Hackers Congress 2019
06.10.2019 // Prague

A view on Grin

Michalis Kargakis

About this talk

- Walkthrough of the project
- Subjective here and there

About me

Software engineer by trade, cypherpunk at heart

- 2014: Bitcoin (btcsuite)
- 2015-2018: Kubernetes, Red Hat
- 2019-: Guardtime

In parallel:

- 2018-2020: MSc in Digital Currency
- Following Grin since Hackers Congress 2017

Grin tl;dr

A cryptocurrency focusing on privacy, scalability, and fairness.

How privacy

How privacy

Mimblewimble is a blockchain design proposed by Jedusor (2016), improved by Poelstra (2016).

On chain:

- No amounts (Confidential Transactions, Bulletproofs)
- No addresses (Interactive tx building)

No amounts

- Confidential Transactions (G. Maxwell, 2016)

  Relying on Elliptic Curves Cryptography (ECC)

- Bulletproofs (B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, G. Maxwell, 2017)

No amounts

$$v1 + v2 = v3 \quad => \quad v1*H + v2*H = v3*H$$

No amounts

$v1 + v2 = v3 \Rightarrow v1*H + v2*H = v3*H$

Problem: Transaction amounts (*v1*, *v2*, *v3*, …, *vN*) are finite so can be brute-forced

No amounts

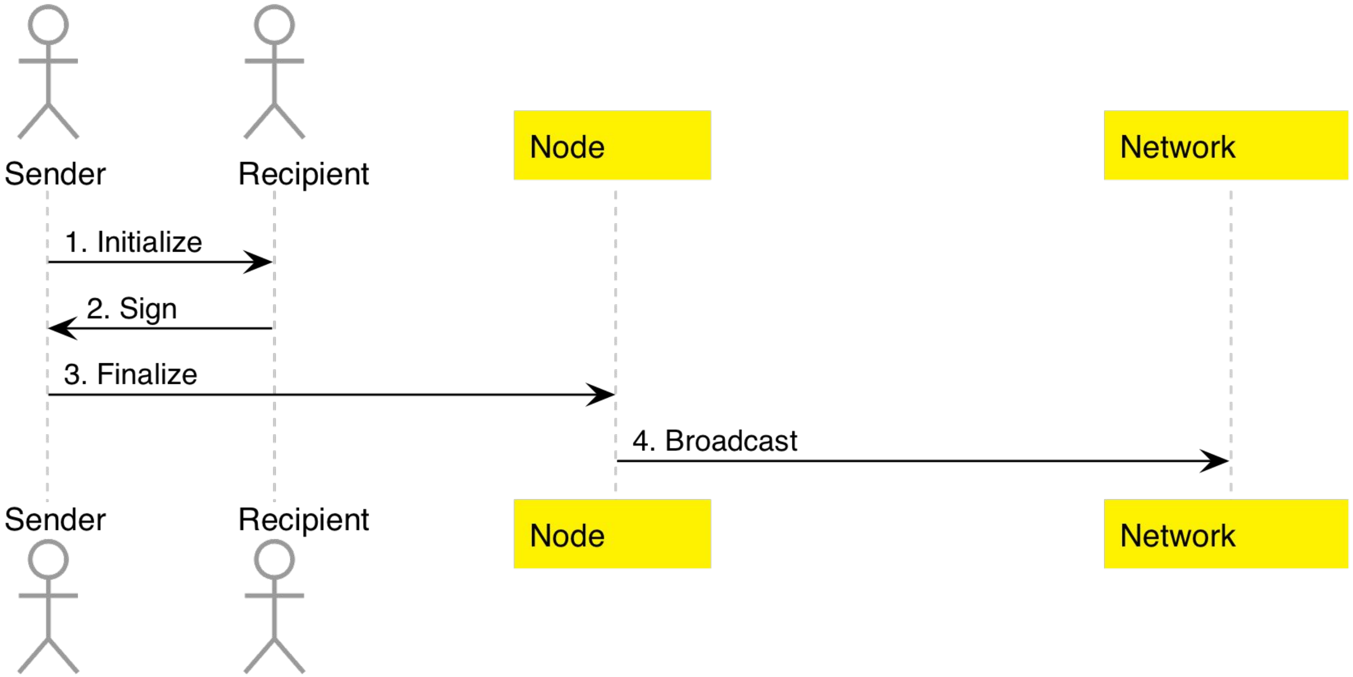
$$v1 + v2 = v3 \quad => \quad v1*H + v2*H = v3*H$$

Problem: Transaction amounts ($v1$, $v2$, $v3$, …, vN) are finite so can be brute-forced

Hence, Pedersen Commitments: **$r*G + v*H$**

$$(ri1*G + vi1*H) + (ri2*G + vi2*H) = (ro3*G + vo3*H)$$

No addresses

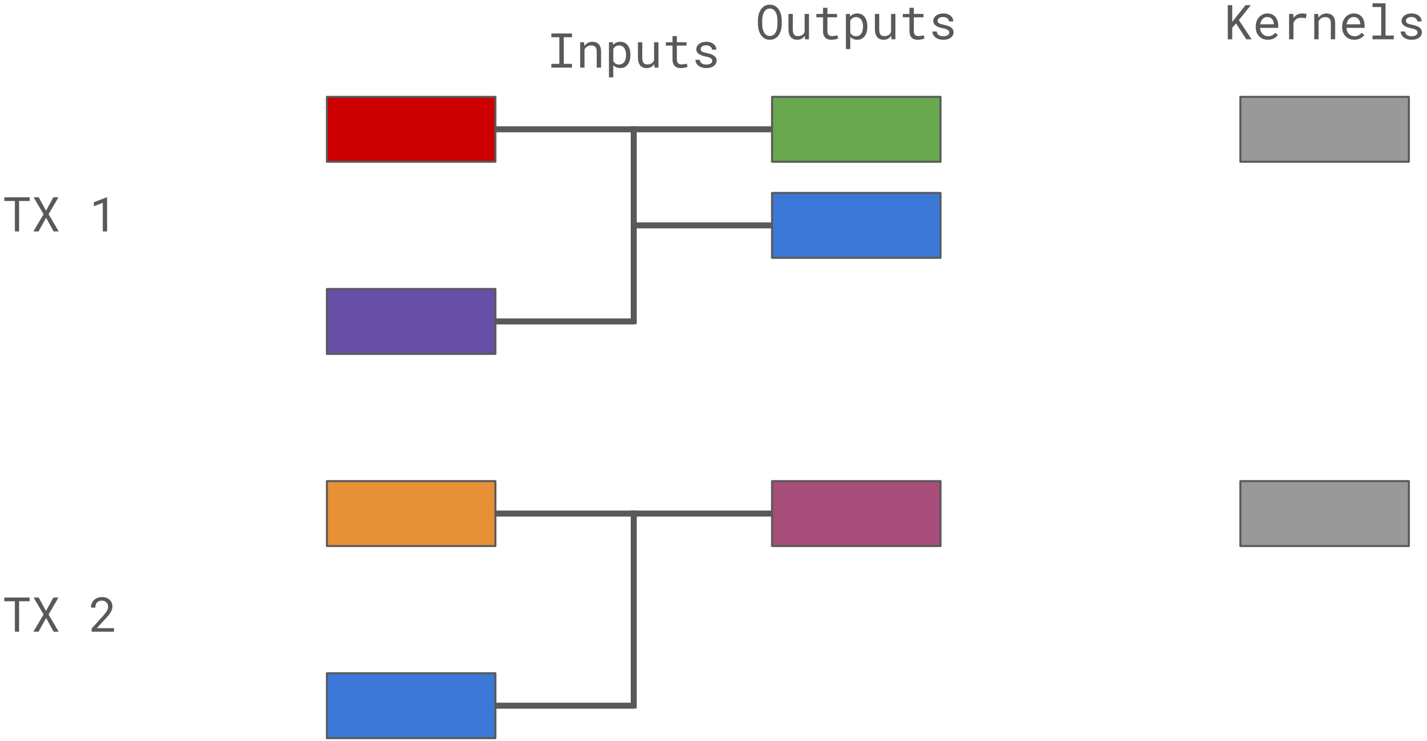


How privacy

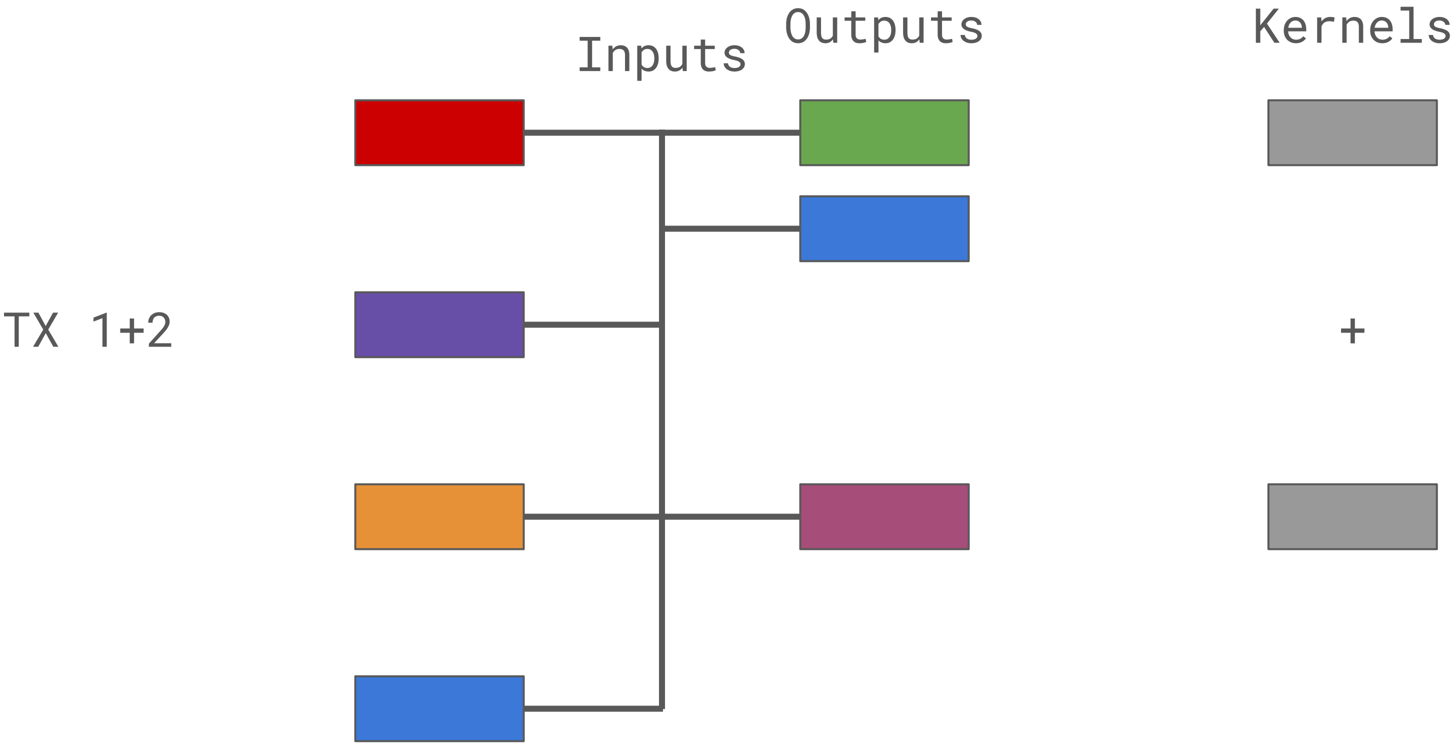
Off chain:

- Tx aggregation (CoinJoin, G. Maxwell, 2013)(OWAS, H. Mouton, 2013)
- Dandelion++ (BIP 156)
- (wip) Overlay networks (I2P, Tor)

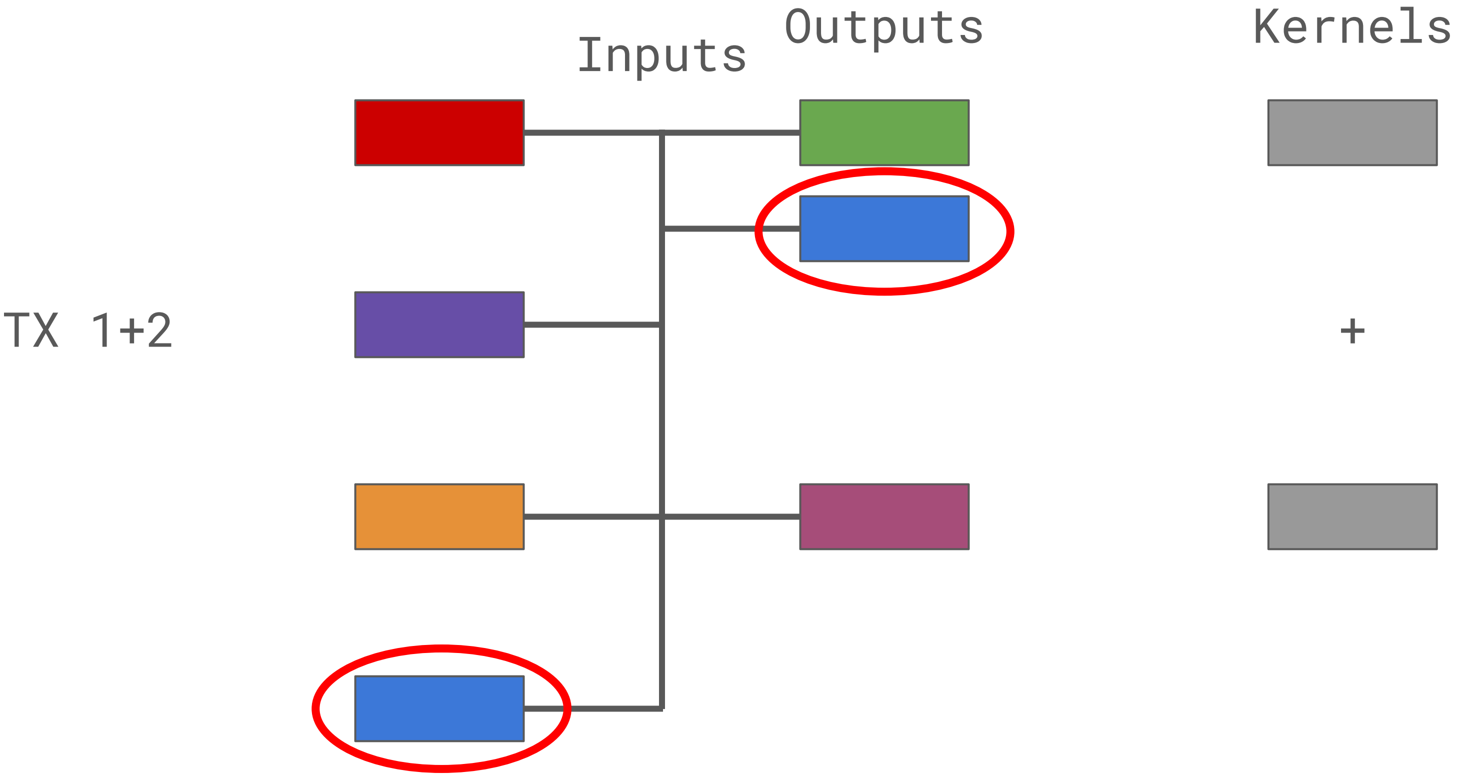
Transaction aggregation



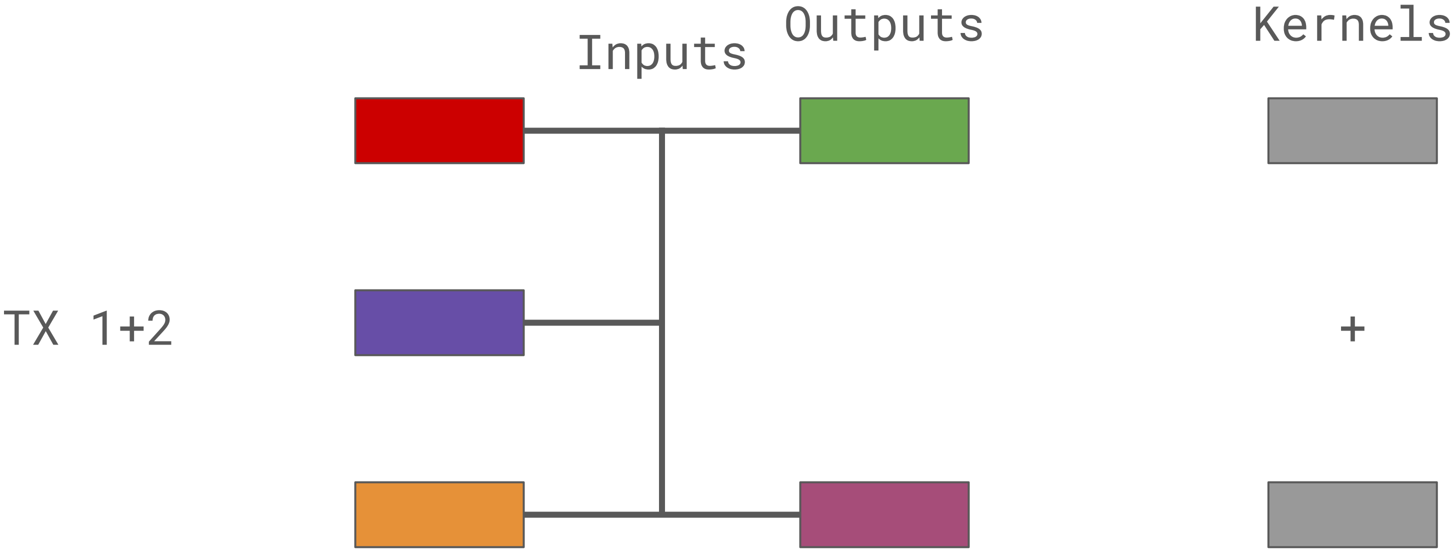
Transaction aggregation



Transaction aggregation



Transaction aggregation



Dandelion++

- Proposed and enhanced by Fanti, et al (2017-2018)
- Defend against deanonymization attacks during tx propagation
- In Grin, also an opportunity to aggregate txs before they are broadcasted to the entire network

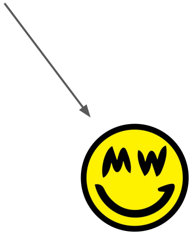
Dandelion++

Pre-Dandelion:

Transaction propagation is mere diffusion

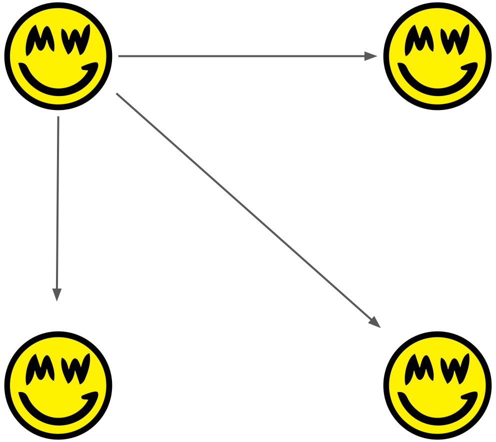
Dandelion++

Pre-Dandelion:



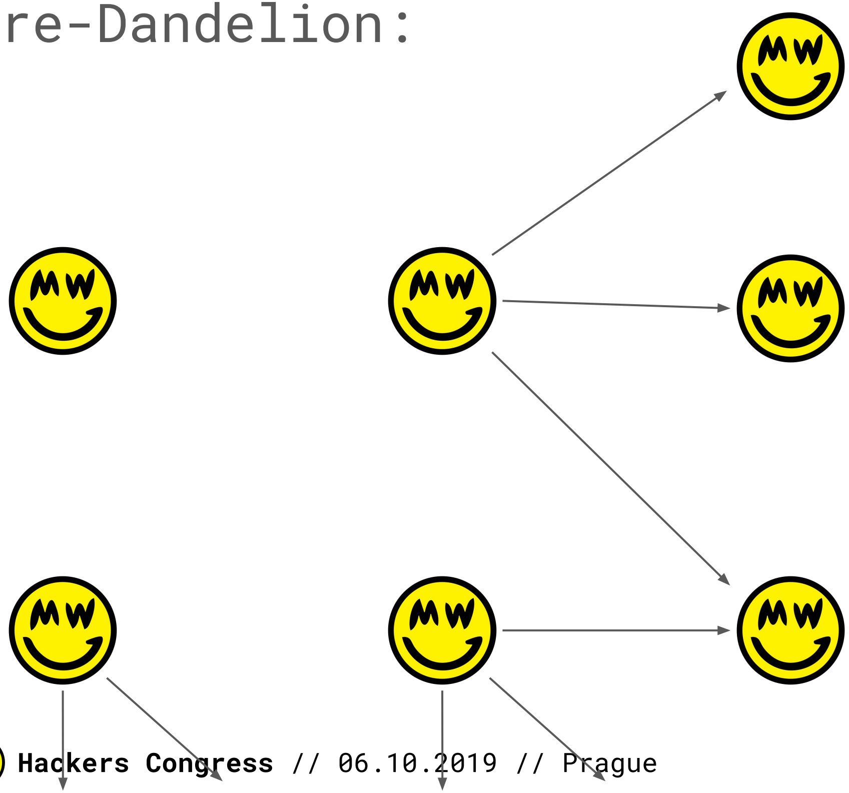
Dandelion++

Pre-Dandelion:



Dandelion++

Pre-Dandelion:



Dandelion++

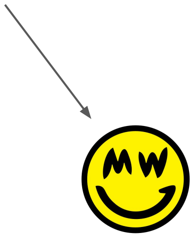
Every epoch*, each node decides:

- either fluff or stem txs**
- if stem, choose an outbound peer to send txs

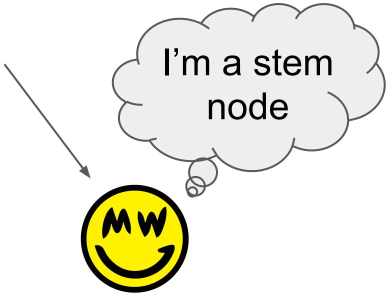
* 10 minutes

** 90% chance to stem / 10% to fluff

Dandelion++

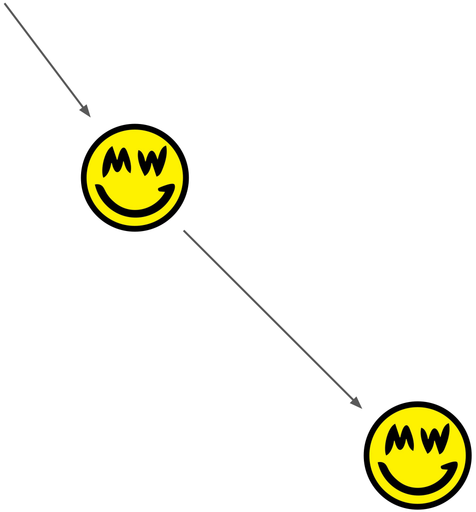


Dandelion++

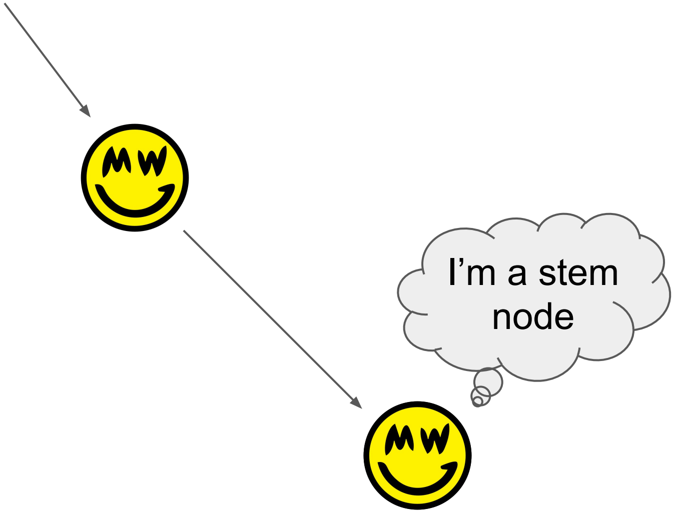


I’m a stem node

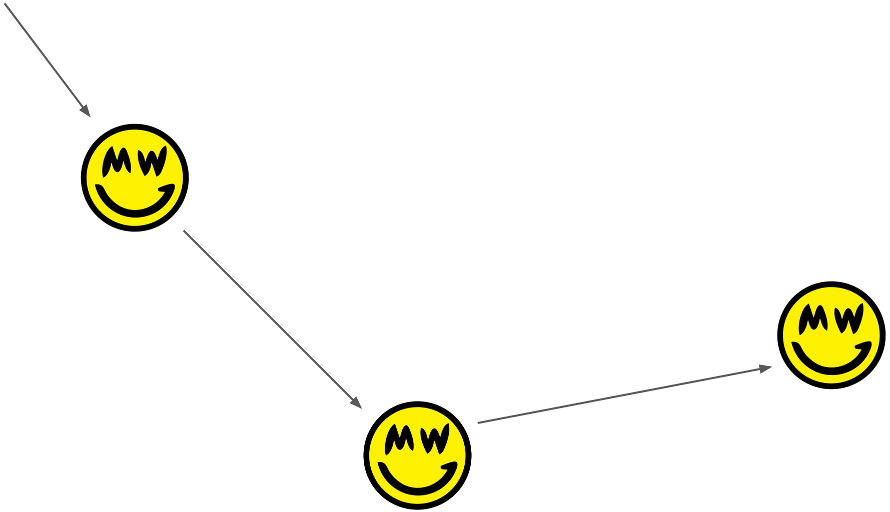
Dandelion++



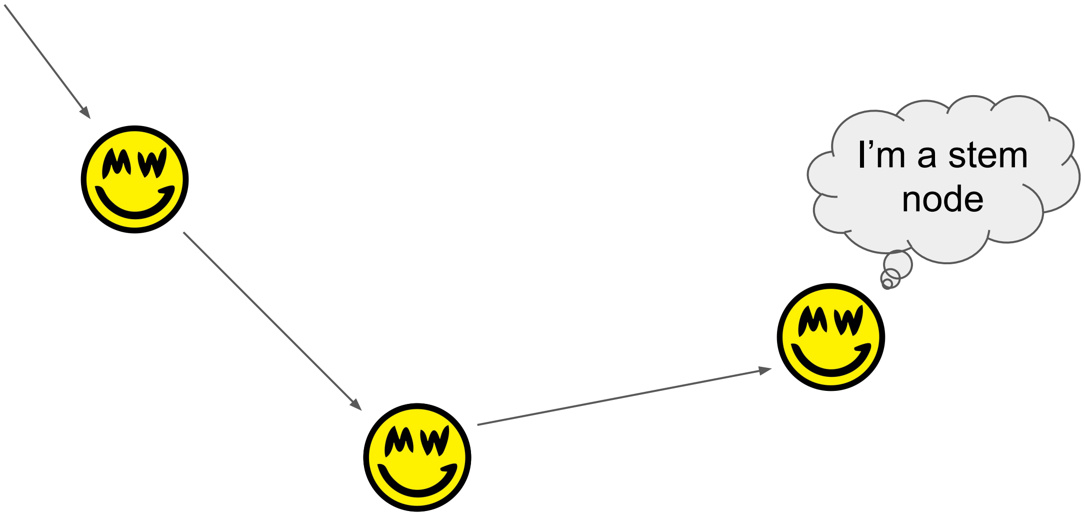
Dandelion++



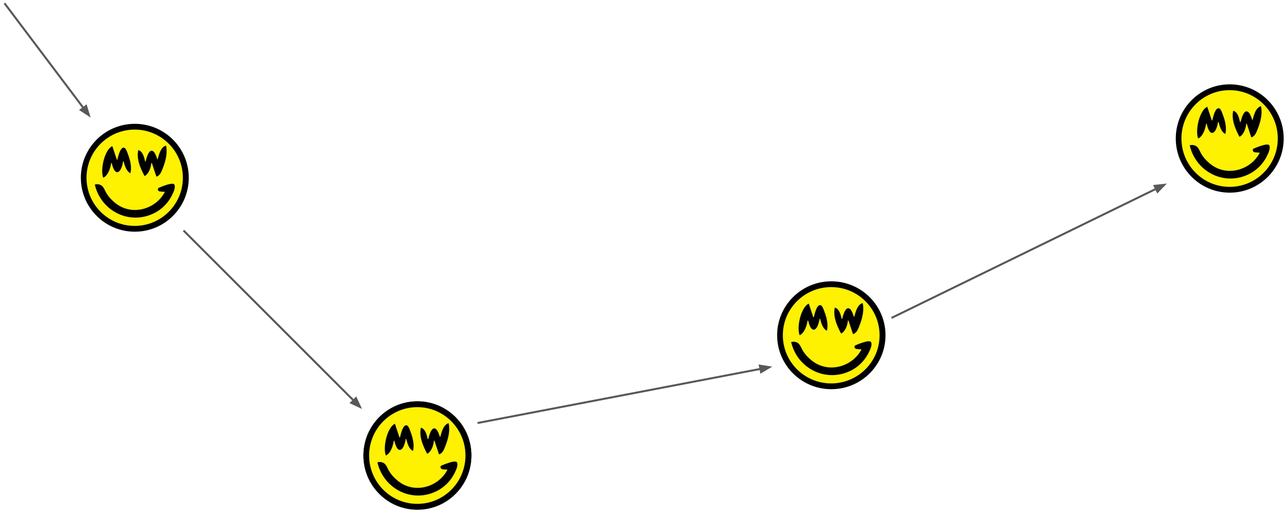
Dandelion++



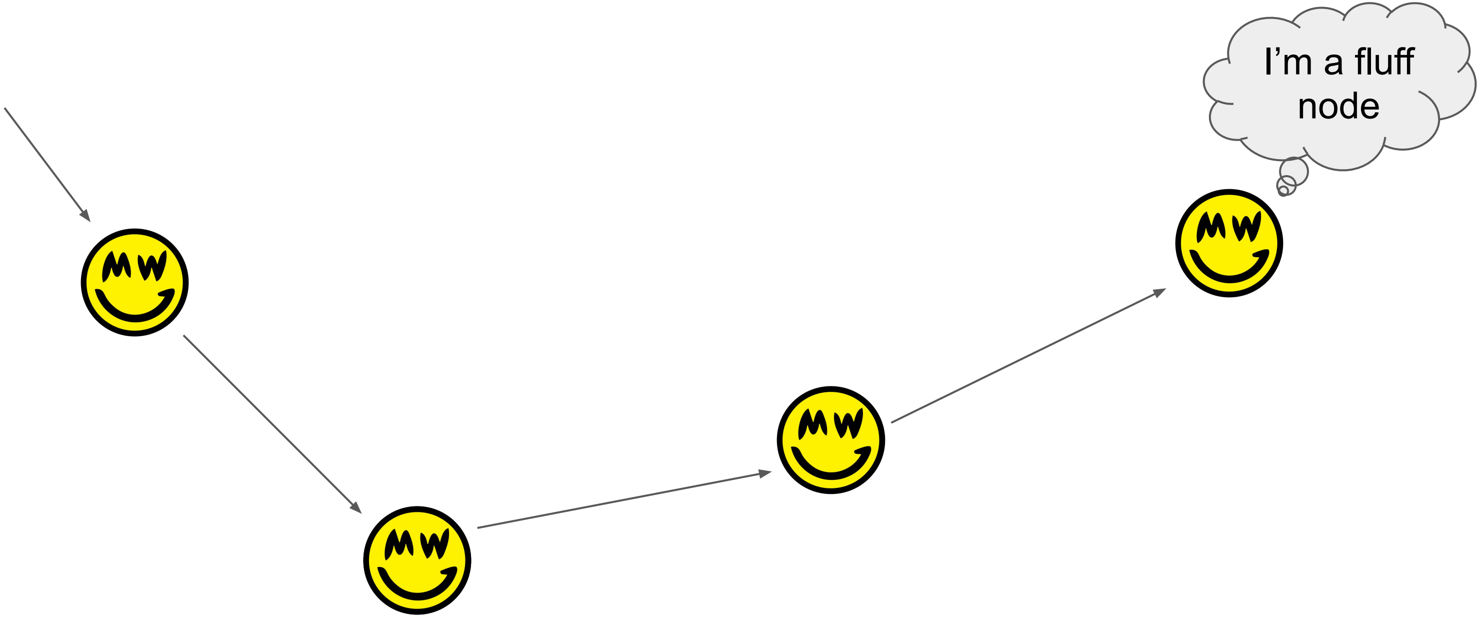
Dandelion++



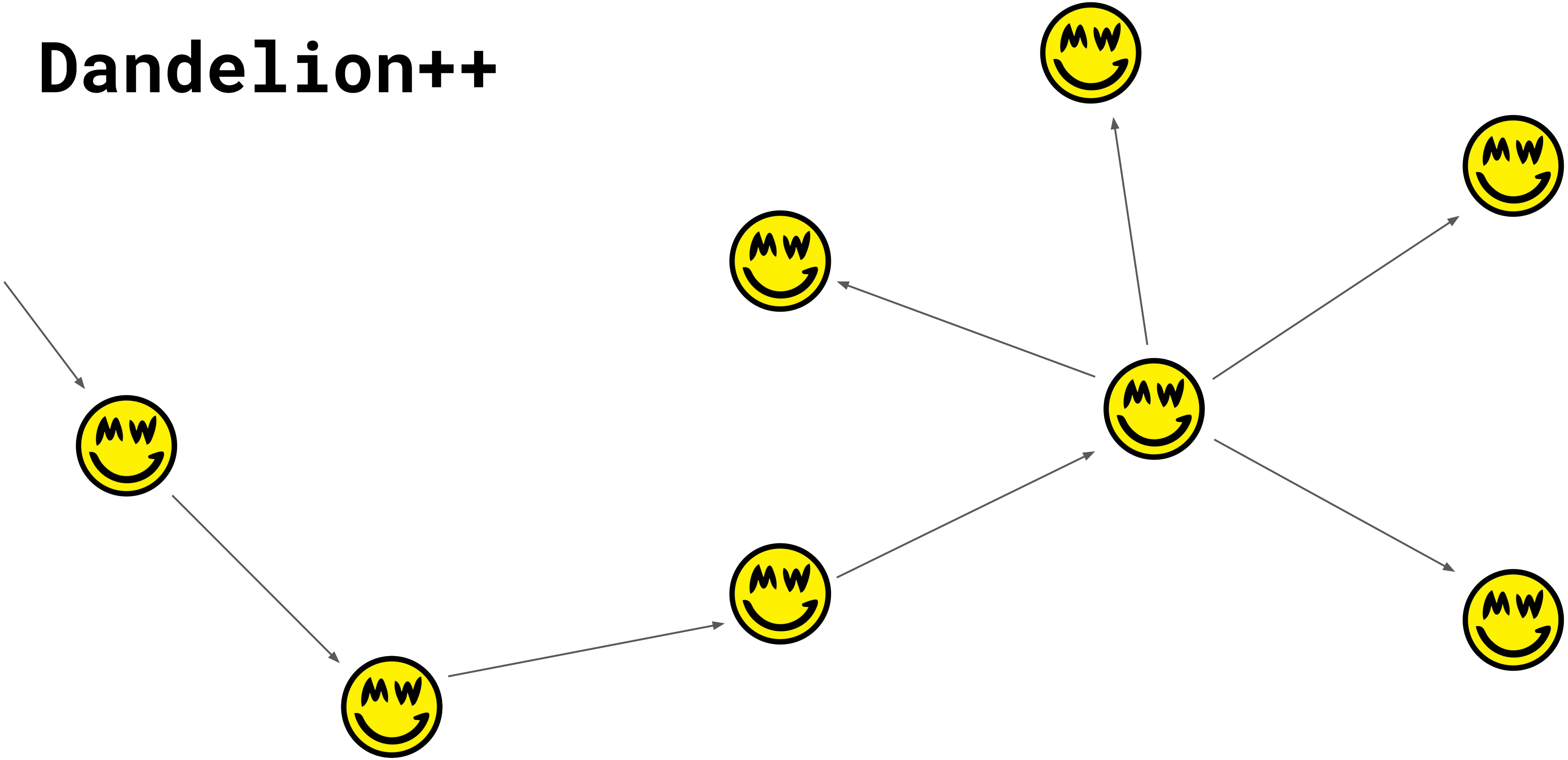
Dandelion++



Dandelion++



Dandelion++



Dandelion++

Overlay networks

I2P

Plan to integrate both at the p2p layer and wallet

WIP PR (p2p): mimblewimble/grin#2932

Tor

RFC proposal for online transacting via Tor

mimblewimble/grin-rfcs#24

How privacy

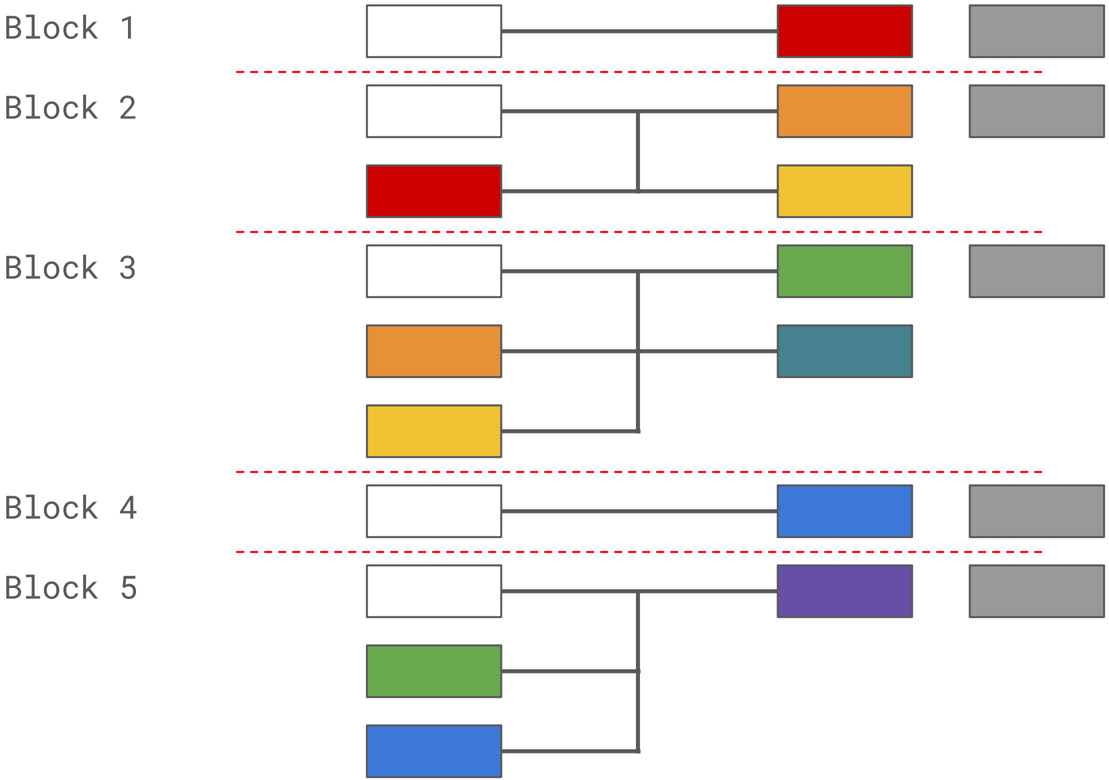
- Not 100% zero-knowledge like ZCash
- Transaction linkability is still an issue
- Keeps cryptographic assumptions to a minimum (no trusted setup or “moon math”)
- Hide in the crowd: piggybacks on network size

How scalability

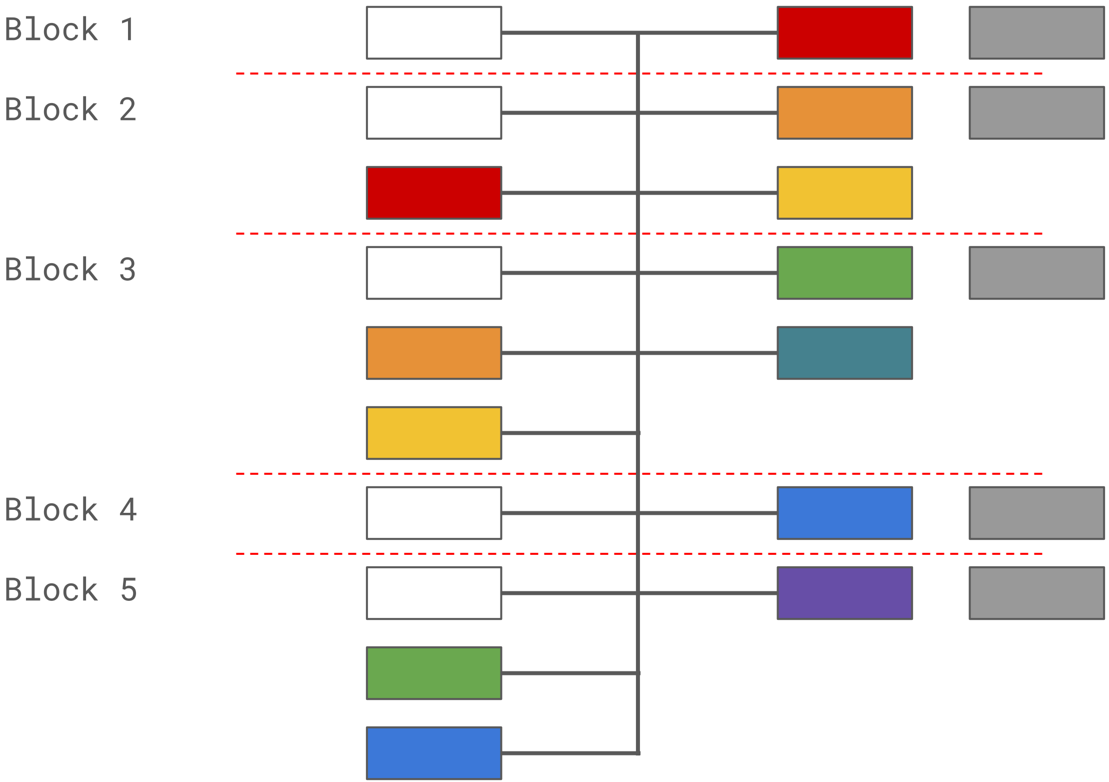
How scalability

- Spent TXO pruning
- Fast IBD

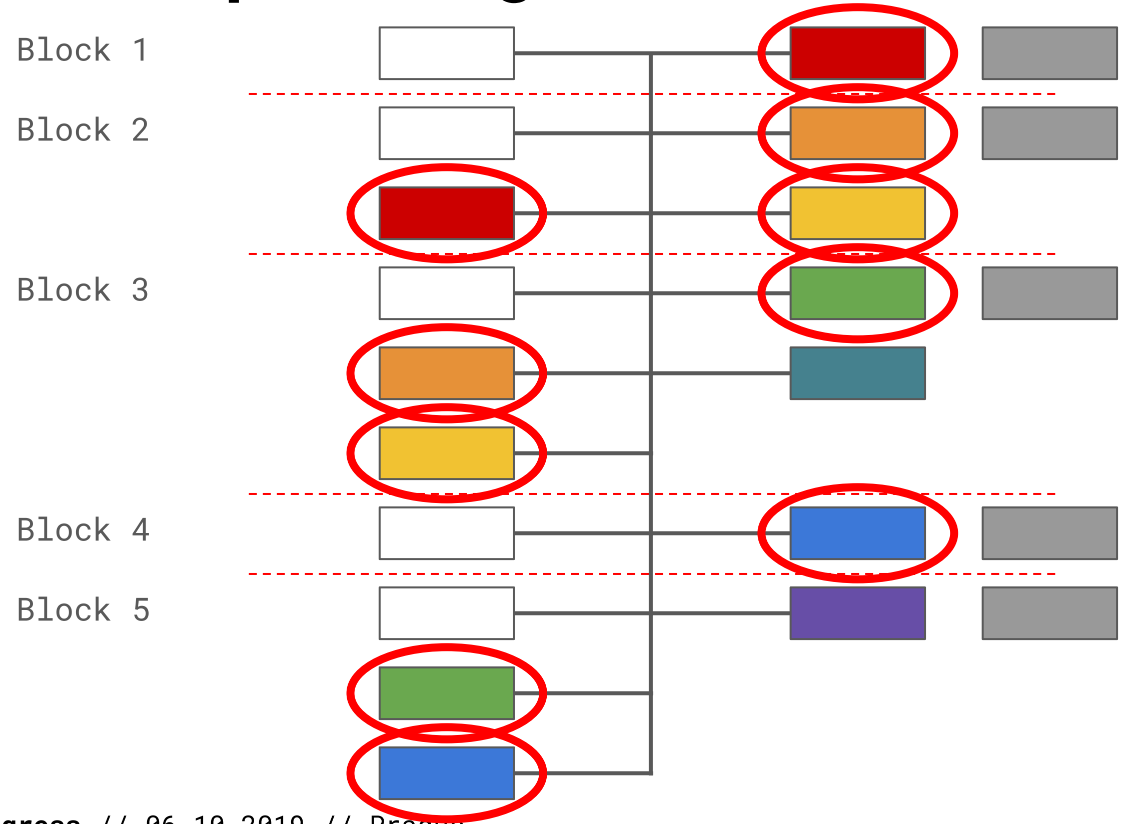
Spent TXO pruning



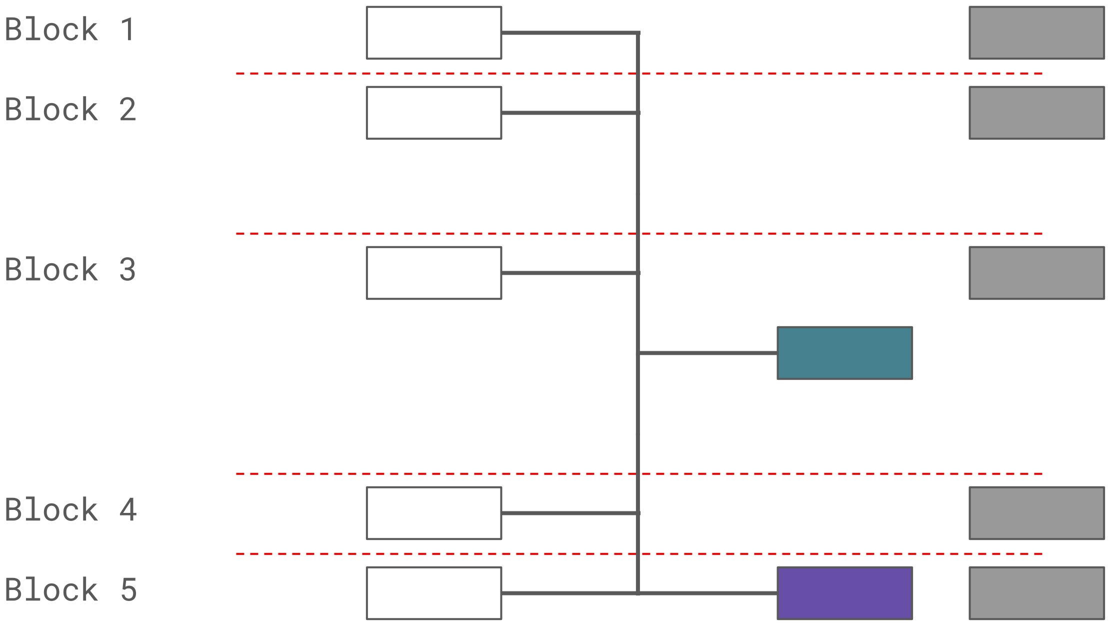
Spent TXO pruning



Spent TXO pruning



Spent TXO pruning



Spent TXO pruning

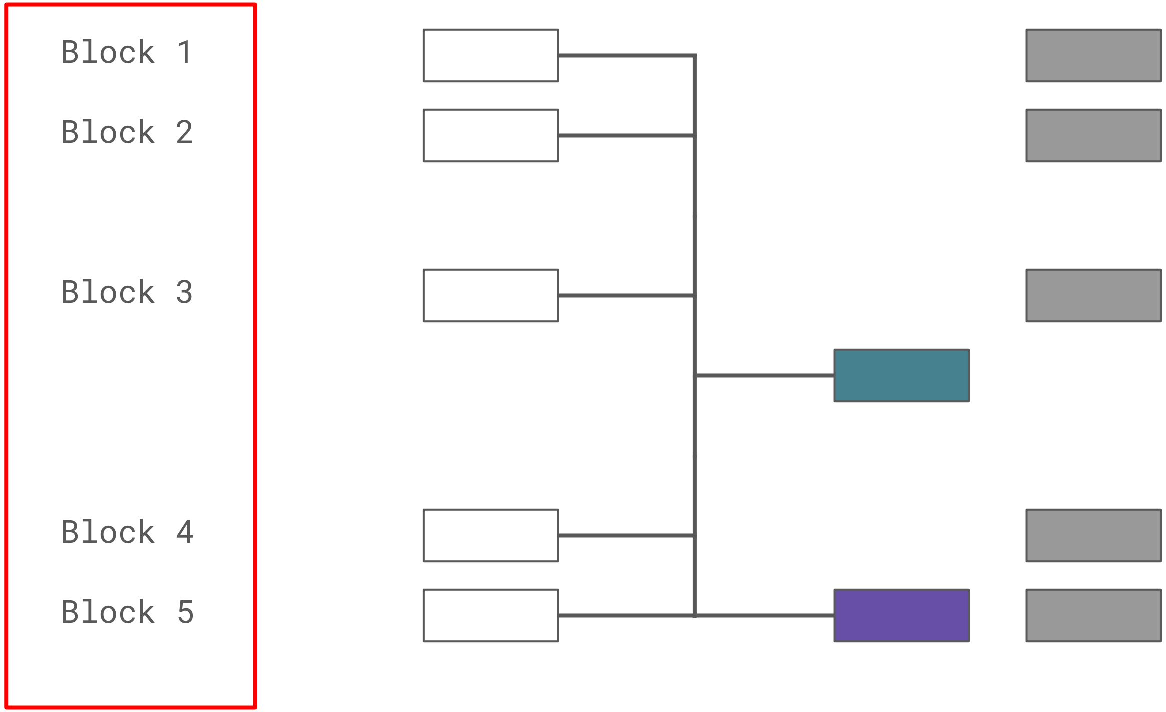
To put things into perspective, Bitcoin today has:

~235GB blockchain size (minus UTXO, minus headers, source: blockchain.com)

~3.4GB UTXO size (source: statoshi.info)

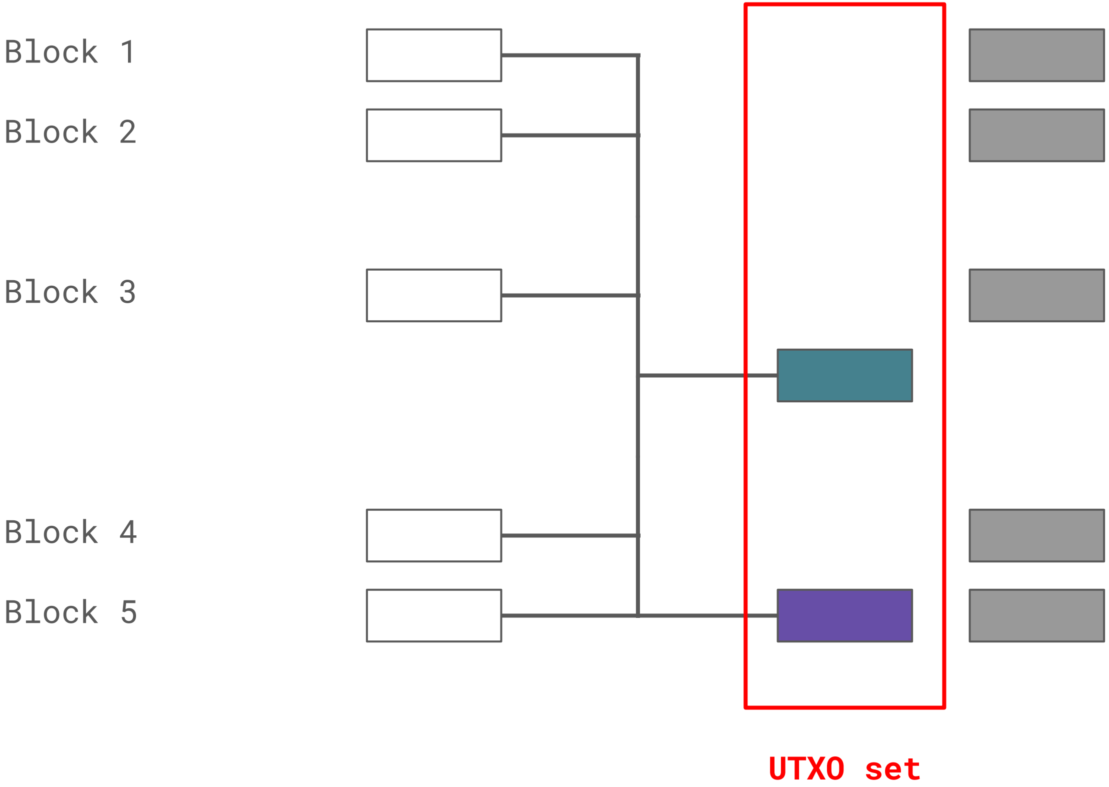
Still need to store all the kernels in Grin though...

Fast IBD



Block headers

Fast IBD



Block 1

Block 2

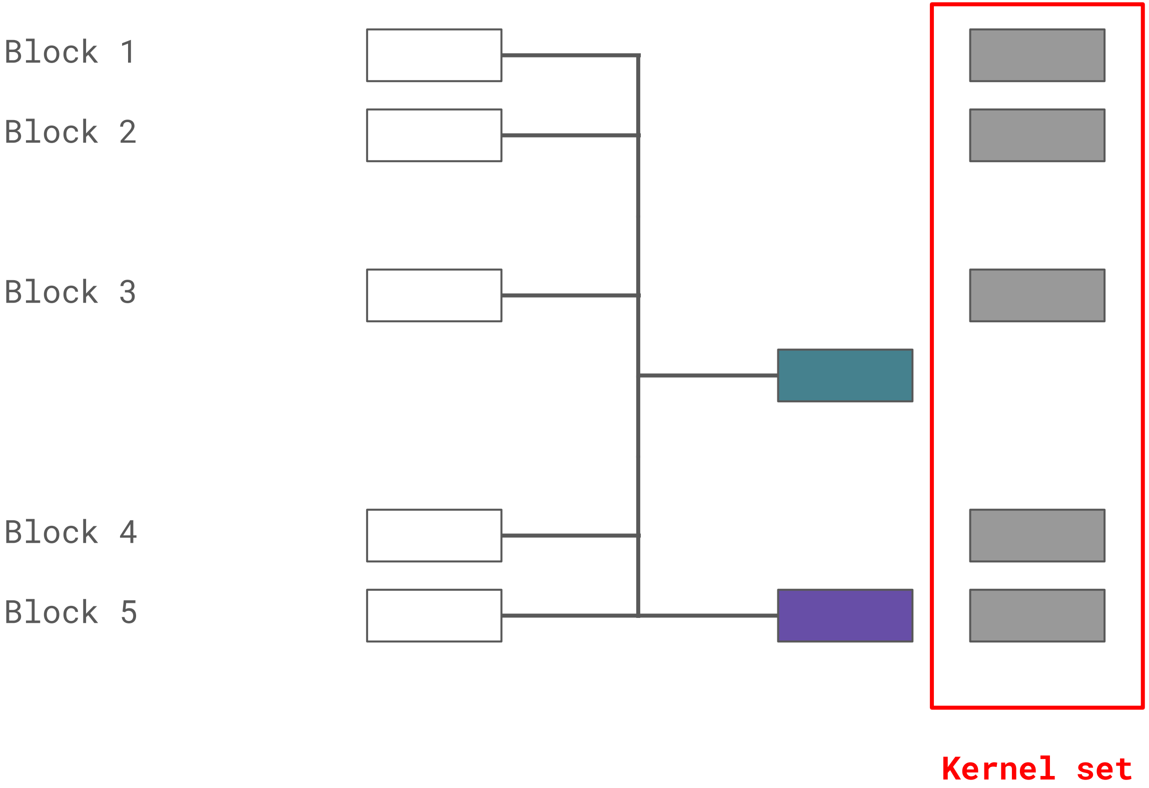
Block 3

Block 4

Block 5

UTXO set

Fast IBD



How scalability

- Not an order of magnitude better than Bitcoin in terms of transaction throughput
- Still need a second layer to scale to Visa-level speed
- Pruning helps a lot

How fairness

How fairness

- Fair launch
- Emission rate
- Proof of Work
- Governance

Fair launch

- **Announced October 20th, 2016 by “Ignotus Peverell**
- Open source, 100% community driven
- Funded solely by donations
- **Launched January 15th, 2019**
- No:
  - ICO
  - Founders’ reward
  - Premine
  - Airdrop
  - ...

Emission rate

1 grin/s forever.

- 60 grin constant coinbase reward / 1m block time
- Simple
- No advantage to early adopters

Proof of Work

Cuckoo Cycle family

- Two PoW algorithms
- One ASIC-resistant (90%) and one ASIC-friendly (10%)
- ASIC-resistant algorithm is phased out in 2 years (still 1+ year left)
- Open ASIC development encouraged (not easy)

Governance

- No foundation
- Technocratic council -> Subteams
- RFC process (mimblewimble/grin-rfcs)
- Public bi-weekly development and governance meetings

Get involved

Rust developers

Crypto researchers

Frontend developers

UI/UX specialists

Graphic designers

Technical writers

Community members

Don't ask for permission, the project is open source:

https://github.com/mimblewimble

Fund the project

A good way to protect your grins:

https://grin-tech.org/funding

Thank you!

github/keybase: @kargakis