grincon<US>(0)
19.01.28 // hero city, san mateo (CA)

Grin Privacy and Scaling

@yeastplume

Overview

1. Mimblewimble in 1 slide
2. A MW Block
3. Privacy Features
4. Privacy Challenges
5. Scalability Features
6. Scalability Challenges

Mimblewimble in one slide

Confidential Transactions

- Pedersen Commit to hide amounts (Blinding + Value)
- C = b*G + v*H
- CIn1 + CIn2 + CIn3 - COut1 - COut2 - COut3 == 0

Key Mimblewimble Insight

- Interactively choose blinding factors to prove ownership
- (113*G + 3*H) - (28*G + 3*H) = 85*G + 0*H

A Grin Block 1/3

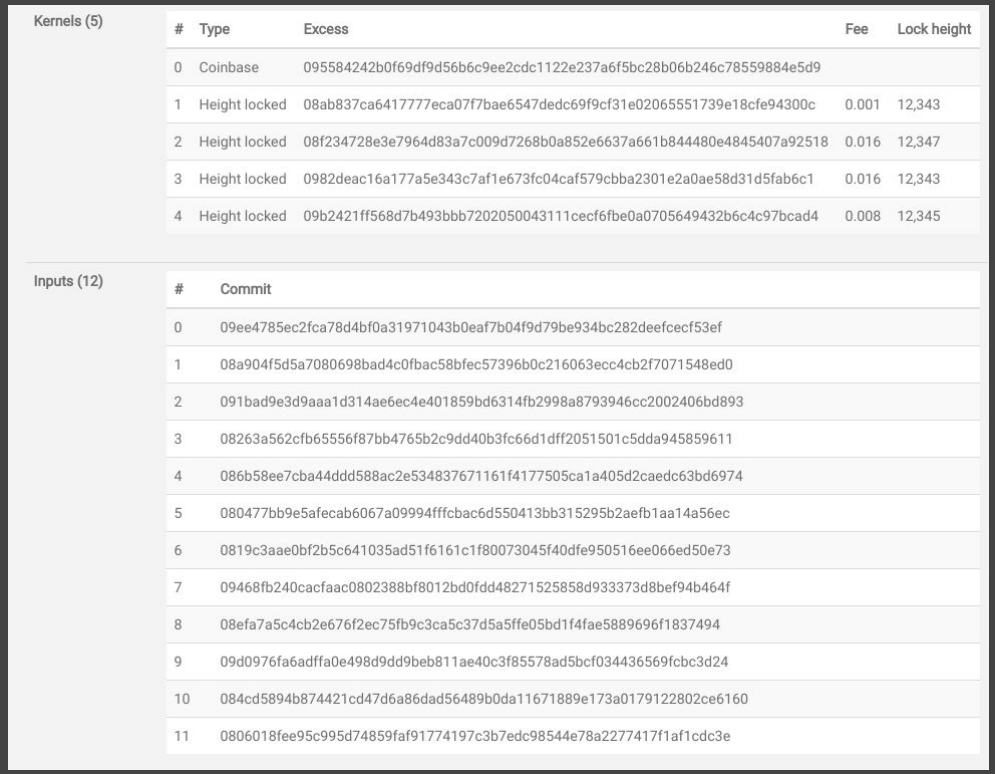
Block 000004d6

Height	12,348
Hash	000004d63a2fa28ddb109db8dae893e85d9599c4158ef65e09861f702cad2dd1
Parent	0000052f1d74dd8aedb3f84ab87d2e7c9635afc0e8c66df0236f4ed6a0730b77
Child(ren)	0000035185d531a7fd50a006be22d92396cb4e728139e9ca70b054896343d571
Version	1
Time	2019-01-24 10:06:36 UTC
Mined in	51s
PoW algorithm	cuckARoo29
AR scale	356
Nonce	2371239233232957133
Solution difficulty	1,234,836,584
Network difficulty	615,633,619
Total difficulty	5,786,434,267,981
Kernel offset	66c3e88ec78242d658421dc123c4e8f61e77a33ea1f69e3aabde9d5cf762d7a8
Total kernel offset	080a298f8470da4fd729c1fad686b0029ddf75248bac78eb37346935f170aa01
Reward	60 + 0.041 Grin

Kernel Offset

- Mitigate transaction reconstruction

A Grin Block 2/3



Kernels (5)

#	Type	Excess	Fee	Lock height
0	Coinbase	095584242b0f69df9d56b6c9ee2cdc1122e237a6f5bc28b06b246c78559884e5d9		
1	Height locked	08ab837ca6417777eca07f7bae6547dedc69f9cf31e02065551739e18cfe94300c	0.001	12,343
2	Height locked	08f234728e3e7964d83a7c009d7268b0a852e6637a661b844480e4845407a92518	0.016	12,347
3	Height locked	0982deac16a177a5e343c7af1e673fc04caf579cbba2301e2a0ae58d31d5fab6c1	0.016	12,343
4	Height locked	09b2421ff568d7b493bbb7202050043111cecf6fbe0a0705649432b6c4c97bcad4	0.008	12,345

Inputs (12)

#	Commit
0	09ee4785ec2fca78d4bf0a31971043b0eaf7b04f9d79be934bc282deefcecf53ef
1	08a904f5d5a7080698bad4c0fbac58bfec57396b0c216063ecc4cb2f7071548ed0
2	091bad9e3d9aaa1d314ae6ec4e401859bd6314fb2998a8793946cc2002406bd893
3	08263a562cfb65556f87bb4765b2c9dd40b3fc66d1dff2051501c5dda945859611
4	086b58ee7cba44ddd588ac2e534837671161f4177505ca1a405d2caedc63bd6974
5	080477bb9e5afecab6067a09994fffcbac6d550413bb315295b2aefb1aa14a56ec
6	0819c3aae0bf2b5c641035ad51f6161c1f80073045f40dfe950516ee066ed50e73
7	09468fb240cacfaac0802388bf8012bd0fdd48271525858d933373d8bef94b464f
8	08efa7a5c4cb2e676f2ec75fb9c3ca5c37d5a5ffe05bd1f4fae5889696f1837494
9	09d0976fa6adffa0e498d9dd9beb811ae40c3f85578ad5bcf034436569fcbc3d24
10	084cd5894b874421cd47d6a86dad56489b0da11671889e173a0179122802ce6160
11	0806018fee95c995d74859faf91774197c3b7edc98544e78a2277417f1af1cdc3e

Kernels
- No way to aggregate (with Schnorr/ secp256k1)
- Doing so would be holy grail
- Features, fee, lock height, excess value, sig

Inputs
- Pedersent Commits
- Referencing previous outputs

A Grin Block 3/3

Outputs (13)

#	Type	Commit
0		080cce2727538d215a13339debda3bff2616e2cb0666402f1898f1fbceb833ba5f
1		09d3ad72a57d3e0a12a6a232b0dcc54ecfbc79f7f8d4546a94bfd0d347cf0b4821
2		08bca992cf2173119b39992e1a185619b9d9796778314d385c940d5b6f35542101
3		080e8c88a0d4a49e347d40cdb48ee1f2e289146f99e0764a01f09cc099d874e603
4		09aa2a791719855f1924ef2e2147af0e1b02acb05cf033f923f37f4765a26de63a
5		09fe2058e2e1e33c1276db6db1bb5bd029355b86281fd4789b4ccd24894a2cfb4f
6		0968e52d329dad8409f90fc8e01d23fe2a113887fee6ab70c282a12649a66a6255
7		08a7cc8506cf7730898879d0e137486efe03ec2e06ae5fb7a2bd418b216987d844
8		09e419bbe04eaadfc4f932a7f4b79652f5f2fe6cd5114e3e347c41881cfc92ce6e
9		0812fc98136d7b32385898fabf16e65b966570c026e71934299ee0bed2bd75e27c
10		0826c68c3a8fa7127190587395015d46f7f65e7148918d716c0d76ffaaeff88cb3
11	Coinbase	0884f46d9ea2922287cbedec3cf9151fc47b25356e49256da11a84e65fa6ddc75c
12		0966958fe678fa522dba861fe5804ff331cb3943a7299cd4be2e34cbce2165455a

Outputs
- Pedersen Commits
- Decoupled from Transaction

Privacy Features

- No visible amounts
- Transactions aggregated
- No initial block download, (blocks don’t need to be kept)
- No identifying information in chain
- Very hard to link inputs to corresponding outputs

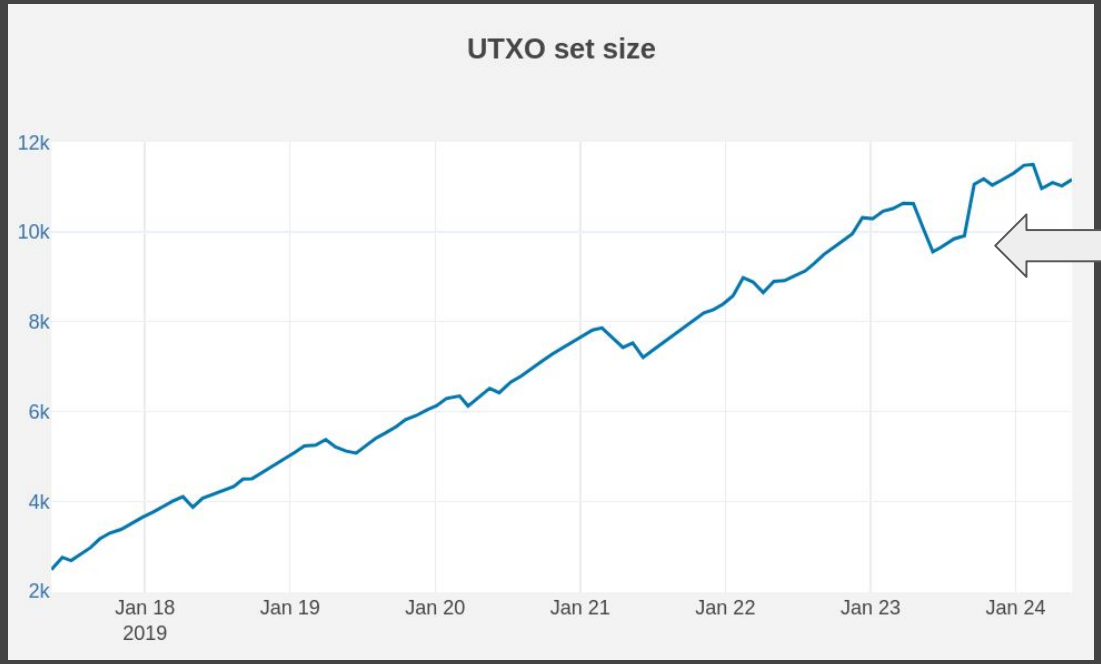
Other Privacy Features

- Wallets Generate Switch commitments
  - Quantamageddon Mitigation
  - Users can optionally reveal information to claim outputs (soft fork)
- Dandelion
  - Obscure/Hide transaction Origin
  - Assists in concealing transaction graph
- 0-Conf Cut-through
  - A -> B, B -> C
  - Becomes A -> C with B cancelled out
- Transaction Aggregation
  - During Dandelion stem phase (minor)

Main Privacy Challenges

- Possibility of TX graph reconstruction (particularly with additional monitoring)
- How resistant are our privacy features to motivated adversaries?

Scalability



Main Scalability Features

- Elegance of MW Privacy
- Output Destruction
  - Outputs are Pruned from PMMR
  - Whole sections of PMMR tree can be pruned
  - Wallet defaults to sweeping outputs
- Block data can be dropped
- Fast Sync
  - Time to sync new node should be (more or less) constant
- Cut-through
  - Theoretical scaling feature but in practice?

Main Scalability Challenges

- Rangeproof Size
  - Bulletproofs good, but can’t use aggregation features
- Kernel immutability
  - Kernels can’t be aggregated, stay around forever
- All remains to be seen
- Pending Technology - A lot of promise but:
  - Add features without bloating data
  - The theoretical doesn’t always work as cleanly in practice

https://grin-tech.org