About

Bitcoin Confidential is a new coin focused on confidentiality. Bitcoin Confidential will be Proof of Stake on the latest Bitcoin codebase using Ring Signatures for all transactions. SmartCash (SMART) holders will get an airdrop of 10 Bitcoin Confidential for every 1 SmartCash held. Bitcoin Confidential is also exploring airdropping coins from other top coins. All Bitcoin Confidential coins will be fungible; from the genesis block, all transactions will be confidential to create a genuinely fungible cryptocurrency using Ring Signatures technology.

Release date and blockchain snapshot is anticipated to be Q3/Q4 2018.

Website: https://www.bitcoinconfidential.com/
Discord: https://discord.bitcoinconfidential.com/
Telegram: https://t.me/bitcoinconfidential
Reddit: https://www.reddit.com/r/BitcoinConfidential/
Gab: https://gab.ai/BitcoinConfidential
Twitter: https://twitter.com/btconfidential
Pre-Ann: https://forum.bitcoin.com/alternative-cryptocurrencies-altcoins/bitcoin-confidential-t83383.html

Features

- Untraceable payments using the RingCT privacy protocol required for all non-staking transactions to create a fully fungible blockchain for all users.
- Improved version of Proof-of-Stake Protocol v3.0 with added features.
- Ring Signatures requires no trusted setup, group, or private key ceremony.
- Coin generation is trustless, verifiably secure, and with an auditable supply.
- Stealth addresses which prevents 3rd parties from observing transactions.
- Cold staking will allow offline wallets to earn rewards for securing the network.
- Latest Bitcoin codebase for maximum compatibility and new features.
- Self-funding budget for ongoing development, marketing and support.

Specifications

Name: Bitcoin Confidential
Ticker: TBD
Algorithm: Improved Proof of Stake V3.0
Consensus Type: PoS
Maximum Supply: Limited total supply.
Block Time: TBD
Block Reward: TBD
Block Size: TBD
Transactions per Second: TBD
Coin Maturity for Staking: 225 Confirmations
Stealth Addresses
Anon Transactions using RingCT
Ring Signatures
Cold Staking
Latest Bitcoin Code
Segwit Ready
Lightning Network Ready

FAQ

What is Bitcoin Confidential?

Bitcoin Confidential is a new coin focused on confidentiality that will be Proof of Stake using Ring Signatures on the latest Bitcoin codebase.

Why the name Bitcoin Confidential?

Confidentiality is a more accurate term than privacy, and the technology is based on Bitcoin code so it is appropriate to continue the brand connection.

Why does Bitcoin Confidential exist?

To better implement privacy from day one and fulfill the mission that the team believes in, which is a completely private and fungible blockchain currency that is accessible to everyone.

Why not just add privacy features to SmartCash rather than create a Sister Coin?

Legislation is becoming unfavorable for confidentiality coins, so SmartCash will focus on merchant adoption first as the primary use case. SmartCash privacy features will be limited to 3rd party implementation, such as wallets with BIP-47.

How is Bitcoin Confidential actually confidential?

Through implementing the Ring Signatures (RingCT) protocol which will be required for every transaction from the genesis block to ensure all non-staking coin transactions maintain confidentiality of sender, receiver, and amounts sent.

Will there be an airdrop?

Yes. For every 1 SmartCash in an address to which you hold the private key at the time of the airdrop blockchain snapshot, you will be able to claim 10 Bitcoin Confidential. Blockheight and date TBD for this snapshot.

What about an airdrop to Bitcoin holders?

Airdrop ratios for other coin blockchains are TBD, as well as which coins will be supported.

When can we expect Bitcoin Confidential to release?

Release date is anticipated to be Q3/Q4 2018. Announcements will be made regarding blockchain snapshots for airdrop eligibility ahead of release.

Will there be masternodes?

No, Bitcoin Confidential will not include a masternode mechanism with regards to voting or uptime requirements for rewards. However, holders may stake their coins to receive rewards for securing the blockchain, and a node may be helpful to stay connected to the blockchain 24/7.

References

Ring Confidential Transactions. Shen Noether, October 2015. "https://eprint.iacr.org/2015/1098.pdf"

1.3. **Strongly Decentralized Anonymous Payment Schemes.** The Ring CT protocol allows hidden amounts, origins, and destinations for transactions which is somewhat similar to Zerocash [BSCG+14]. One possible differentiator is that the use of proof of work for coin generation is possible with Ring CT as opposed to in ZeroCash, where it seems all coins must be pregenerated by a trusted group.

Noether, page 6

CryptoNote v 2.0. Nicolas van Saberhagen, October 2013. "https://cryptonote.org/whitepaper.pdf"

Security Analysis of Proof-of-Stake Protocol v3. Blackcoin. 2016. "https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf" **Bitcoin: A Peer-to-Peer Electronic Cash System.** Satoshi Nakamoto, 2008. "https://bitcoin.org/bitcoin.pdf"

An Empirical Analysis of Anonymity in Zcash. George Kappos, Haaroon Yousaf, Mary Maller, Sarah Meiklejohn, 27th USENIX Security Symposium, 2018. https://arxiv.org/abs/1805.03180

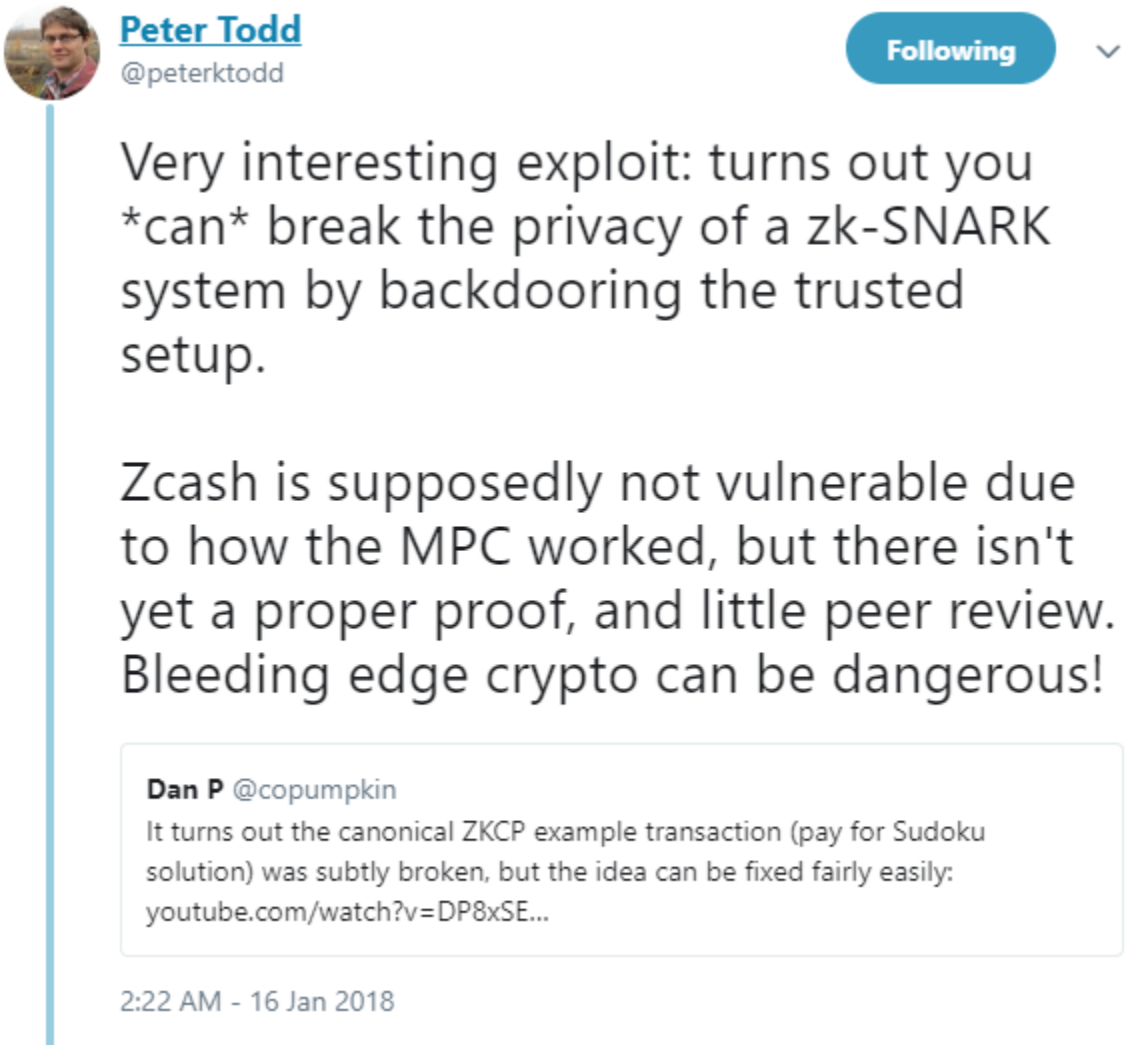
An Empirical Analysis of Traceability in the Monero Blockchain. Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, Nicolas Christin, April 2018. https://arxiv.org/abs/1805.03180

3 Deducible Monero Transactions

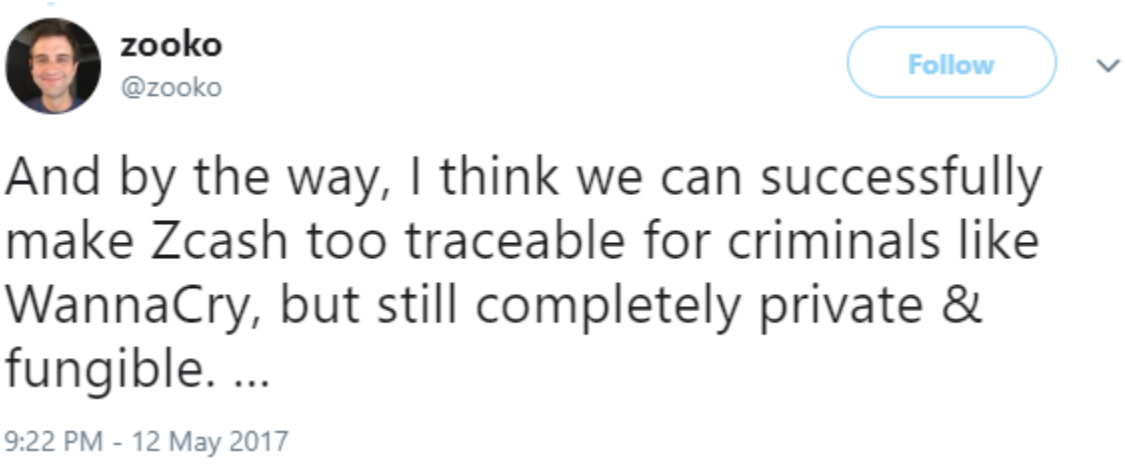
A significant number of Monero transactions do not contain any mixins at all, but instead explicitly identify the real TXO being spent. Critically, at the beginning of Monero's history, users were allowed to create zero-mixin transactions that do not contain any mixins at all. Figure 5 shows the fraction of transactions containing zero-mixin inputs over time. As of April 15, 2017 (at block height 1288774), a total of 12158814 transaction inputs do not contain any mixins, accounting for 64.04% of all inputs overall.

Lee et al, page 6

Commentary



https://twitter.com/peterktodd/status/953165586334232577



https://twitter.com/zooko/status/863202798883577856

Articles

https://spectrum.ieee.org/tech-talk/computing/networks/the-crazy-security-behind-the-birth-of-zcash

https://www.wired.com/story/monero-privacy/

Videos

"Ring Confidential Transactions" https://www.youtube.com/watch?v=zHN_B_H_fCs