer Anti-Theft Electronic Gold

Eyal Avramovich
github.com/bitcoinvault

Abstract. Satoshi Nakamoto's original vision for Bitcoin was to create a peer-to-peer version of electronic cash. The majority of successful forks of the protocol try to improve on this vision further and provide a more scalable and efficient system for payments. We see Bitcoin's greatest promise not as a medium of exchange but as a store of value – a better form of gold, not cash. We propose a set of modifications to the original protocol aimed at fulfilling this promise by creating the ultimate electronic store of value. By increasing Bitcoin's effective transaction confirmation time of 10 minutes to 24 hours, we are able to tackle Bitcoin's greatest flaw as a form of gold – susceptibility to theft. A system geared less towards paying for coffee and more towards holding one's life savings with complete peace of mind, where every transaction is alerted on-chain for 144 blocks and can be canceled on emergency with a recovery key that was never used prior and hence invulnerable. The bootstrap of this system is not via hard fork but through a fairer mechanism of expedited mining, allowing the system to catch up to Bitcoin in a short period of time. We would like to give all credit to the creator of the Bitcoin Royale whitepaper [1] which created the vision of no-theft electronic gold. As a team, we would like to move forward with that idea and start implementing all the crucial features mentioned below and make it even more advanced with the 3rd private key solution that is revealed as an additional feature in paragraph 6.2.

1. Introduction

Bitcoin [2] is an innovative decentralized payment system launched in 2009 allowing parties to transact directly without going through a trusted financial institution. The system relies on proof-of-work to maintain a distributed ledger without a trusted operator, that is secure as long as honest nodes control more CPU power than any cooperating group of attacker nodes. Bitcoin was originally described by its creator Satoshi Nakamoto as an "electronic cash system".

Multiple successful modifications of the original protocol have been released over the years in the form of forks of the Bitcoin codebase. These include Litecoin [3] that launched in 2011 to reduce transaction confirmation time and change the proof-of-work algorithm to favor consumer-grade hardware such as GPU; Bitcoin Cash [4] that launched in 2017 to scale the original protocol's transaction throughput by increasing block size; and Bitcoin Gold [5] that also launched in 2017 to render specialized mining equipment obsolete by changing the hashing algorithm.

True to the original vision, the primary focus in these forks and others is to make Bitcoin a better system of cash. Limitations of the original protocol such as high transaction fees, 10 minute confirmation times and approximate throughput of only 4 transactions per second hinder Bitcoin's ability to compete with the centralized online payment systems dominant today.

2. Electronic Cash or Electronic Gold

Whereas Bitcoin did not see much success with consumer adoption as electronic cash, it has been significantly more successful as a form of electronic gold. There is a long standing industry debate whether Bitcoin is superior as a medium of exchange or in fact as a store of value. Gold is not an effective means of payment for day-to-day goods and services. Consumers primarily invest in gold to hedge against inflation and preserve future purchasing power. Unlike national currencies, Bitcoin's fixed monetary policy and limited supply make it particularly attractive in this regard.

History shows that systems can rarely be designed to meet several competing goals at once. Optimizing Bitcoin to become a better medium of exchange diminishes its potential as a store of value. On the same note, by sacrificing further on the properties required for useful electronic cash, we can vastly improve its utility as electronic gold. In this paper, we propose a series of modifications to the original Bitcoin protocol focused on a single goal – creating the ultimate store of value.

If we no longer prioritize competing as an online payment system, we need not focus on transaction fees or transaction throughput. After all, gold is expensive to transport and is normally acquired for long term investment. A property that is particularly relevant to our efforts is transaction confirmation time. Tradeoffs on this front, such as substantially increasing Bitcoin's average 10 minute confirmation time, can yield cardinal advantages. Since we would not expect to freight a shipment of gold across locations in under 10 minutes anyways, this sacrifice seems natural.

3. The Problem of Theft

The key requirement from a store of value is to be nonperishable. Theft is one of the primary risks of loss when dealing with anything of value. Gold performs rather well in this regard. Physical theft of gold is significantly riskier to execute than any virtual attack on an electronic asset. In addition, a thief would have a hard time hiding a sizable cargo of stolen gold from the authorities, especially across borders. Laundering and liquidating stolen gold in large quantities while remaining anonymous is no simple task either.

Unfortunately, Bitcoin fares poorly by comparison. Funds are protected by the protocol with sets of cryptographic private keys. Gaining electronic access to these keys allows an attacker to seize all funds remotely, immediately and irrevocably. Laundering stolen funds is also significantly easier since transactions are pseudonymous, traceability can be disrupted by use of mixers [6] and Sybil identities can be created in bulk. As a result, cryptocurrency theft is on the rise with over $1 billion stolen in 2018 [7]. Community-curated lists of major incidents [8] show that even professional institutions well-versed in the latest security practices are prone to attack.

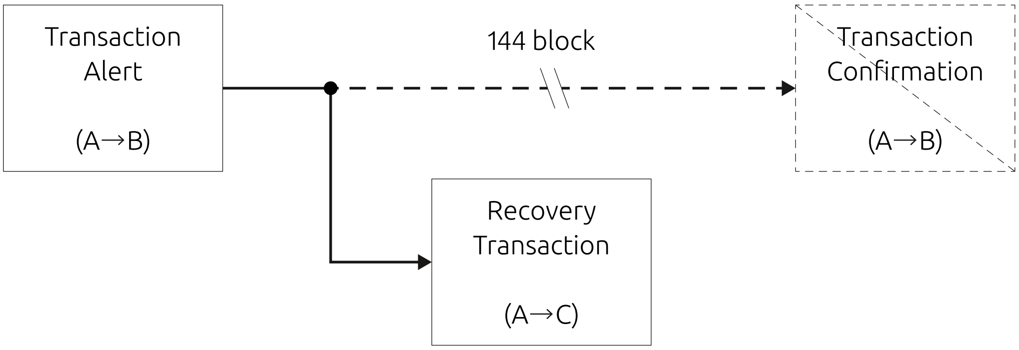
Secure management of private keys by end-users is proving to be one of the major challenges of Bitcoin. Since keys must be regularly used to interact with funds and the signed transactions must be transmitted over the Internet, every key eventually becomes vulnerable. Security-conscious practices like splitting funds between "hot" and "cold" wallets are cumbersome and fail to solve the problem at the root. Incidents show that hot wallets unavoidably hold significant amounts [9, 10] and use of cold wallets only reduces interaction with keys but does not eliminate it completely [11].

4. Anti-Theft Solution

As a means to eliminate theft, we propose a solution based on a new, sophisticated locking script and protocol modification. A transaction performed using the new locking script will by default be delayed by 24 hours. When a miner adds a transaction to a new block, the transaction will no longer be committed immediately. Instead, it will be added on-chain as an alert for the duration of 144 blocks (assuming block time of 10 minutes). If left undisturbed for 144 blocks, the transaction will change from alert state to "confirmed".

The benefit of on-chain alerts is that coin owners will receive uncensorable advance notifications whenever their coins are moved. The owner will have 24 hours to act upon the alert and will be able to override the transfer if unauthorized. Delayed withdrawals are a proven anti-theft industry standard in custodial wallets and the traditional banking system. Coinbase Vault [12], for example, has a wait time of 48 hours. Our proposed solution provides the same protection without a trusted third party.

Emergency override of a transaction in alert state requires a special recovery transaction and is carried out immediately without being subject to the 24 hour delay. The recovery transaction requires a special recovery key that must be incorporated into the locking script during the wallet creation. Once a recovery key has been registered for a given wallet, it cannot be changed.



The private recovery key used for the emergency override is intended to be a fresh key that has never been used before. This key can be generated offline and should never be connected to the Internet or inputed to any device. The registration process only requires the public part of this key, ensuring that the private key can remain unused. Unlike cold wallet keys that must be used occasionally and are thus vulnerable to theft, the recovery key will be used for the first time only in the emergency override itself, and therefore can be completely theft resistant. Once the recovery key has been used, it is to be considered compromised and all funds should be immediately transferred to a new wallet protected by a new unused recovery key.

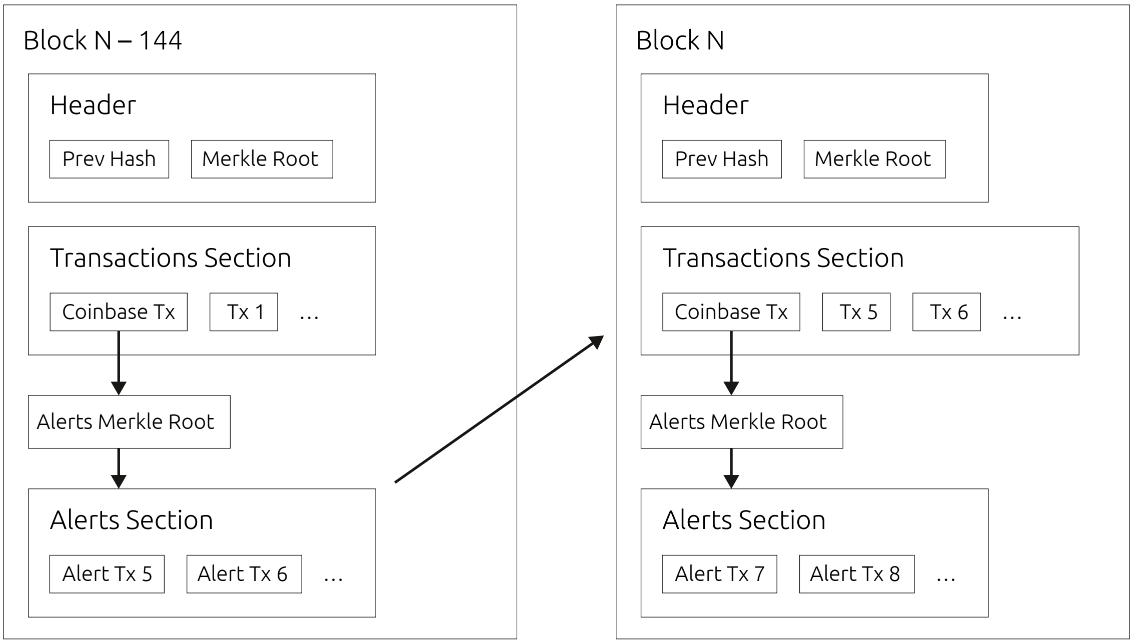
The original Bitcoin Royale concept of digital gold assumed delaying all the transactions in the system by 24 hours, making the coin a secure, slow-moving store of value. We would like to expand this concept to take the best of two worlds – the digital gold and digital cash, without any compromise on security.

Alongside the slow-moving alerts we conditionally keep the fast-moving, "instant" transactions. To provide the highest security, sending such a transaction will require a user to perform a blockchain-based 2FA, using the 3rd key provided during wallet creation.

5. Blocks

Like the original Bitcoin protocol, every block contains a list of confirmed transactions and holds the Merkle root hash of these transactions in its header. Since some transactions must wait 24 hours on-chain, they cannot be added immediately to a block's transactions section. Instead, they are added to a new special section that does not exist in the original Bitcoin protocol – the alerts section. The Merkle root hash for the alerts section is stored in the input of the coinbase transaction maintaining block header compatibility with the original Bitcoin.

When a new block is mined, the miner looks back 144 blocks and examines the alert section of block N-144. All alerts for transactions that are still valid become confirmed and populate the transactions section of the new block.



The steps for mining block N are as follows:

1) Add new regular transactions to block N alerts section (not confirmed).
2) Add new instant transactions to block N transactions section (confirmed)
3) Add new recovery transactions to the block N transactions section (confirmed).
4) Go over block N-144 alerts section and add the valid transactions to block N transactions section (confirmed).

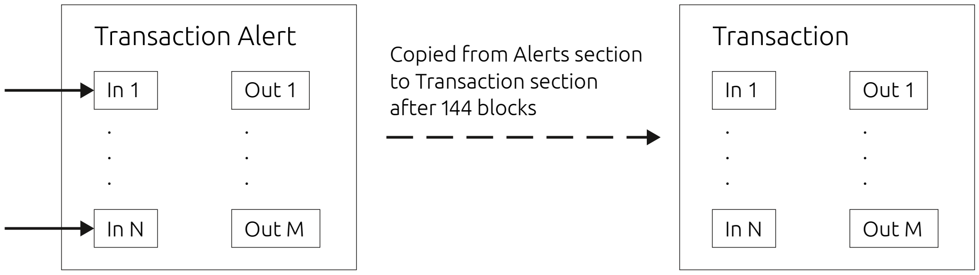
6. Scripts

The core functionality of Bitcoin Vault is available via the sophisticated locking script, which behaves differently based on the number of signatures presented in the unlocking script. Two variants are available:

1. Alert locking script – requiring either one or two signatures. If one signature is presented, an alert transaction is generated. If two signatures are presented, a recovery transaction is generated.
2. Alert + instant locking script – requiring either one, two or three signatures. If one signature is presented, an alert transaction is generated. If two signatures are presented, an instant transaction is generated. If all three signatures are presented, a recovery transaction is generated.

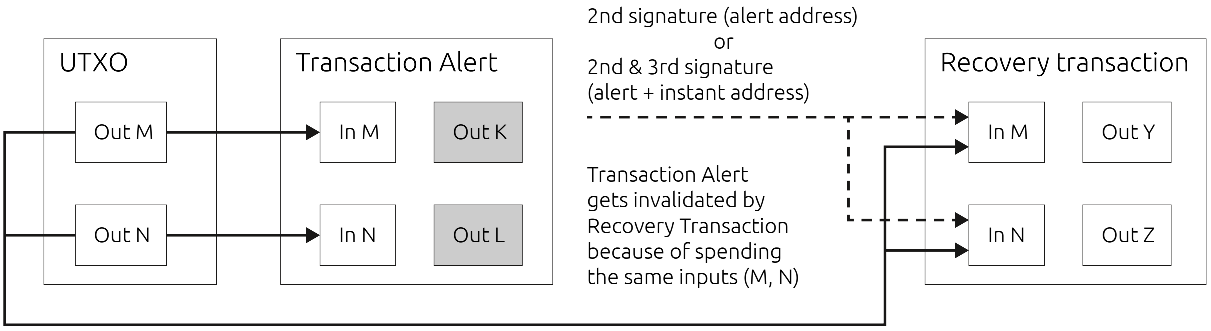
7. Transactions

Coin transfers are performed using regular transactions identical to those in the Bitcoin protocol. Their format does not change as they're moved from the alert section to the transactions section.


Transaction Alert
In 1
Out 1
In N
Out M
Copied from Alerts section to Transaction section after 144 blocks
Transaction
In 1
Out 1
In N
Out M

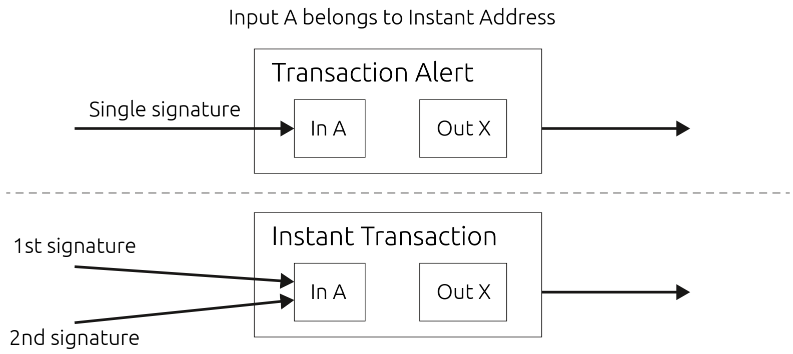
7.1. Recovery Transactions

A recovery transaction spends the same UTXO as the recovered alert. The difference is that it presents more signatures to the same UTXO: 2 in case of alert locking script, or 3 in case of alert + instant locking script. When a recovery transaction is processed, the recovered UTXO is spent, thus invalidating any existing alerts relying on this UTXO and preventing them from becoming confirmed past their 24 hour delay.


UTXO
Out M
Out N
Transaction Alert
In M
Out K
In N
Out L
2nd signature (alert address)
or
2nd & 3rd signature
(alert + instant address)
Transaction Alert gets invalidated by Recovery Transaction because of spending the same inputs (M, N)
Recovery transaction
In M
Out Y
In N
Out Z

7.2. Instant Transactions

An instant transaction allows bypassing the default 24-hour delay for the transaction confirmation and speed up the transaction confirmation to about 10 minutes. Its mechanism is similar to the multisig wallet. It requires an additional signature from a separate private key that should be safely stored in a separate location. That's why instant transactions can only be sent from special P2SH addresses – instant addresses, generated from the alert + instant locking script.



8. Compatibility

Our design attempts to make the protocol as compatible as possible with the standard Bitcoin protocol. The underlying goal is to minimize necessary code changes to existing Bitcoin full nodes, wallets, pools and miners. However, if the changes are performed on an already existing blockchain, they require a hard fork

In order to avoid changing the format of the block header, thus making the coin incompatible with bitcoin ASIC miners, the Merkle root hash for the alerts section is stored in the input of the standard coinbase transaction.

If the hard fork is required, it is our goal to make the transition as easy as possible for the existing coin users. All the existing script types don't change their behavior, so all the coins existing before the hard fork are spendable in an usual way. We will however strongly advise to switch to the new, more secure scripts.

9. Incentive

The system borrows the incentive model from Bitcoin that has proven itself successful over the last decade. The incorporation of alerts requires minor modifications to this model. Miners are incentivized to include the transaction alerts to a block by the promise of fee calculated from the difference between value of outputs and inputs. The fees are calculated from the future block transactions,and distributed to the original miner – the one including transaction alerts.

The future miner will still receive block reward for mining a new block, all fees from the new instant, registration and recovery transactions and the promise of future fee from transaction alerts. The future miner is obligated by consensus rules to include all alerts from N-144 block to the transaction sections excluding those that were recovered.

In case of cancellation of the alert, the fees for the original miner of the alert are unrecoverable and the total cost is the fee of the original alert plus fee for the recovery transaction.

10. Related Work

We are particularly impressed with the work of Malte Möser et al. on Bitcoin Covenants [13]. Their extension of the Bitcoin script language enables restrictions on the future use of coins, which can be used to implement a variety of security measures. The primary of which is vault transactions, which resemble our proposed delayed withdrawals mechanism.

We have opted for a simpler implementation that does not require a recursive array of custom scripts to be implemented by wallets. Our proposal is more than an optional extension, it is a fundamental change to the protocol with a wide mandatory effect on transactions. Shifting the burden of implementation to miners and leaving the end-user transaction experience identical to the default, enable us to better carry out our mission of creating true electronic gold.

References

1. Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
2. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://www.bitcoin.org/bitcoin.pdf, 2008.
3. Litecoin Project, “Litecoin, open source P2P digital currency”, https://litecoin.org, 2014.
4. “Bitcoin Cash”, https://www.bitcoincash.org, 2018.
5. bitcoingold.org, “Bitcoin Gold”, https://bitcoingold.org, 2018.
6. J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, “Coinparty: Secure multi-party mixing of bitcoins”, In: *CODASPY ’15*, 2015.
7. CipherTrace, “Cryptocurrency Anti-Money Laundering Report, 2018 Q4”, https://ciphertrace.com/crypto-aml-report-2018q4, 2019.
8. “BLOCKCHAIN GRAVEYARD”, https://magoo.github.io/Blockchain-Graveyard, 2019.
9. C. Zhao, “Binance Security Breach Update (May 7 2019)”, https://binance.zendesk.com/hc/en-us/articles/360028031711, 2019.
10. J. Buck, “Coincheck: Stolen $534M ln NEM Were Stored On Low Security Hot Wallet“, https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet, 2018.
11. J. Preissler, “Important Notice: Only trade TIO on trade.io”, https://medium.com/@trade.io/important-notice-only-trade-tio-on-trade-io-823d59fd7104, 2018.
12. KM. Cutler, “Coinbase Launches A More Secure Bitcoin Storage Option Called ‘Vault’”, https://techcrunch.com/2014/07/02/coinbase-vault, 2014.
13. M. Möser, I. Eyal, E. Gün Sirer, “Bitcoin Covenants”, In: *Financial Cryptography and Data Security, FC 2016, Lecture Notes in Computer Science*, Vol. 9604. Springer, Berlin, Heidelberg.