Grin: a technical introduction

@hashmap
BUIDL Asia 2019

About Grin

Better money ツ

A lightweight implementation of a cryptocurrency that aims to be privacy preserving, scalable, and fair.

About me

- Grin core developer
- Grin Council member
- Co-founder of a cypherpunk collective cycle42 (https://cycle42.com/)

Contents

- Mimblewimble
- Grin project
- Demo

Mimblewimble history

- Blockchain design proposed by Tom Elvis Jedusor (*Je suis Voldemort* - I am Voldemort), August 2016
- Mimblewimble is a tongue-tying curse used in "The Deathly Hallows"
- Improved by Andrew Poelstra, October 2016
- Grin project initial code published by Ignotus Peverell (the original owner of the invisibility cloak), October 2016
- Name Grin comes from Gringotts Wizarding Bank

Mimblewimble properties

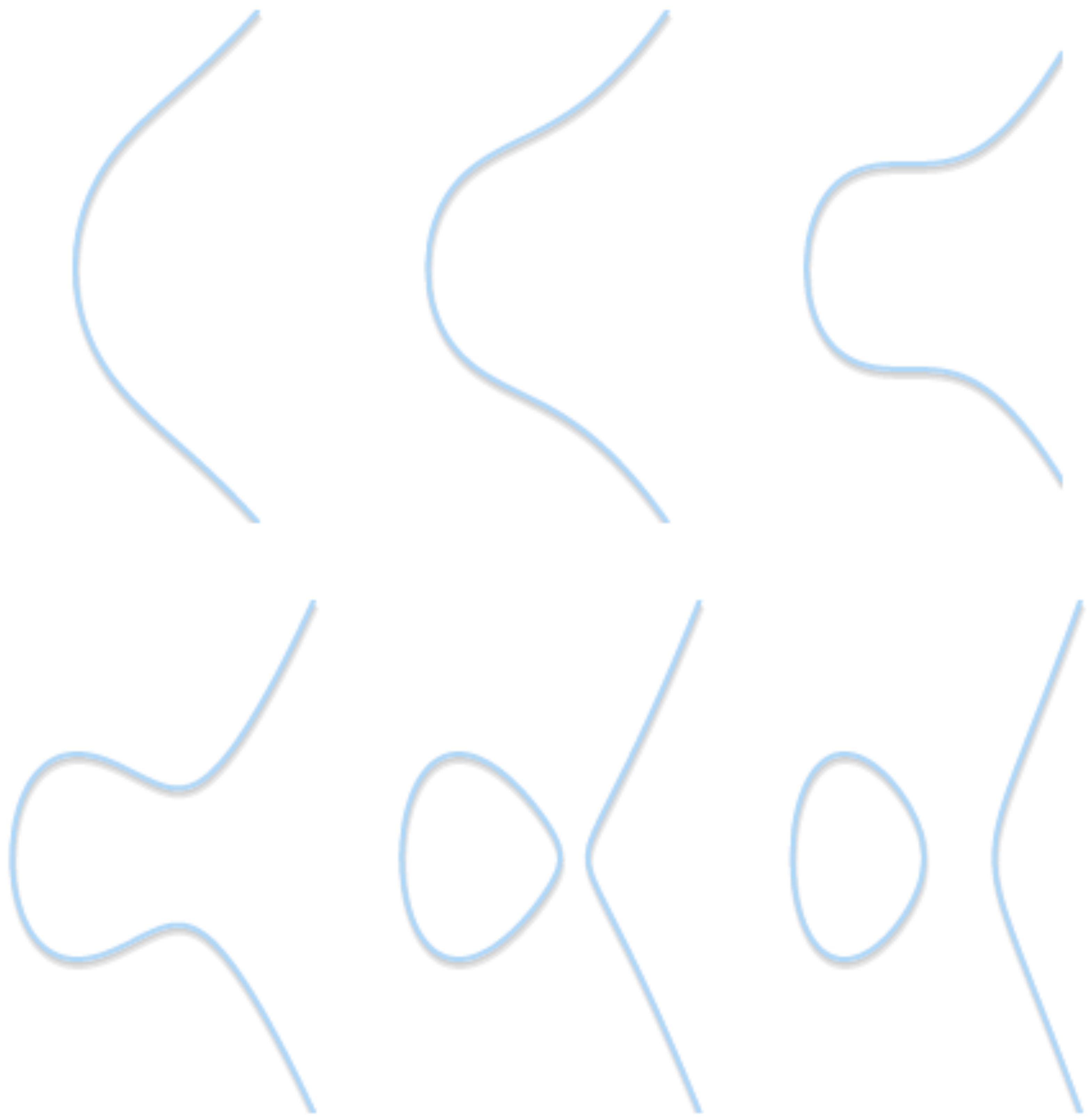
- Scalable: Little data required for full sync.
- Fungible: No amounts, no scripts, no addresses.
- Requires interaction to build transactions.
- Proven math (Elliptic Curves Cryptography).

Refresher: Elliptic curves

$$y^2 = x^3 + ax + b$$

$$4a^3 + 27b^2 \neq 0$$

And infinity point 0



https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

Refresher: Elliptic curves on $\mathbb{F}_p$

$$\Big\{(x,y) \in (\mathbb{F}_p)^2 \quad | \quad y^2 \equiv x^3 + ax + b \pmod{p},$$

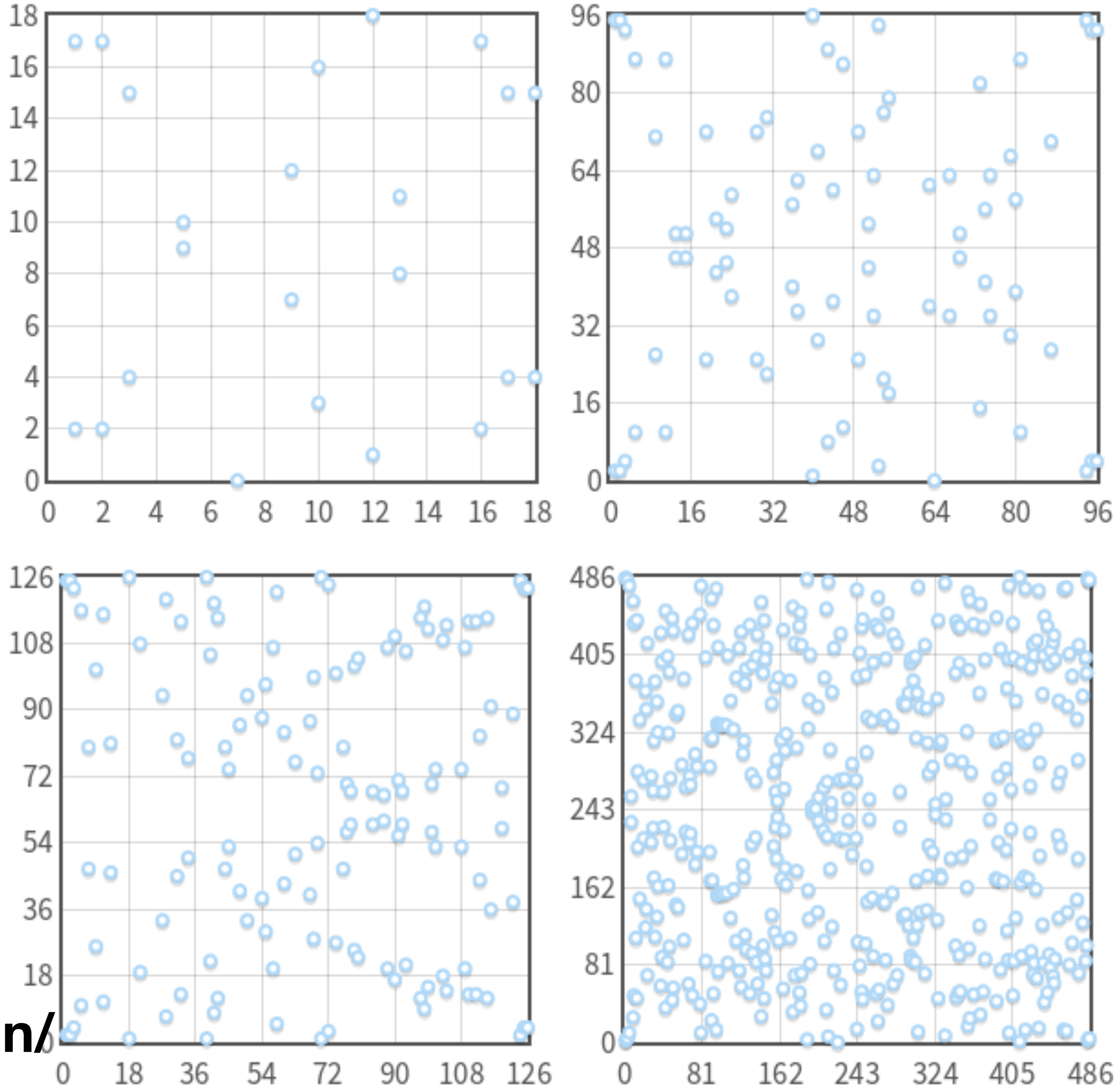
$$4a^3 + 27b^2 \not\equiv 0 \pmod{p}\Big\} \ \cup \ \{0\}$$

mod p:

$$(18 + 9) \bmod 23 = 4$$

$$(7 - 14) \bmod 23 = 16$$

$$4 \cdot 7 \bmod 23 = 5$$



https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

Elliptic Curve Cryptography

- Curve C
- Point addition $G + H$
- Scalar multiplication $k \cdot H$
- Commutativity, associativity (Abelian group) $(k + j) \cdot H \;= k \cdot H + j \cdot H$
- Discrete logarithm is hard $Q = n \cdot P$ can't find n knowing Q, P
- Private key k public key $k \cdot H$

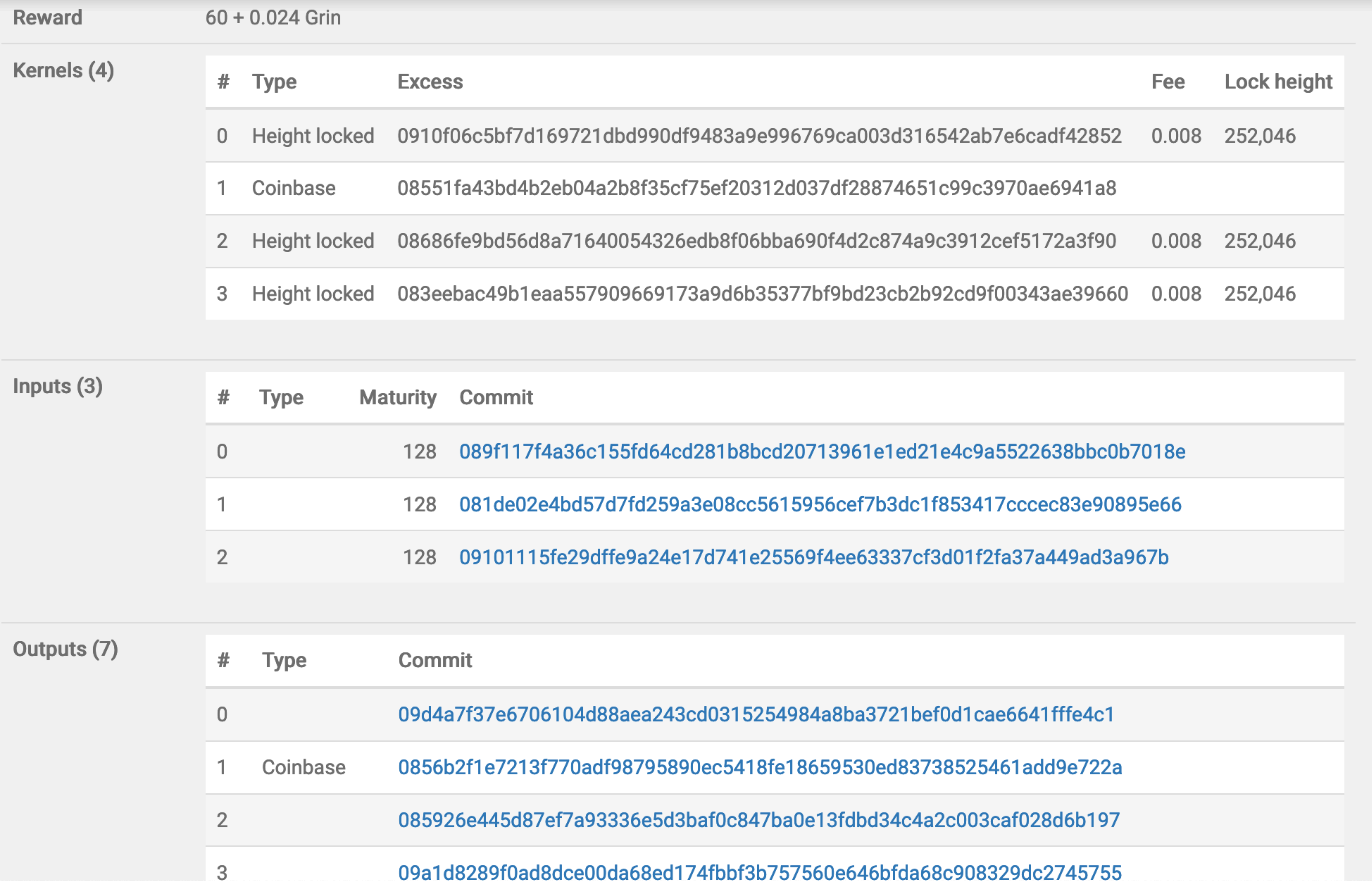
Hiding transaction amount

- Transaction $v_{i1} + v_{i2} = v_{o1}$
- Hiding $v_{i1} \cdot H + v_{i2} \cdot H = v_{o1} \cdot H$
- Validation without revealing v_{i1}, v_{i2}, v_{o1}
- Easy to attack

Hiding a number in Pedersen commitment

- Transaction amount v
- Pedersen commitment $r \cdot G + v \cdot H$
- where $G, H \in C$
- private key (blinding factor) r
- Need to remember $r \cdot G$

Block



Reward 60 + 0.024 Grin

Kernels (4)

#	Type	Excess	Fee	Lock height
0	Height locked	0910f06c5bf7d169721dbd990df9483a9e996769ca003d316542ab7e6cadf42852	0.008	252,046
1	Coinbase	08551fa43bd4b2eb04a2b8f35cf75ef20312d037df28874651c99c3970ae6941a8		
2	Height locked	08686fe9bd56d8a71640054326edb8f06bba690f4d2c874a9c3912cef5172a3f90	0.008	252,046
3	Height locked	083eebac49b1eaa557909669173a9d6b35377bf9bd23cb2b92cd9f00343ae39660	0.008	252,046

Inputs (3)

#	Type	Maturity	Commit
0		128	089f117f4a36c155fd64cd281b8bcd20713961e1ed21e4c9a5522638bbc0b7018e
1		128	081de02e4bd57d7fd259a3e08cc5615956cef7b3dc1f853417cccec83e90895e66
2		128	09101115fe29dffe9a24e17d741e25569f4ee63337cf3d01f2fa37a449ad3a967b

Outputs (7)

#	Type	Commit
0		09d4a7f37e6706104d88aea243cd0315254984a8ba3721bef0d1cae6641fffe4c1
1	Coinbase	0856b2f1e7213f770adf98795890ec5418fe18659530ed83738525461add9e722a
2		085926e445d87ef7a93336e5d3baf0c847ba0e13fdbd34c4a2c003caf028d6b197
3		09a1d8289f0ad8dce00da68ed174fbbf3b757560e646bfda68c908329dc2745755

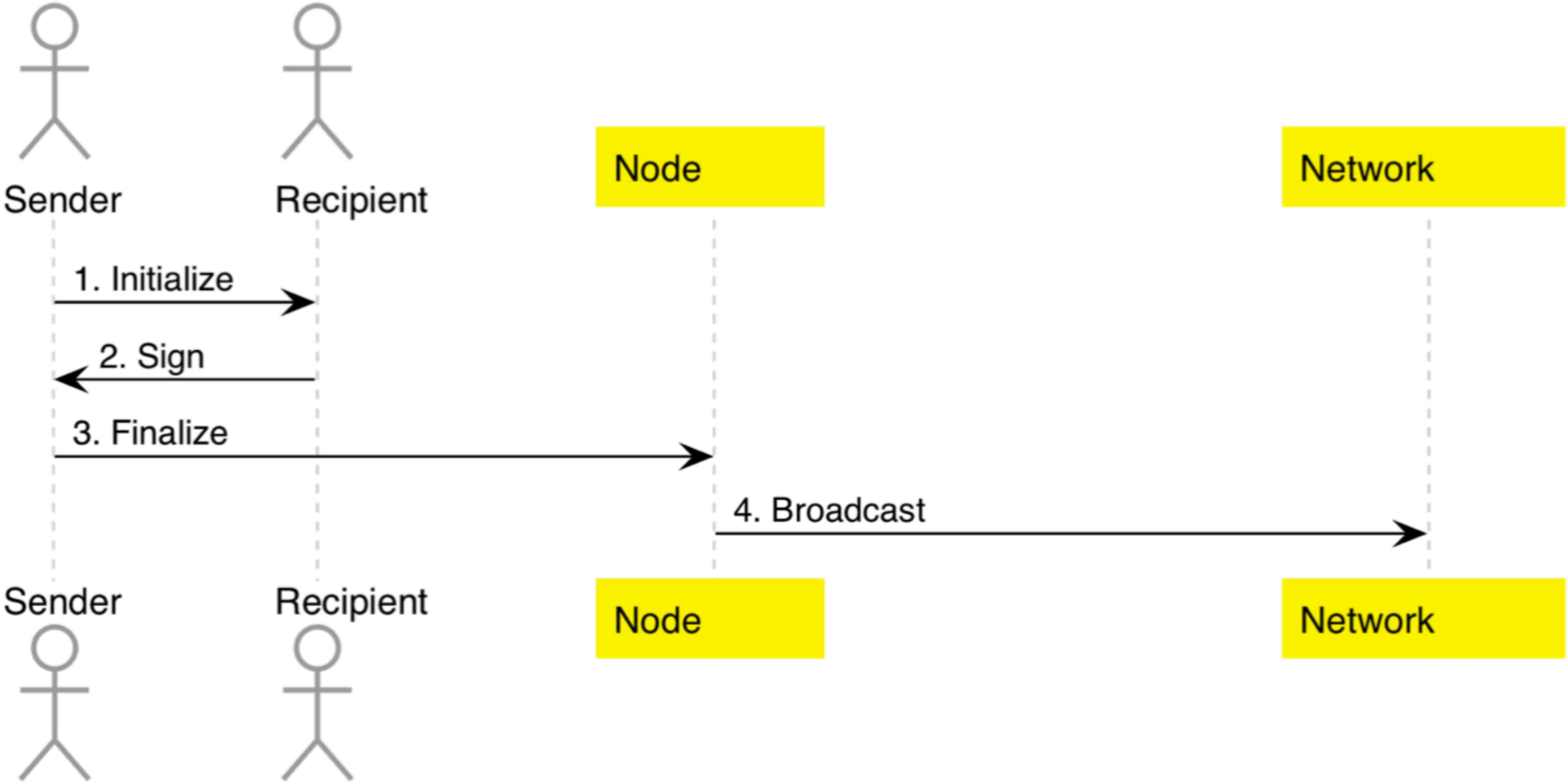
Turtles all the way down

- Transaction (kernel(s), inputs, outputs)
- Block (kernels, inputs, outputs)
- Chain (kernels, inputs, outputs)

Validation: the main principle

- No new money created (except block reward)
- Transaction level: sum inputs (+ kernel) == sum outputs
- UTXO level: sum outputs == number of blocks * 60 (+ kernels)
- Rangeproof (Bulletproofs) to prevent negative values
- Bonus - spent coins add 0 (+kernels)!

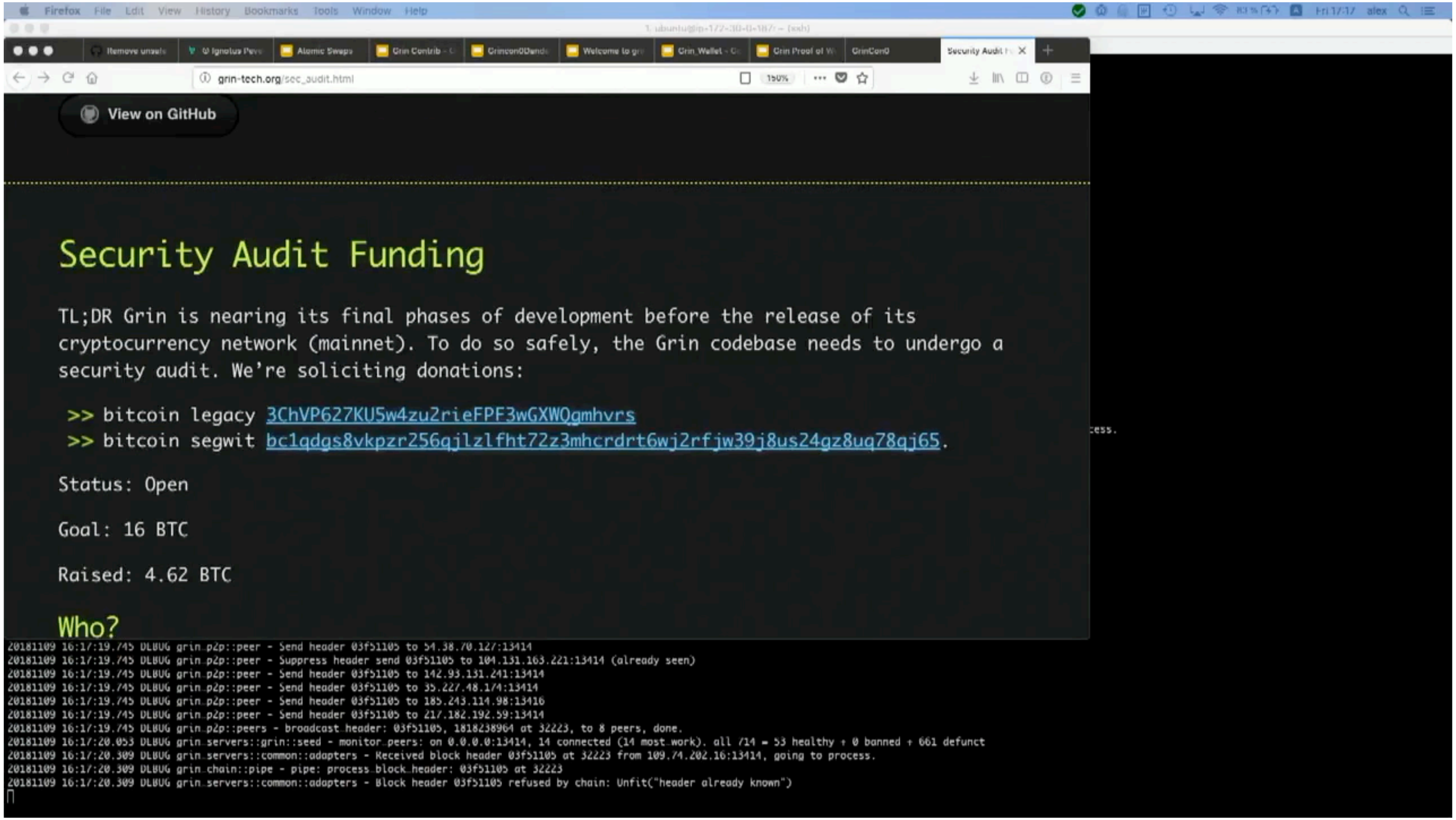
Interactive transaction building



Grin project

- Announced October 20th, 2016 by Ignotus Peverell
- First Mimblewimble implementation
- Written in Rust
- Open source, 100% community driven
- Funded by donations
- No: ICO, CEO, DevCo, advisors, investors, founder rewards, premine, pre-allocation
- Fair launch

Ignotus Peverell
Grincon0, Berlin, November 9th 2018



Security Audit Funding

TL;DR Grin is nearing its final phases of development before the release of its cryptocurrency network (mainnet). To do so safely, the Grin codebase needs to undergo a security audit. We're soliciting donations:

>> bitcoin legacy 3ChVP627KU5w4zu2rieFPF3wGXWQgmhvrs
>> bitcoin segwit bc1qdgs8vkpzr256qjlzlfht72z3mhcrdrt6wj2rfjw39j8us24gz8uq78qj65.

Status: Open

Goal: 16 BTC

Raised: 4.62 BTC

Who?

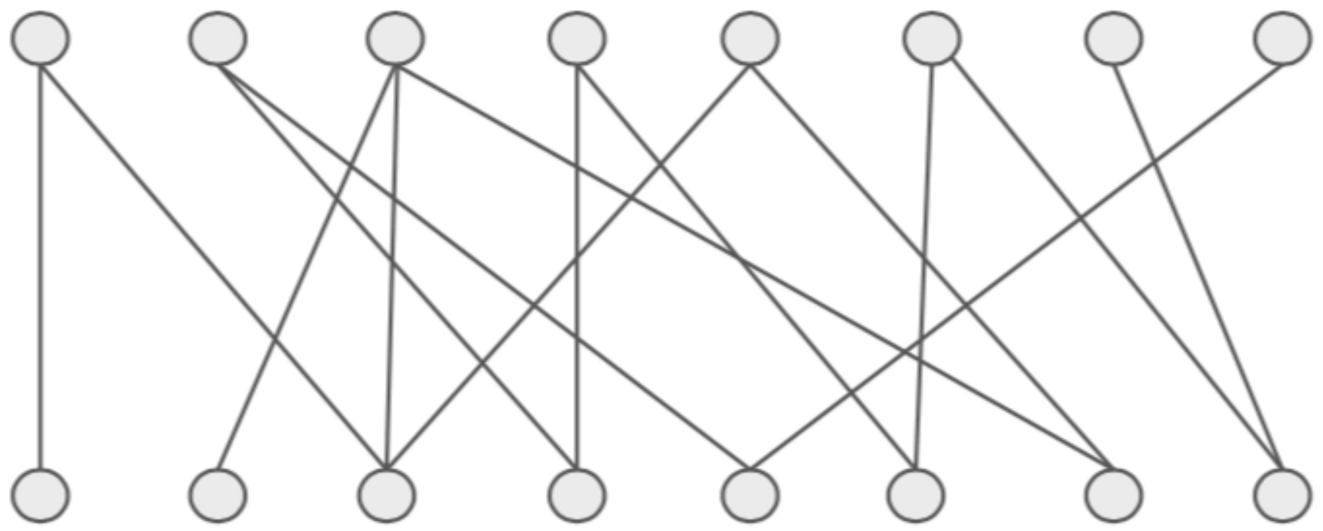
```
20181109 16:17:19.745 DEBUG grin_p2p::peer - Send header 03f51105 to 54.38.70.127:13414
20181109 16:17:19.745 DEBUG grin_p2p::peer - Suppress header send 03f51105 to 104.131.163.221:13414 (already seen)
20181109 16:17:19.745 DEBUG grin_p2p::peer - Send header 03f51105 to 142.93.131.241:13414
20181109 16:17:19.745 DEBUG grin_p2p::peer - Send header 03f51105 to 35.227.48.174:13414
20181109 16:17:19.745 DEBUG grin_p2p::peer - Send header 03f51105 to 185.243.114.98:13416
20181109 16:17:19.745 DEBUG grin_p2p::peer - Send header 03f51105 to 217.182.192.59:13414
20181109 16:17:19.745 DEBUG grin_p2p::peers - broadcast_header: 03f51105, 1818238964 at 32223, to 8 peers, done.
20181109 16:17:20.053 DEBUG grin_servers::grin::seed - monitor_peers: on 0.0.0.0:13414, 14 connected (14 most_work). all 714 = 53 healthy + 0 banned + 661 defunct
20181109 16:17:20.309 DEBUG grin_servers::common::adapters - Received block header 03f51105 at 32223 from 109.74.202.16:13414, going to process.
20181109 16:17:20.309 DEBUG grin_chain::pipe - pipe: process_block_header: 03f51105 at 32223
20181109 16:17:20.309 DEBUG grin_servers::common::adapters - Block header 03f51105 refused by chain: Unfit("header already known")
```

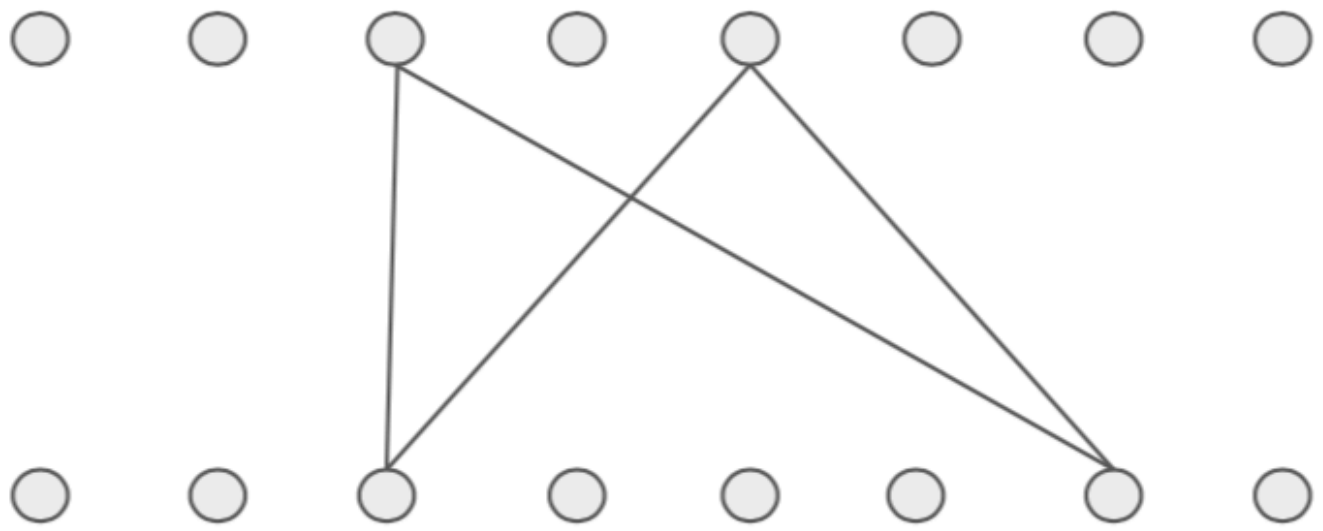
Technologies used

- Schnorr signatures
- Bulletproofs: zero knowledge range proof
- Dandelion: privacy-preserving transaction propagation
- Scriptless scripts

Proof of work

- Finding 42-cycles in random bipartite graphs with billions of nodes
- Creator: John Tromp
- Family of algorithms

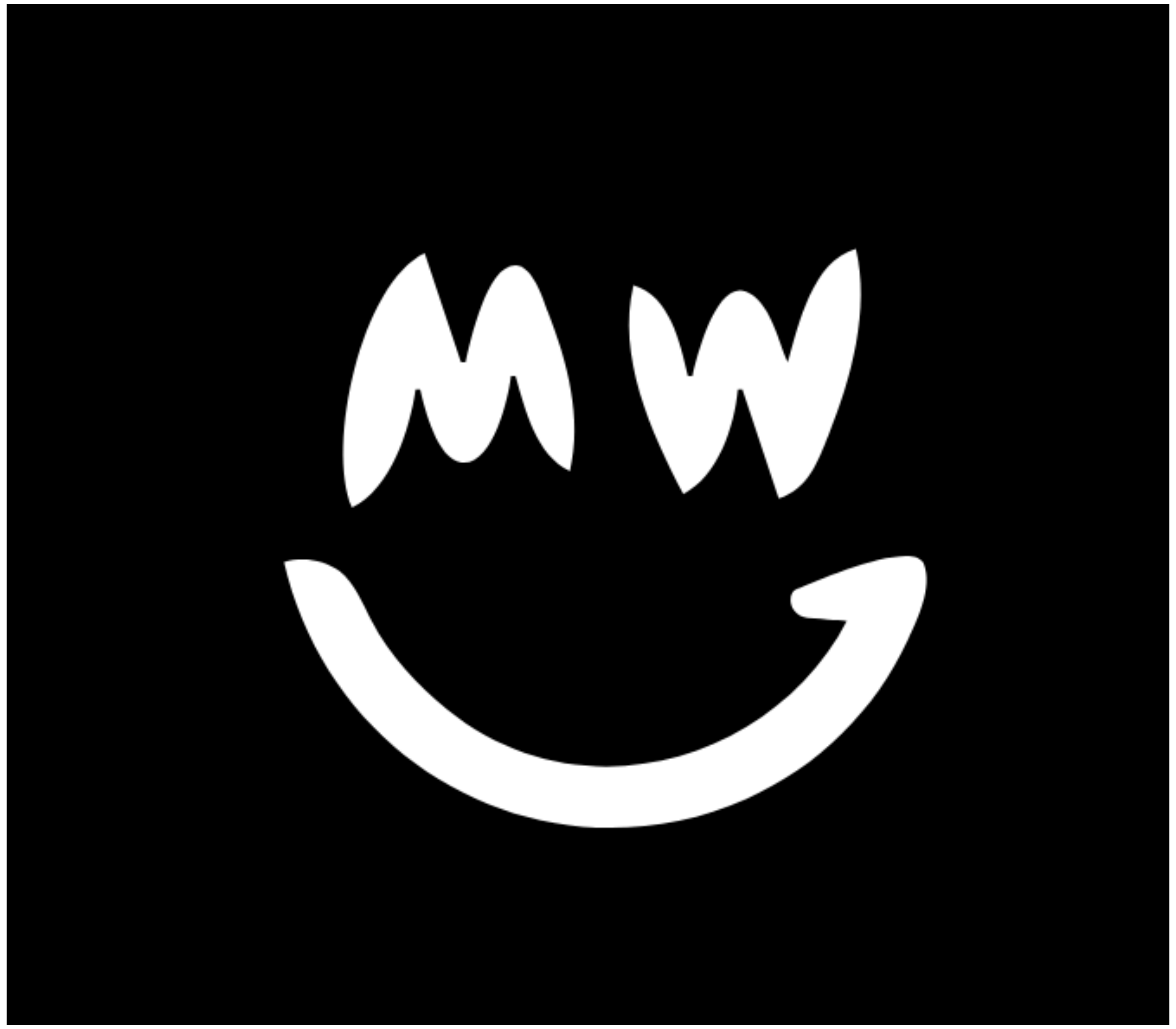




Grin resources

- Web site http://grin-tech.org/
- Forum http://grin-forum.org/
- Github https://github.com/mimblewimble
- Gitter chat https://gitter.im/grin_community/Lobby

Demo



고맙습니다

- https://hasmap.dev
- Twitter @hashmap

D327 50FD D334 BC55 A5A5 ACEB 5EA3 C2D2 455E D9C8