Zcoin

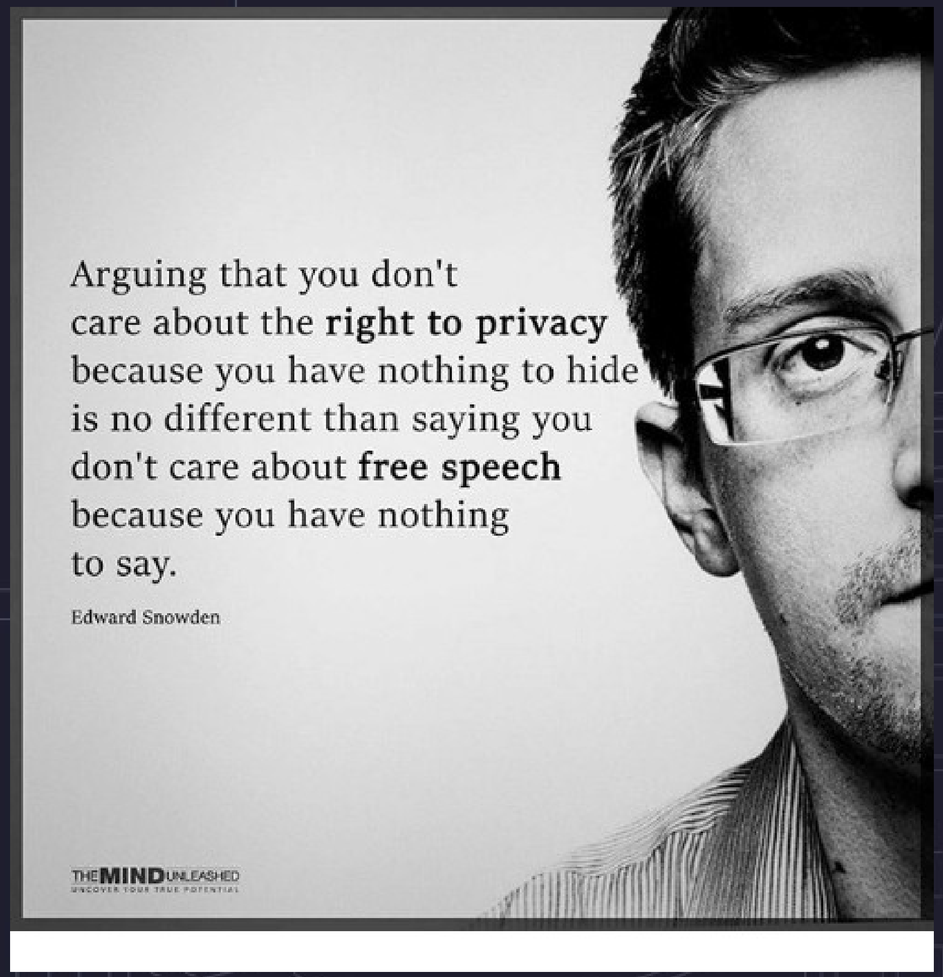
Trustless and simple ZKP

bitfish

Sigma & Lelantus

- Simple and Trustless ZKP

Why do you need blockchain privacy?



- Do you want anyone to know?
  - What you bought before
  - Your potential networth
  - How much you earn and who you get it from
- Do businesses want people to know
  - Who their suppliers are and how much they are paying them?
  - Who their customers are and how much they are buying?
  - The value and terms of their contracts?
- For cryptocurrencies or blockchains to be used, privacy is a must!

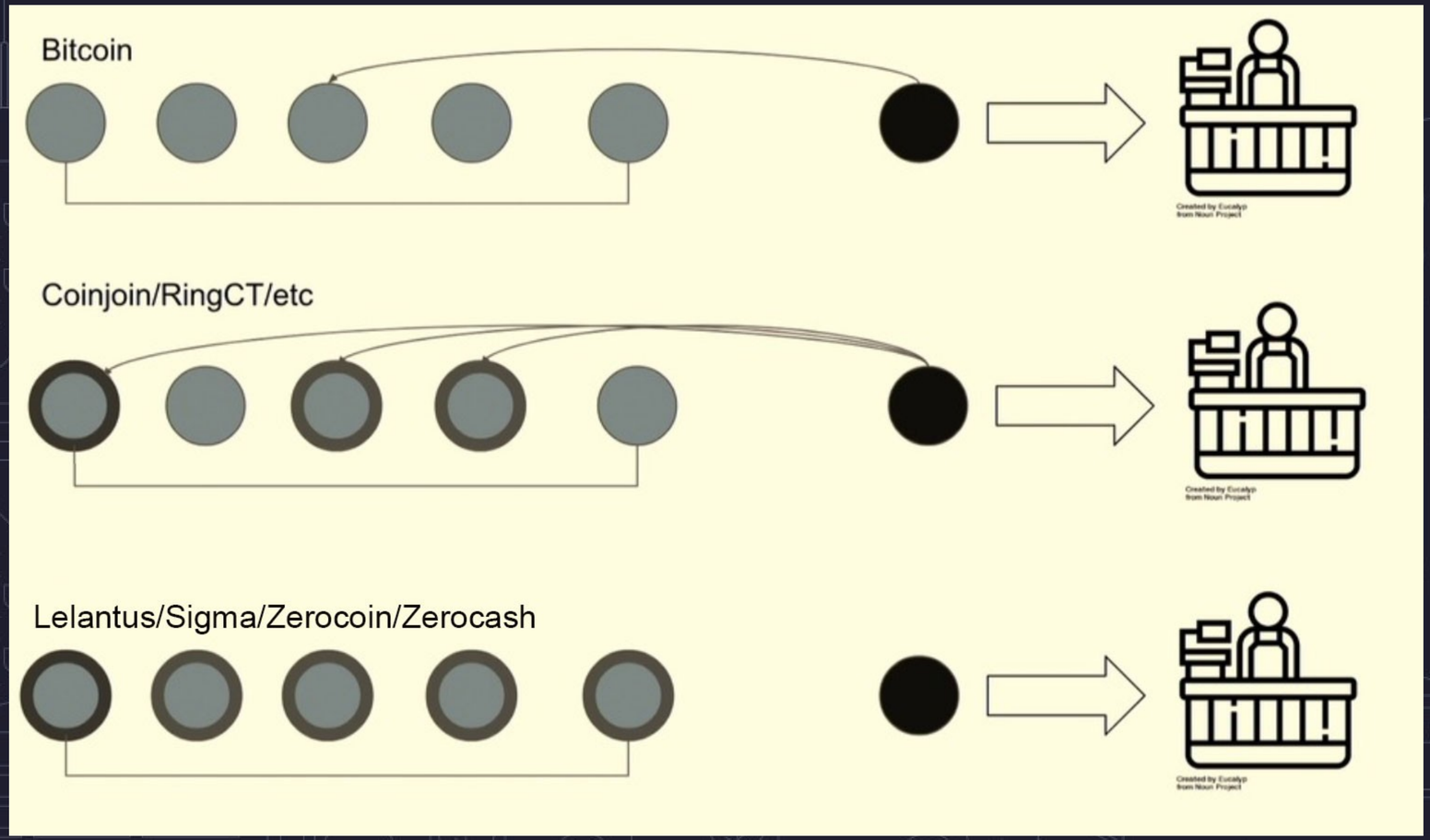
What do you need for a blockchain privacy system?

- High anonymity that stands the test of time
- Good performance that can scale
  - Small proof sizes (doesn’t occupy much space on the blockchain)
  - Quick verification times (nodes can check the validity quickly)
  - Low proof times + resources (the time it takes to create a private transaction)
- Easy to use
- Minimal trust required

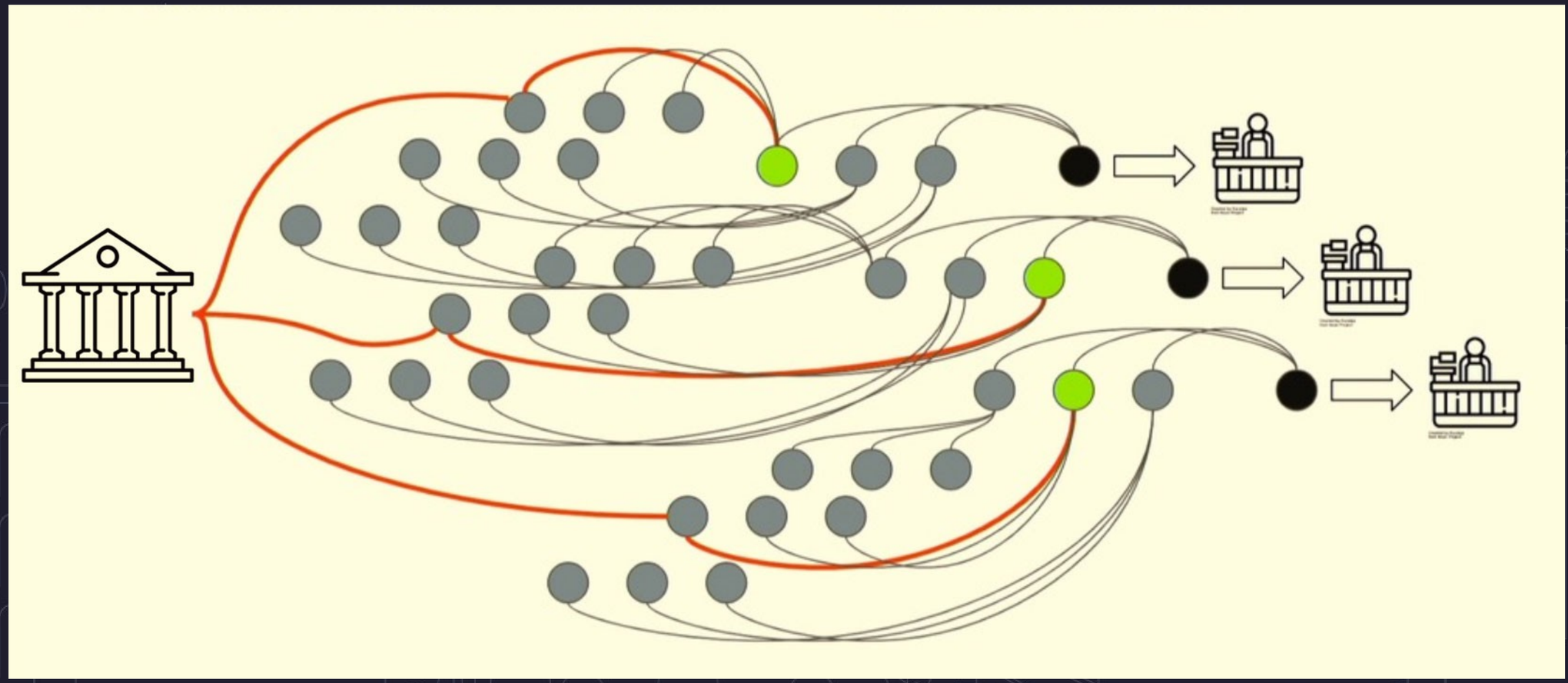
Why do we need yet another privacy protocol?

- No holy grail of privacy protocols: always trade offs
- Privacy protocols that are ‘good enough’ today may not be good enough a few years down the line.
- Are mixing or decoy transaction models enough?
  - ❖ RingCT
  - ❖ Coin mixers or tumblers (Cash Shuffle)
  - ❖ Mimblewimble

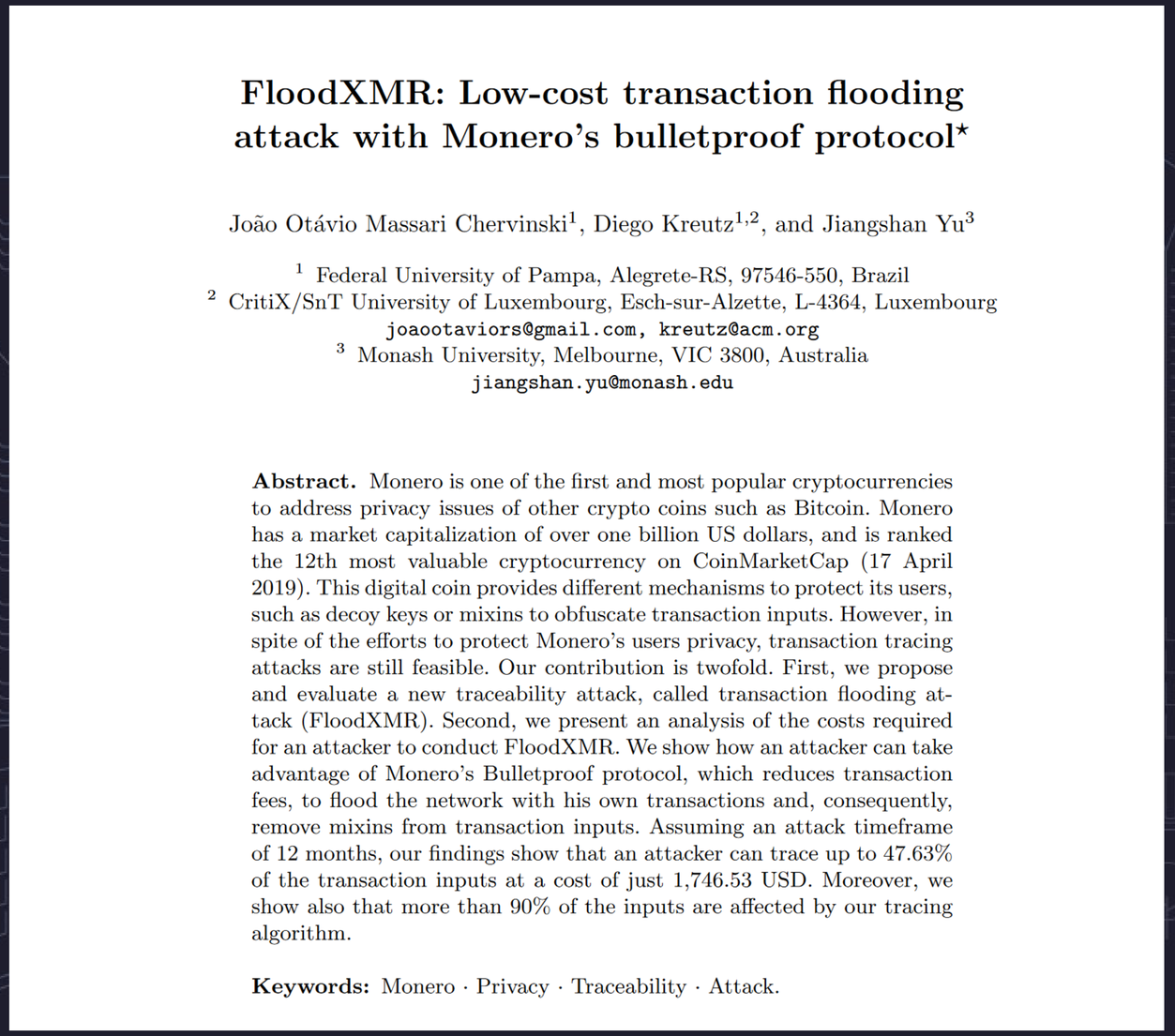
Decoy Systems vs ZKP



Decoy Systems vs ZKP



Decoy Systems vs ZKP



FloodXMR: Low-cost transaction flooding attack with Monero's bulletproof protocol*

João Otávio Massari Chervinski[1], Diego Kreutz[1,2], and Jiangshan Yu[3]

[1] Federal University of Pampa, Alegrete-RS, 97546-550, Brazil
[2] CritiX/SnT University of Luxembourg, Esch-sur-Alzette, L-4364, Luxembourg
joaootaviors@gmail.com, kreutz@acm.org
[3] Monash University, Melbourne, VIC 3800, Australia
jiangshan.yu@monash.edu

Abstract. Monero is one of the first and most popular cryptocurrencies to address privacy issues of other crypto coins such as Bitcoin. Monero has a market capitalization of over one billion US dollars, and is ranked the 12th most valuable cryptocurrency on CoinMarketCap (17 April 2019). This digital coin provides different mechanisms to protect its users, such as decoy keys or mixins to obfuscate transaction inputs. However, in spite of the efforts to protect Monero's users privacy, transaction tracing attacks are still feasible. Our contribution is twofold. First, we propose and evaluate a new traceability attack, called transaction flooding attack (FloodXMR). Second, we present an analysis of the costs required for an attacker to conduct FloodXMR. We show how an attacker can take advantage of Monero's Bulletproof protocol, which reduces transaction fees, to flood the network with his own transactions and, consequently, remove mixins from transaction inputs. Assuming an attack timeframe of 12 months, our findings show that an attacker can trace up to 47.63% of the transaction inputs at a cost of just 1,746.53 USD. Moreover, we show also that more than 90% of the inputs are affected by our tracing algorithm.

Keywords: Monero · Privacy · Traceability · Attack.

- FloodXMR shows some weaknesses of decoy systems
- Flooding with transaction spam to make others mix with you.
- Cost is about 17,000 USD (figure disputed) a year or so to deanonymize ~50% of transactions. Cheap transactions actually hurt them by making it cheap to do an attack
- How much is too expensive?

What about zkSNARKs?

- Trusted setup is a problem with zkSNARKs
  - Against the idea of “Don’t trust, verify”
  - Mitigated by Sapling MPC
- Extremely complicated cryptography and construction
  - Only a handful of cryptographers in the world understand it well
  - Often called moon math
- Experimental cryptographic assumptions

Summary

Eleven months ago we discovered a counterfeiting vulnerability in the cryptography underlying some kinds of zero-knowledge proofs. This post provides details on the vulnerability, how we fixed it and the steps taken to protect Zcash users.

The counterfeiting vulnerability was fixed by the Sapling network upgrade that activated on October 28th, 2018. The vulnerability was specific to counterfeiting and did not affect user privacy in any way. Prior to its remediation, an attacker could have created fake Zcash without being detected. **The counterfeiting vulnerability has been fully remediated in Zcash and no action is required by Zcash users.**

The counterfeiting vulnerability was discovered by a cryptographer employed by the Zerocoin Electric Coin Company (aka The Zcash Company) on March 1st, 2018. It was not reported publicly at the time in order to protect against it being exploited prior to its remediation, and to provide information and remediated code to other projects that were also vulnerable. We employed stringent operational security measures to keep its existence a secret, even from our own engineers.

We believe that no one else was aware of the vulnerability and that no counterfeiting occurred in Zcash for the following reasons:

- Discovery of the vulnerability would have required a high level of technical and cryptographic sophistication that very few people possess.
- The vulnerability had existed for years but was undiscovered by numerous expert cryptographers, scientists, third-party auditors, and third-party engineering teams who initiated new projects based upon the Zcash code.

What about Zerocoin?

- Very large proof sizes (25 kB and even reductions can only bring it to 10 kB)
- Trusted setup still exists although done by third party (RSA Factoring Challenge held in 1991)
- Long verification times (300-400ms) per spend transaction
- Usage of fixed denominations
  - Susceptible to timing analysis
  - Inefficient since many spends are needed to fulfil arbitrary amounts
  - Variable anonymity set since it needs to be spread over each denomination.
- Zcoin recently found a cryptographic flaw in one of its proofs allowing forgeries to be made. Although Zerocoin can be fixed, it is non trivial to do so.

Cryptographic description of Zerocoin attack

By Reuben Yap | April 30, 2019 | No Comments

This article has been updated on the 4 May 2019 to add additional potential fixes to Zerocoin with credits to Dmitry Khovratovich at the bottom of this post.

Following our earlier disclosure of the Zerocoin vulnerability that Zcoin discovered, to the best of our knowledge all major projects utilizing Zerocoin have either used sporks to disable Zerocoin or have rolled out an emergency patch to disable Zerocoin and as such this attack will no longer work on them.

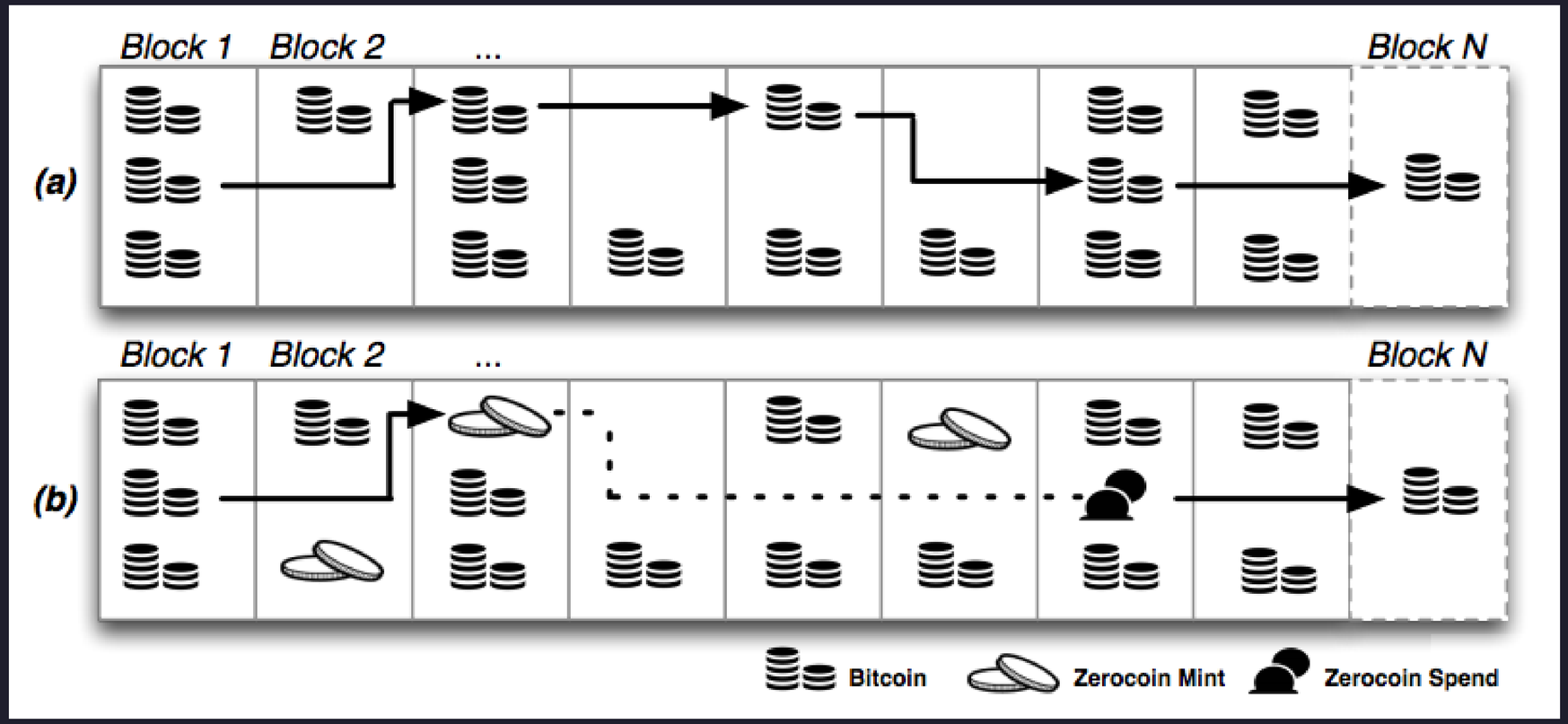
We are releasing this information to assist those who wish to explore fixing Zerocoin and for projects to ascertain whether they've been an target of this attack.

Cryptographic Flaw Description

To spend Zerocoin you need to do the following:

1. Public value of minted coin `C = g^S * h^r (mod p)` is taken and two Pedersen commitments are made to `C` under different groups (`C1` and `C2`)
2. `P1` = ZK proof that `C1` and `C2` are commitments to the same value without disclosing the value in question
3. `P2` = ZK proof that `C2` is committed to the value that is contained in the RSA accumulator
4. `P3` = ZK proof that `C1` is committed to the value which itself is a commitment to the serial `S`

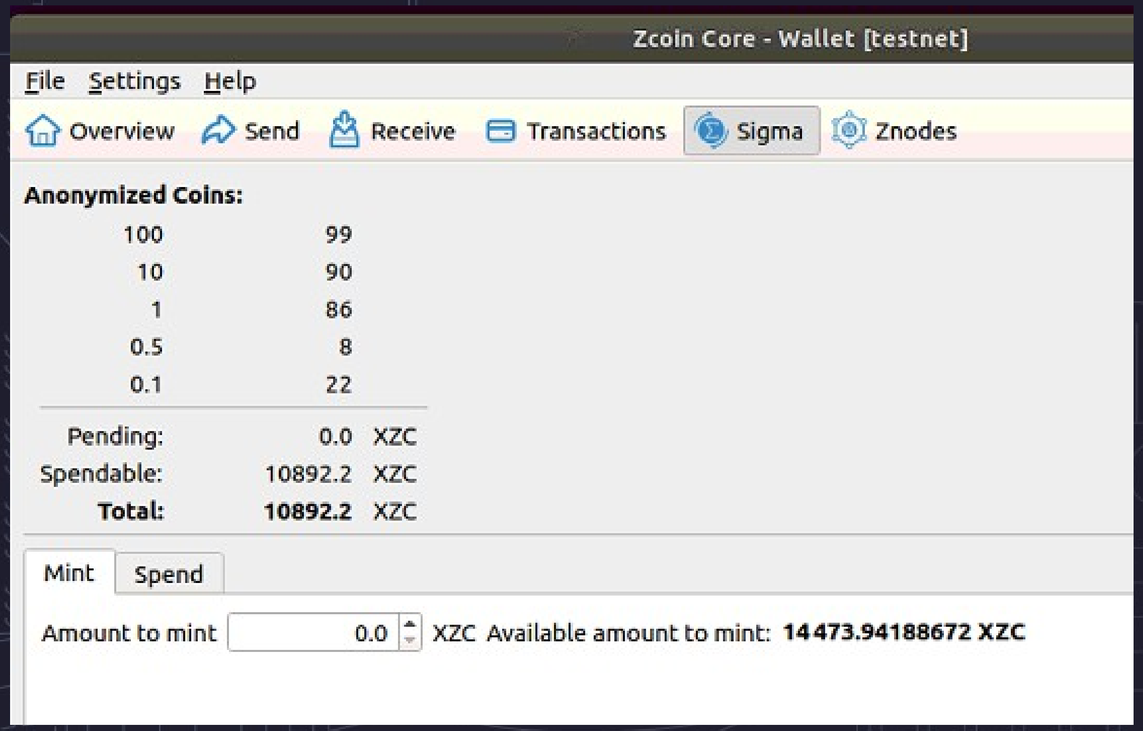
Mint Spend Repeat

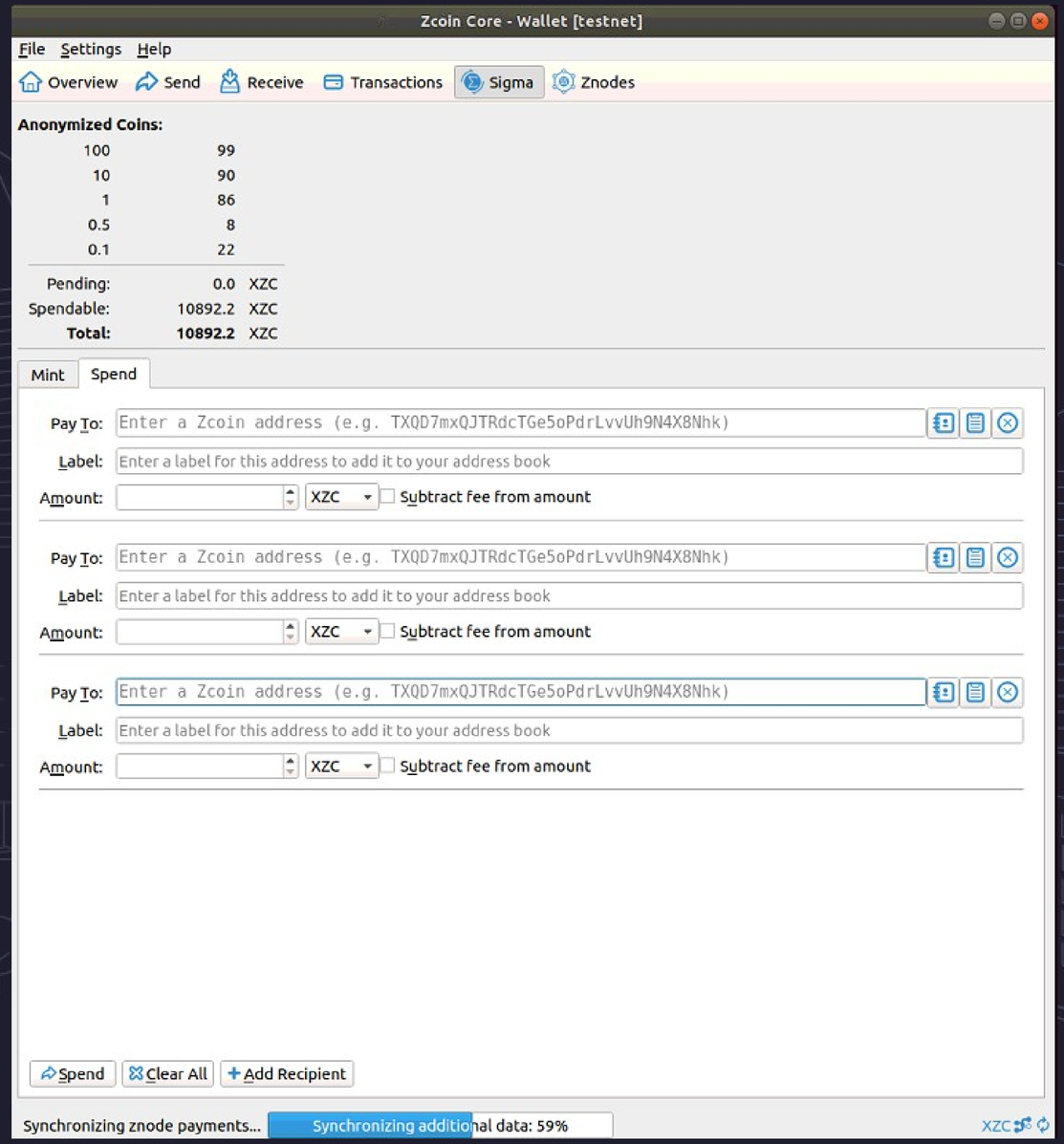


What is Sigma?

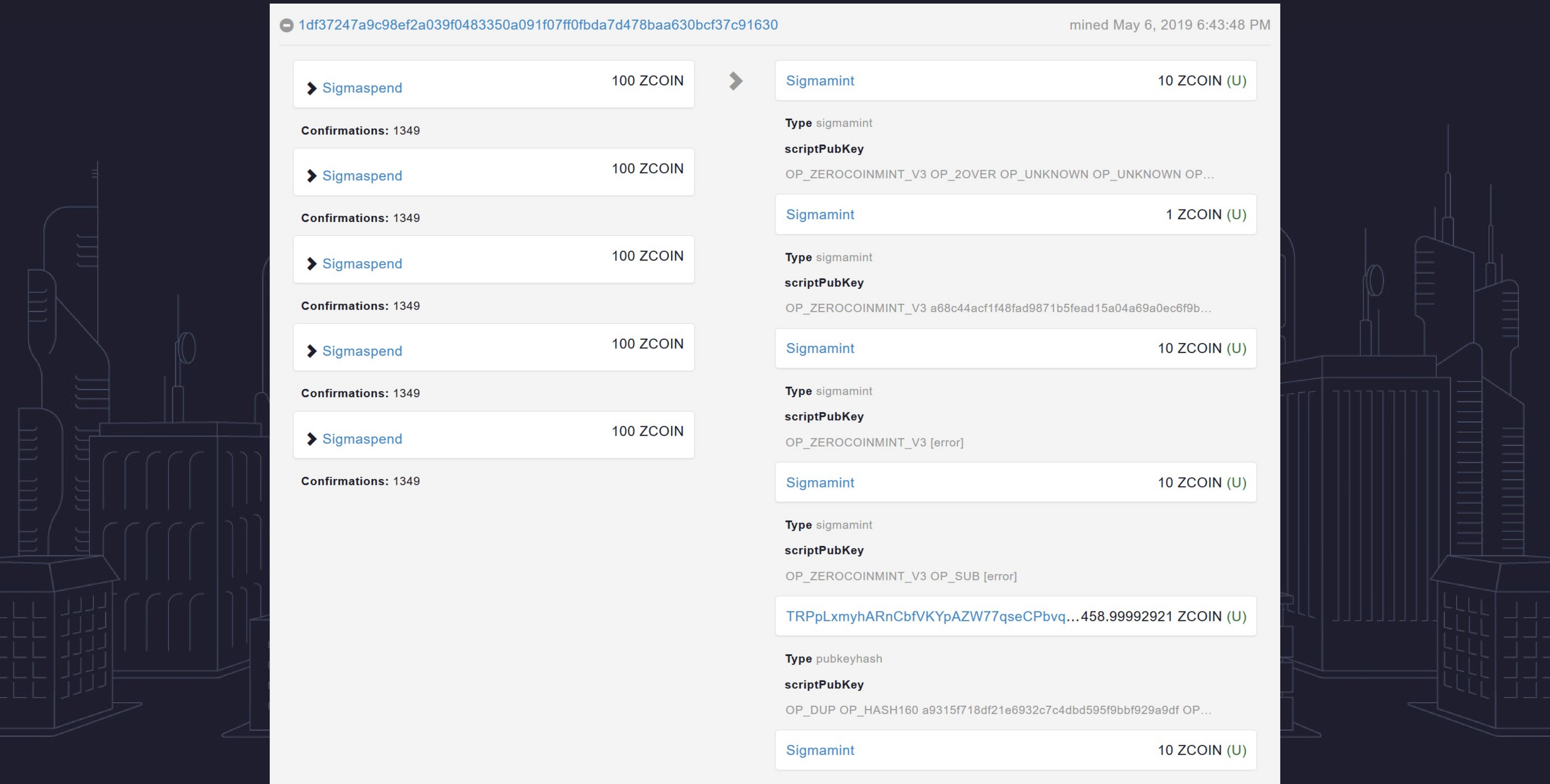
- Replaces the Zerocoin construction
- Based on paper by Jens Groth and Markulf Kohlweiss called One-out-of-Many-Proofs Or How to Leak a Secret and Spend a Coin
- Proof sizes for anonymity sets of 2^14 to 2^18 remain 2kB or less.
- No trusted setup.
- Simple cryptographic construction with full security proofs
- Proofs can be batch verified:
  - Anonymity set 2^16 = 35 ms per proof
  - Anonymity set 2^18 = 180 ms per proof
- Launched on Testnet!
- Expect another month to mainnet.

Sigma in Action





Sigma in Action



The problem with fixed denominations

- Zerocoin and Sigma both use fixed denominations for e.g. 0.1, 0.5, 1, 10, 100
- This is because redemption has to be IN FULL
- If you have a ten dollar note, how do you spend 1.50 to someone else?
- Redeem entire ten dollar note
  - Give 1.50 to third party
  - 8.50 change comes back
- What happens with 8.50 change? Mixes with other unclean funds that can deanonymize.
- Anonymity set within each denomination.

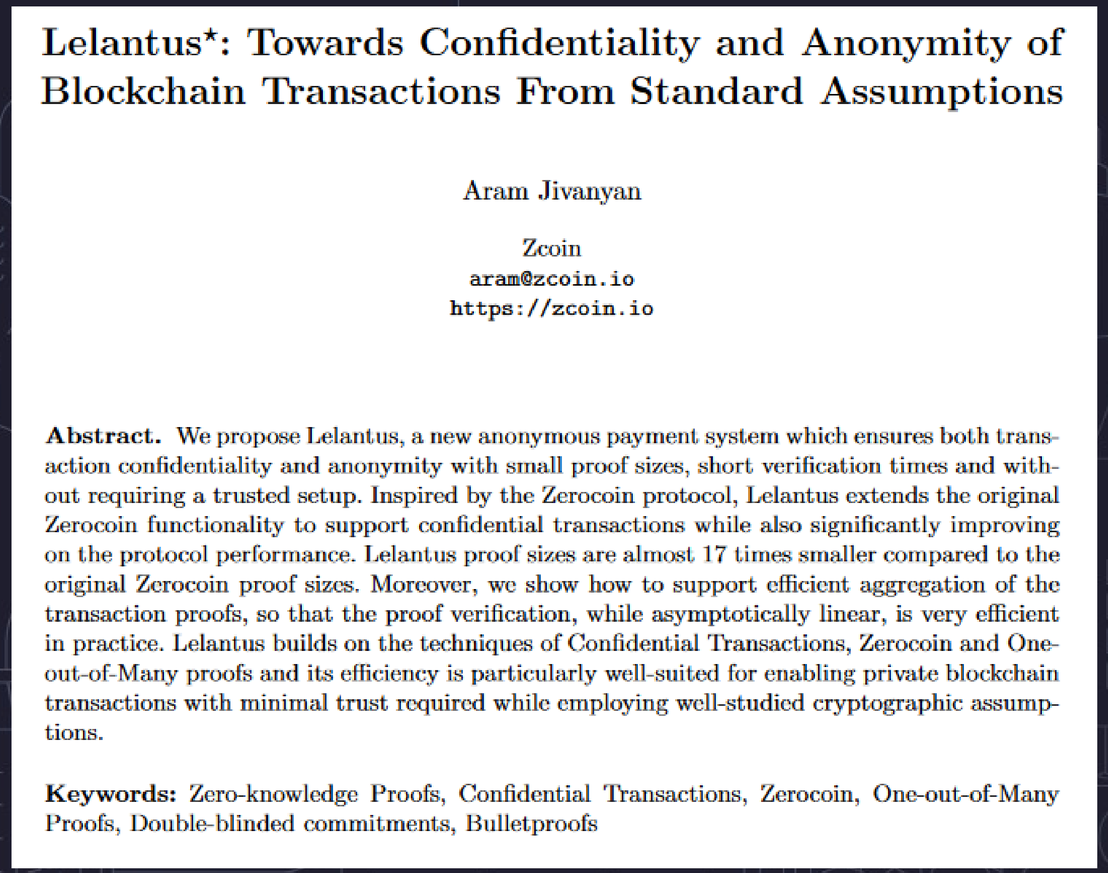
Lelantus

Lelantus builds on Zerocoin’s construction, One Out of Many Proofs and Bulletproofs.
Developed by Zcoin under cryptographer Aram Jivanyan
Operates on same principles of Zerocoin but some key differences

- Doesn’t require trusted setup (uses One out of N proofs instead of RSA accumulators)
- Small proof sizes (less than 2 kb)
- **Doesn’t require fixed denominations.** Burn and spend any arbitrary amount.
- Doesn’t require separate accumulators for each denomination, one global accumulator for all amounts.
- **Has ability to be extended to transfer coins** while in burnt state

Uses DDH cryptographic assumptions

Lelantus



Lelantus*: Towards Confidentiality and Anonymity of Blockchain Transactions From Standard Assumptions

Aram Jivanyan

Zcoin
aram@zcoin.io
https://zcoin.io

Abstract. We propose Lelantus, a new anonymous payment system which ensures both transaction confidentiality and anonymity with small proof sizes, short verification times and without requiring a trusted setup. Inspired by the Zerocoin protocol, Lelantus extends the original Zerocoin functionality to support confidential transactions while also significantly improving on the protocol performance. Lelantus proof sizes are almost 17 times smaller compared to the original Zerocoin proof sizes. Moreover, we show how to support efficient aggregation of the transaction proofs, so that the proof verification, while asymptotically linear, is very efficient in practice. Lelantus builds on the techniques of Confidential Transactions, Zerocoin and One-out-of-Many proofs and its efficiency is particularly well-suited for enabling private blockchain transactions with minimal trust required while employing well-studied cryptographic assumptions.

Keywords: Zero-knowledge Proofs, Confidential Transactions, Zerocoin, One-out-of-Many Proofs, Double-blinded commitments, Bulletproofs

- Cryptographic libraries complete and built entirely by Zcoin (working in private repo)
- Undergoing peer review, much simpler construction makes it easier to audit
- Prominent cryptographers have positive feedback on it Jens Groth (Dfinity), Sarang Noether (Monero), Ariel Gabizon (Zcash)
- Proof of concept made by Sarang and available to public inspection
- Still optimizing, Lelantus+ under development to reduce proof times
- https://eprint.iacr.org/2019/373.pdf

Comparison Chart

	Anonymity Set Size	Trusted Setup	Proof/Private TX Size	Proof Generation Time	Verification Time	Cryptographic Assumptions
Monero	11	NO	~2 -5 kb	<2s	50 ms	Well studied
Zerocash	2^{32}	YES	0.3KB	1-20s	8ms	Relatively New
Zerocoin	2^{13}	YES	25 kB	2-10s	~300ms	Well studied (RSA)
Sigma	2^{16}	NO	~1.5 kB	1.5s	13ms with batch Max 200+ ms without	Well studied (DDH)
Lelantus	2^{16}–2^{17}	NO	~1.5 kB	1.5 – 5s	36-70ms with batch	Well studied (DDH)

Finding out more

- Zcoin.io
- Lelantus: Private transactions with hidden origins and amounts based on DDH (lelantus.io). Paper and presentation with math details
- team@zcoin.io
- Welcome research and comments.
- Telegram @zcoinproject
- Twitter @zcoinofficial