Bitcoin Wednesday
05.12.2018 // Amsterdam

Mimblewimble / Grin

Jasper van der Maarel

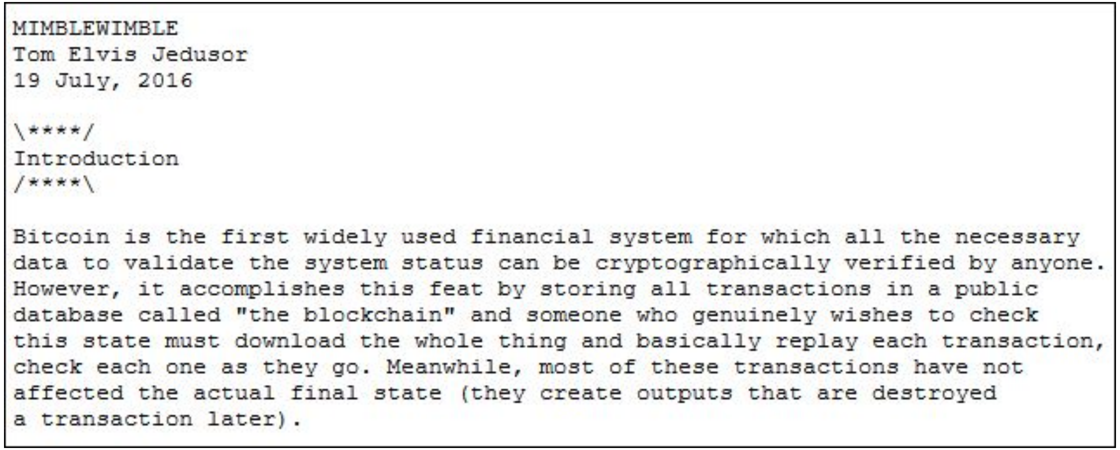
Contents

- What is MW ?
- What is Grin?
- Why is Grin?
- How is Grin?
- When is Grin?

What is Mimblewimble?

Mimblewimble

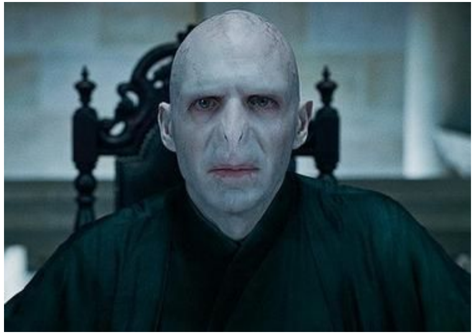
August 2nd, 2016: document by “Tom Elvis Jedusor”



MIMBLEWIMBLE
Tom Elvis Jedusor
19 July, 2016

****/
Introduction
/****\

Bitcoin is the first widely used financial system for which all the necessary data to validate the system status can be cryptographically verified by anyone. However, it accomplishes this feat by storing all transactions in a public database called "the blockchain" and someone who genuinely wishes to check this state must download the whole thing and basically replay each transaction, check each one as they go. Meanwhile, most of these transactions have not affected the actual final state (they create outputs that are destroyed a transaction later).



Mimblewimble

Proposal of new blockchain format

Bitcoin transaction:
- Inputs (spend old outputs)
- Outputs

Verification:
- Signatures on inputs
- Amounts add up

Mimblewimble

Pedersen Commitments: $C = xG + vH$

Confidential Transactions:

$$C_{out1} + C_{out2} - C_{in1} - C_{in2} - C_{in3} == 0$$

Mimblewimble

Pedersen Commitments: $C = xG + vH$

Confidential Transactions:

$$C_{out1} + C_{out2} - C_{in1} - C_{in2} - C_{in3} == 0$$

Key Mimblewimble insight: excess value

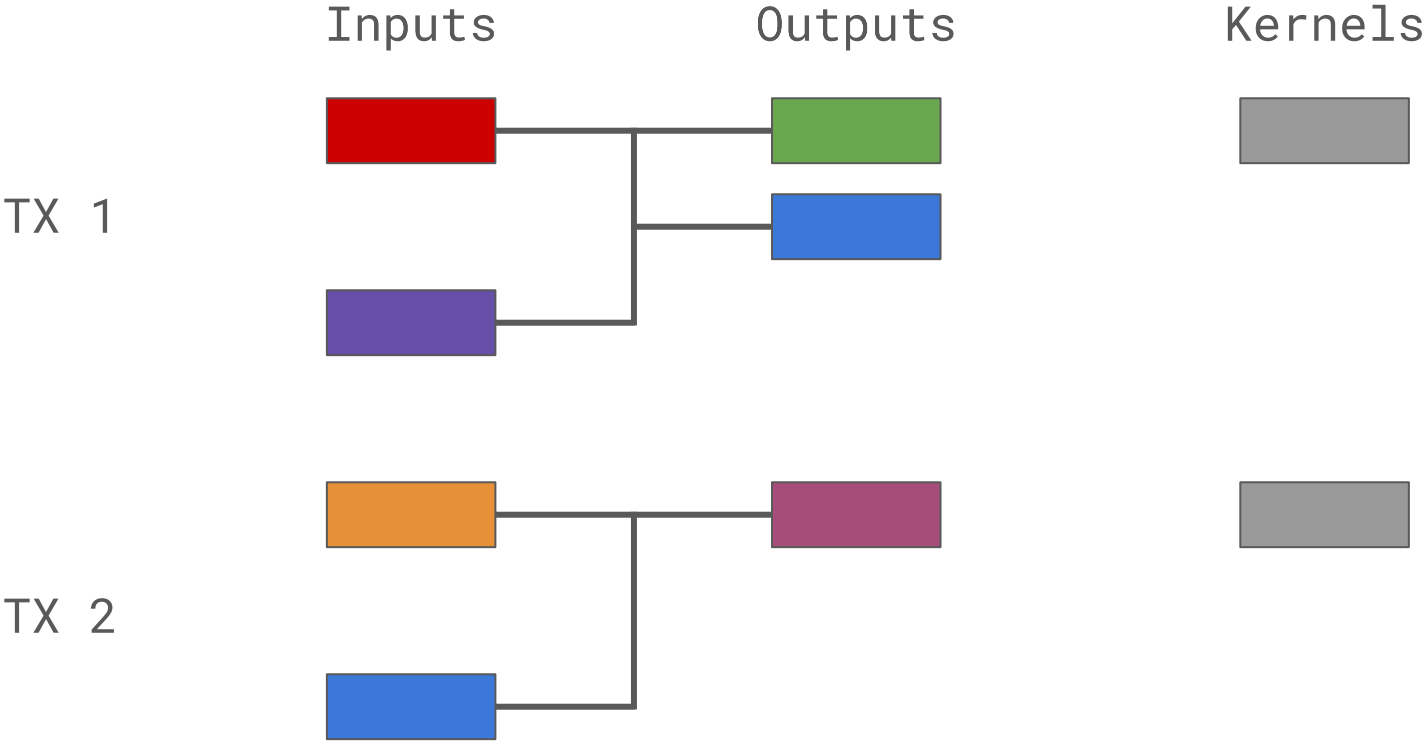
$$(\underset{\substack{\Uparrow\\ \boxed{\text{Recipient's blinding}}}}{113*G} + 3*H) - (\underset{\substack{\Uparrow\\ \boxed{\text{Sender's blinding}}}}{28*G} + 3*H) = \underset{\substack{\Uparrow\\ \boxed{\text{Excess}}}}{85*G} + 0*H$$

Mimblewimble transactions

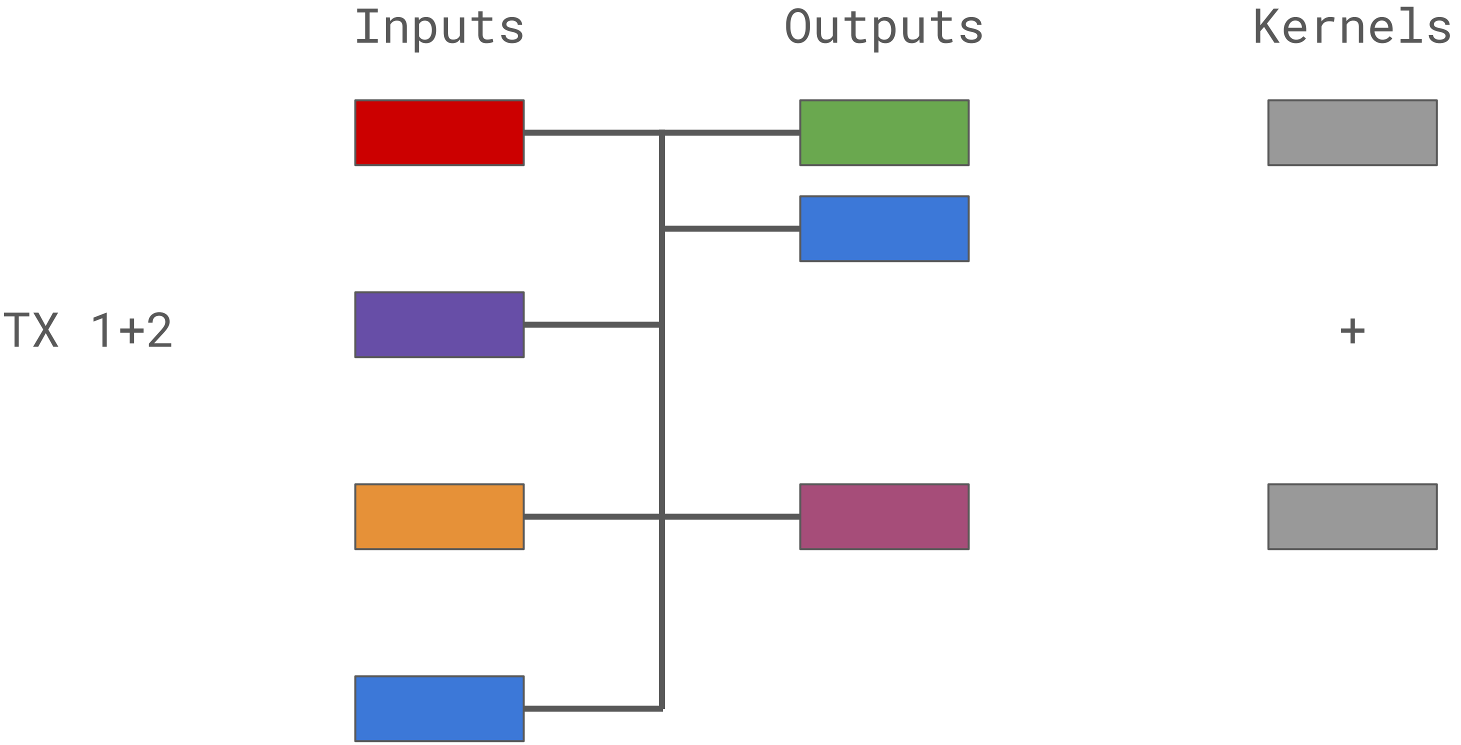
- Inputs: reference old unspent outputs
- Outputs: new commitments
- Kernels: excess and a signature

sum outputs - sum inputs == sum excess

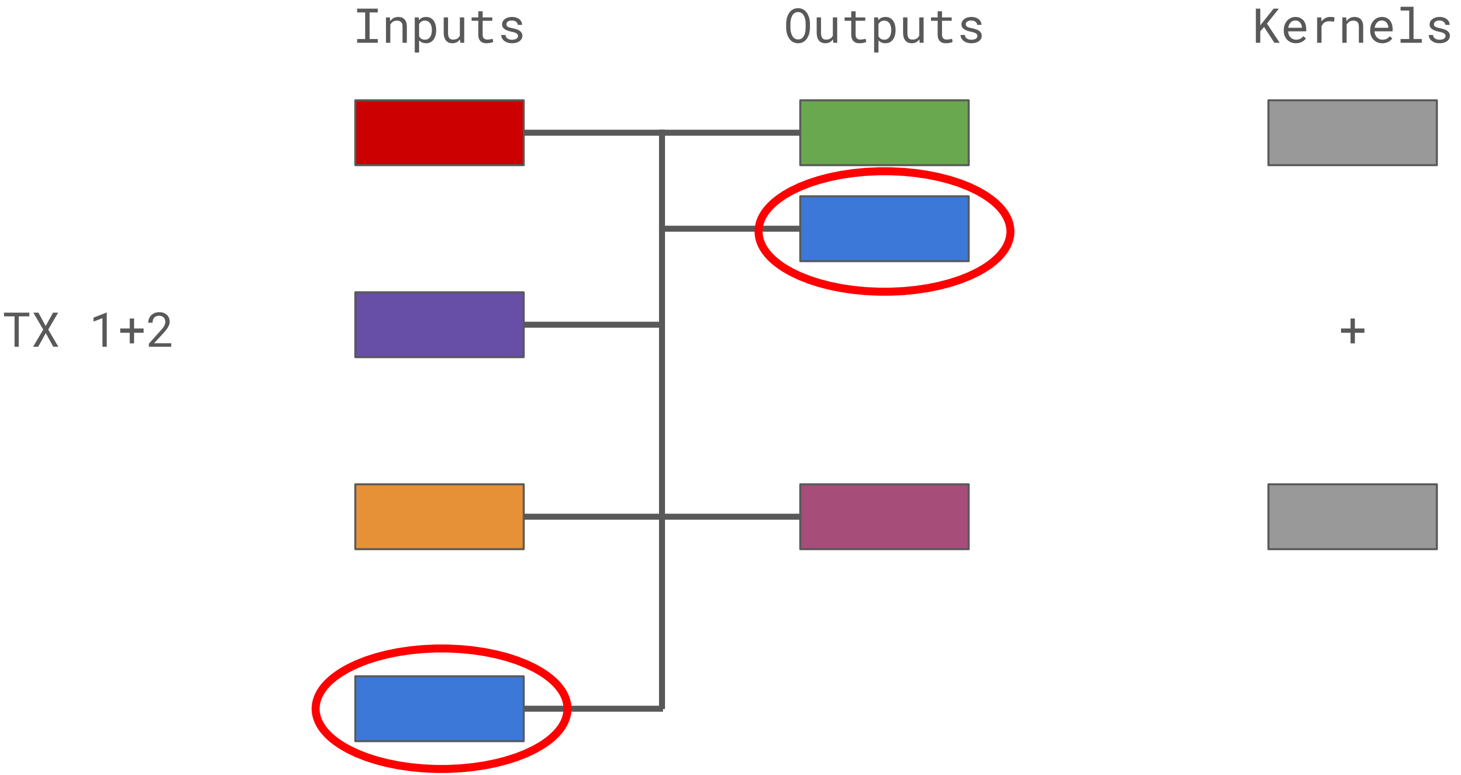
Mimblewimble transactions



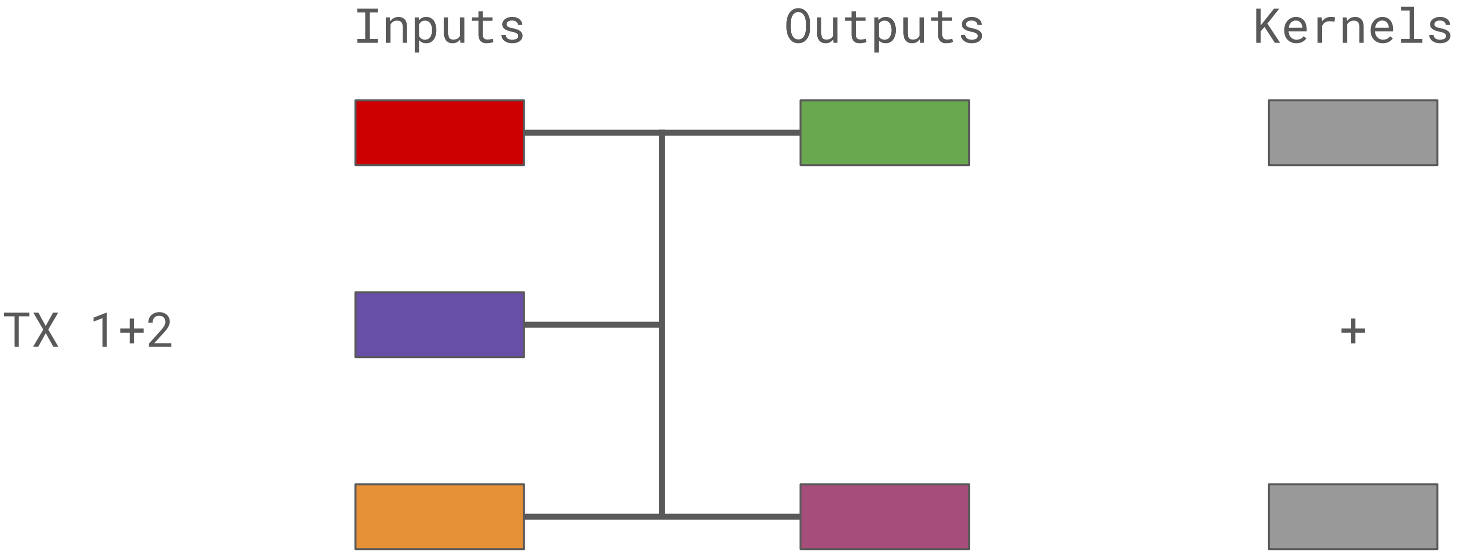
Mimblewimble transactions



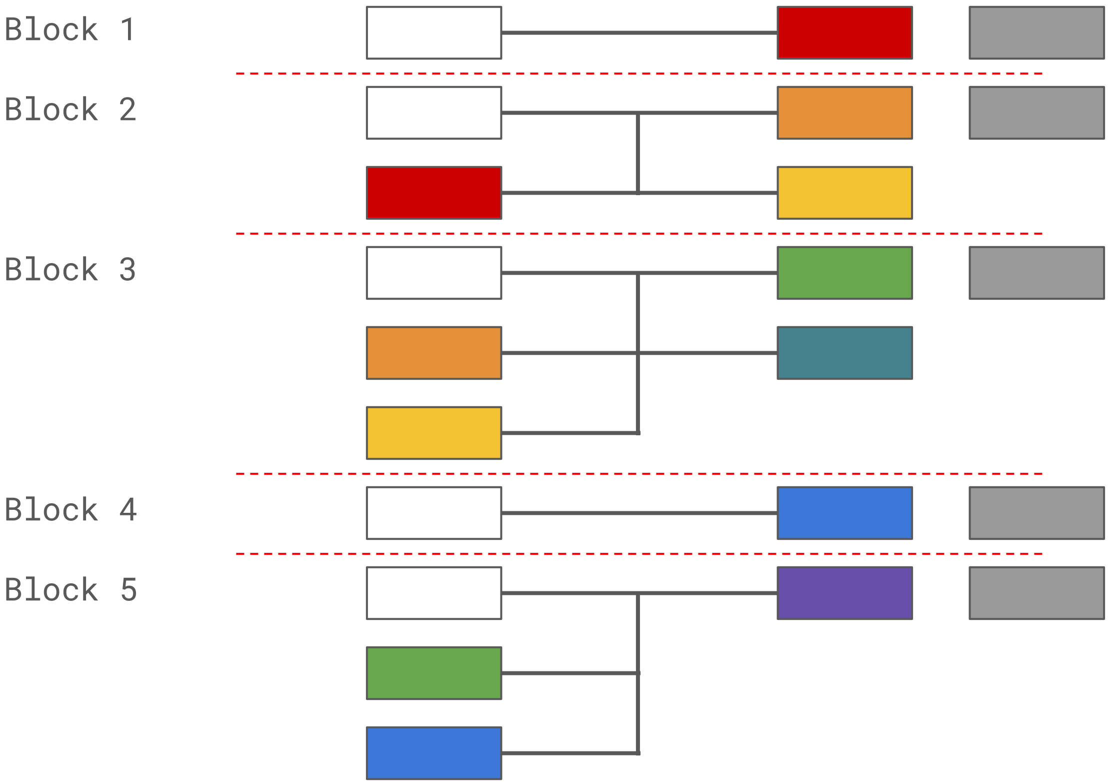
Mimblewimble transactions



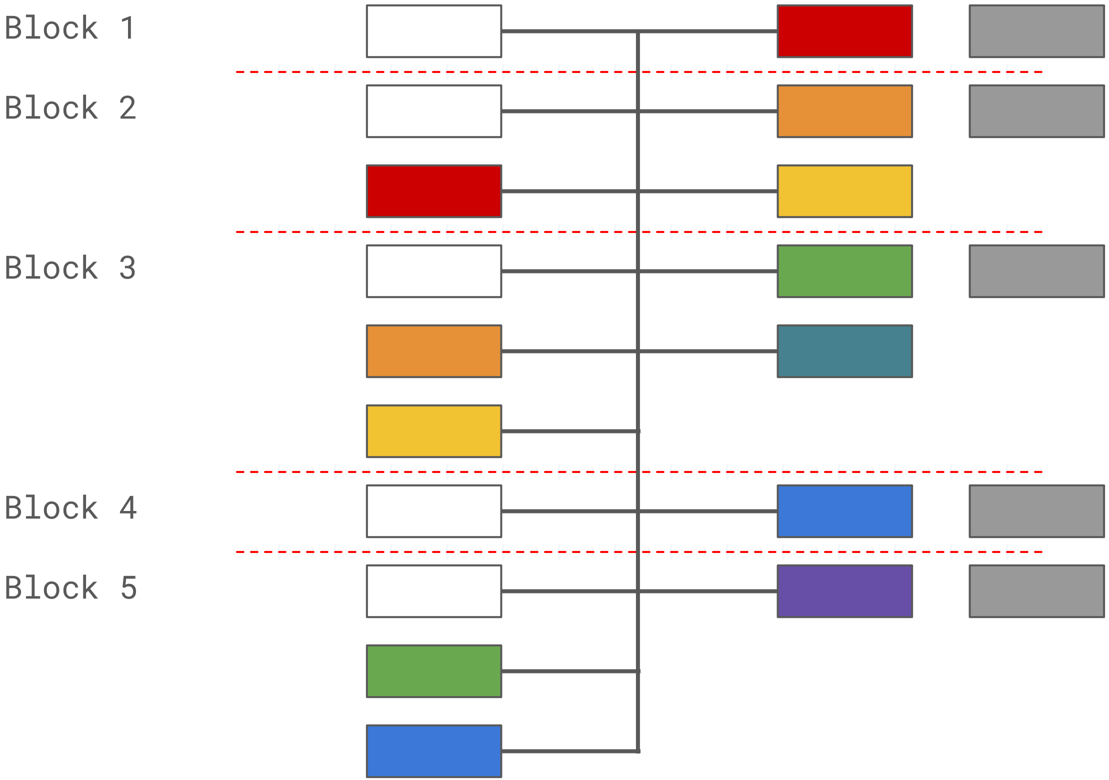
Mimblewimble transactions



Mimblewimble blockchain



Mimblewimble blockchain



Block 1

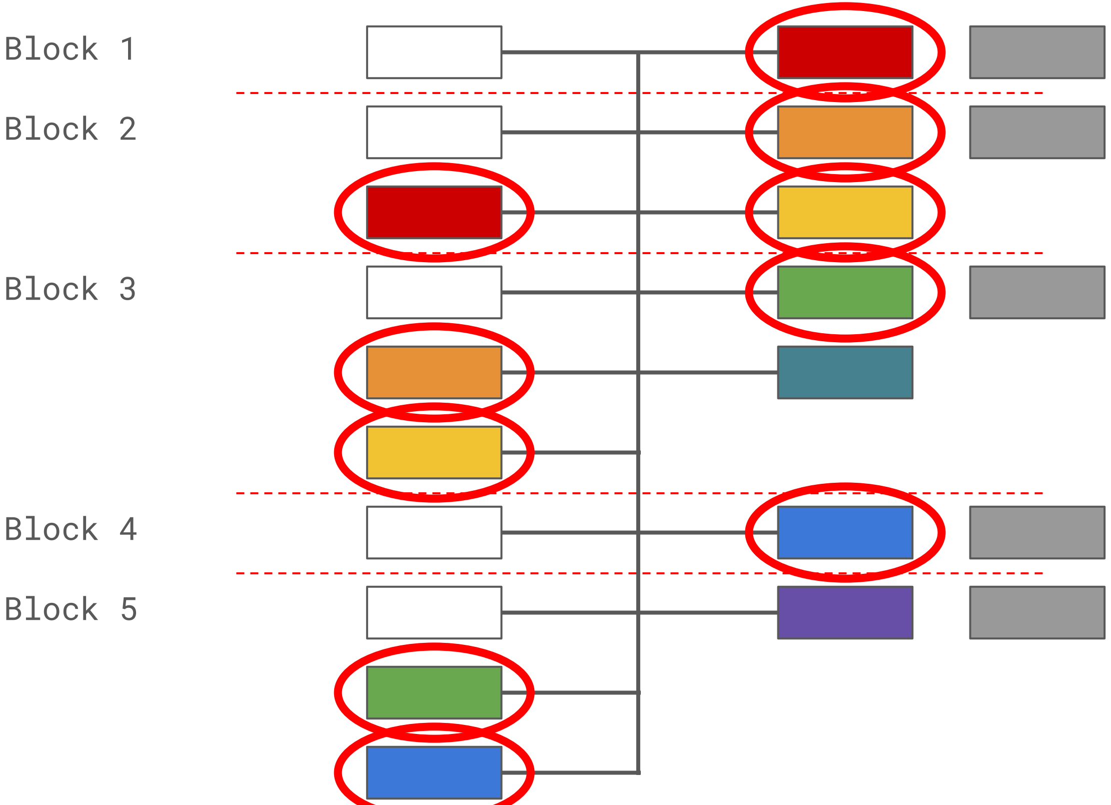
Block 2

Block 3

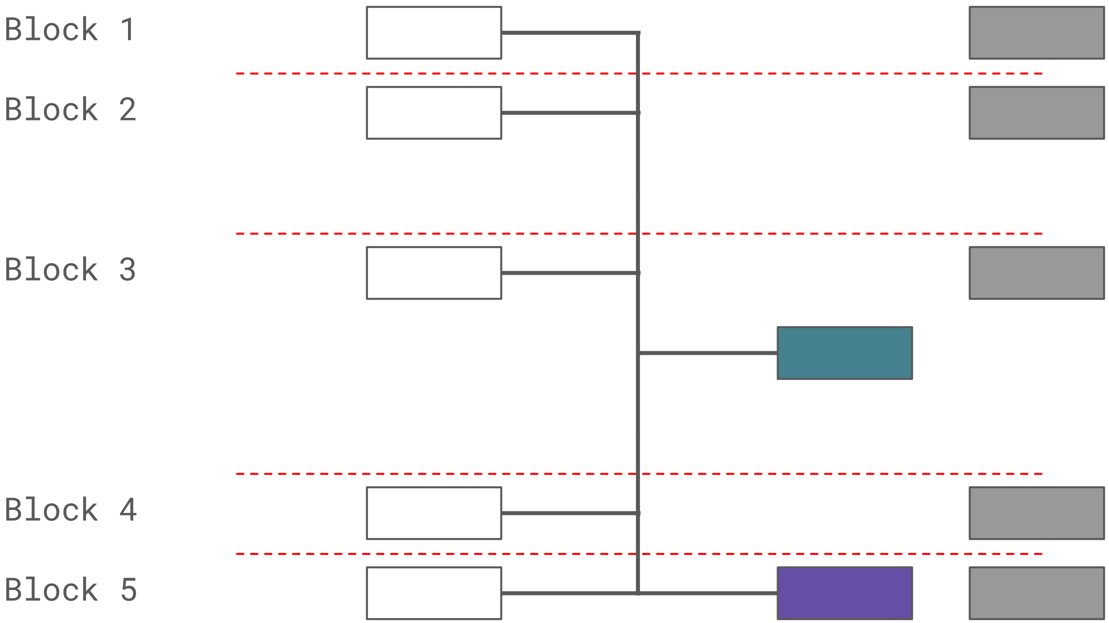
Block 4

Block 5

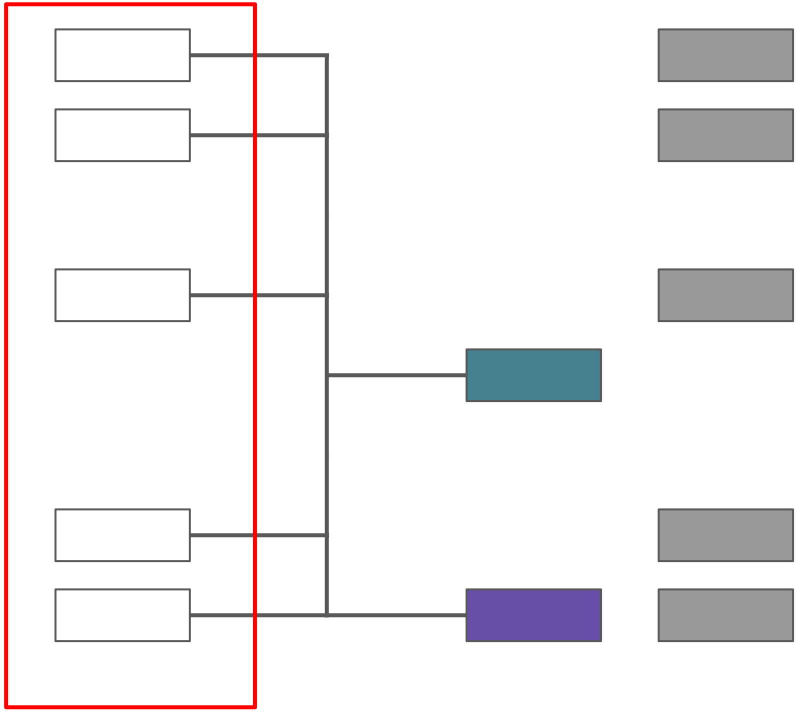
Mimblewimble blockchain



Mimblewimble blockchain

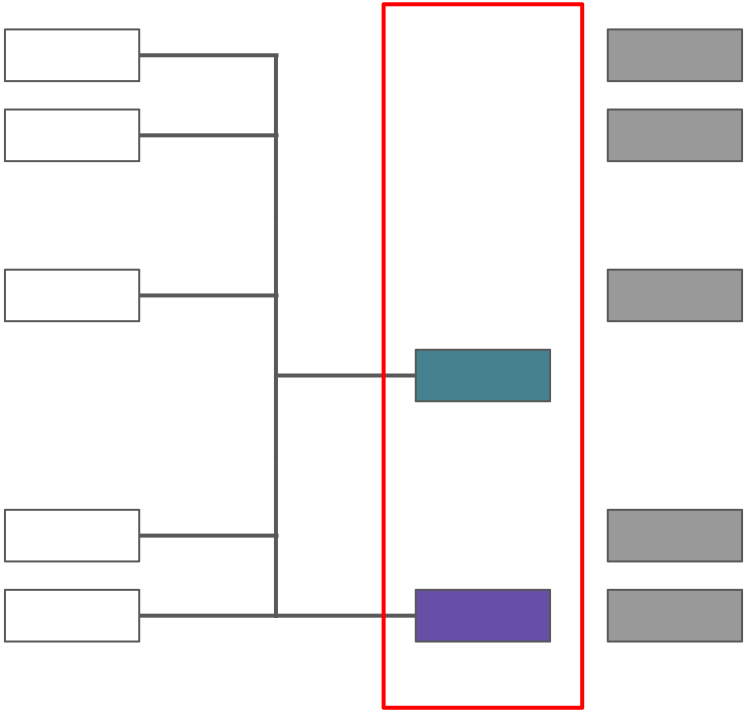


Initial sync



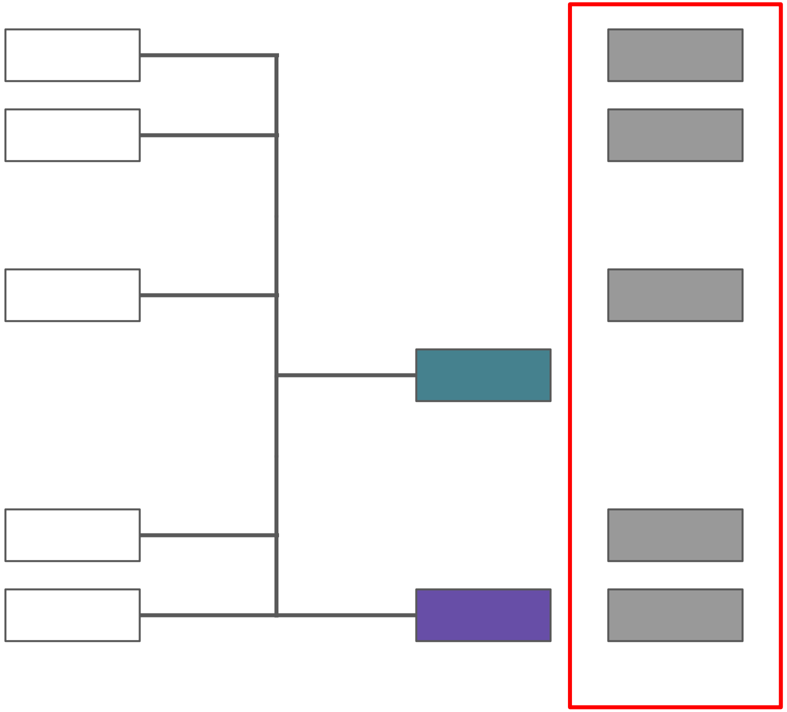
Block headers

Initial sync



UTXO set

Initial sync



Kernel set

Mimblewimble pros/cons

Pros:

+ No amounts
+ No addresses
+ Improved scaling

Mimblewimble pros/cons

Pros:

+ No amounts
+ No addresses
+ Improved scaling

Cons:

- No addresses: interactive transactions
- No scripting, but scriptless scripts

Grin

What is Grin?

October 20th, 2016: “Ignotus Peverell” announces Grin

First Mimblewimble implementation

Fully open source

Over time, more contributors joined

Built by the community

No: ICO, founder reward, premine, pre-allocation, pre...

Why is Grin?

MW tech is worth experimenting with

Bitcoin is very conservative

Sidechains are/were a mythical beast

Some MW-native concepts are impossible in Bitcoin

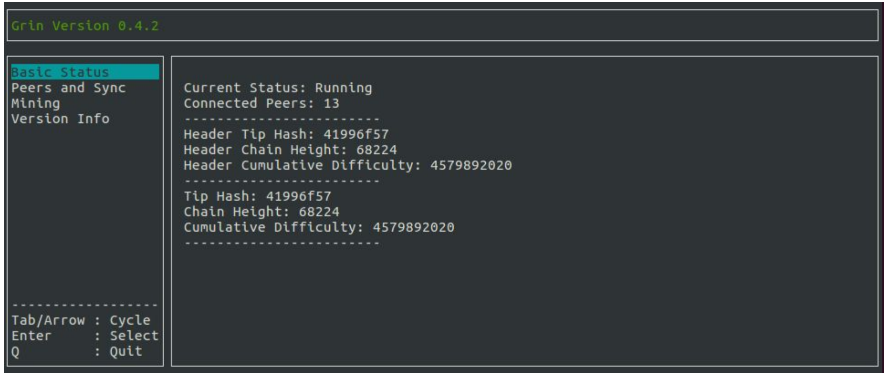
Can implement many state-of-the-art technologies

Technology

- Fully working MW chain
- Fast sync
- Transaction aggregation
- Bulletproofs
- Dandelion w/ aggregation
- Schnorr signatures
- Cuckoo-family PoW (ASIC resistant + ASIC friendly)
- Wallet supporting multiple transport methods
- Support for multisig
- Support for atomic swaps

Technology

Node

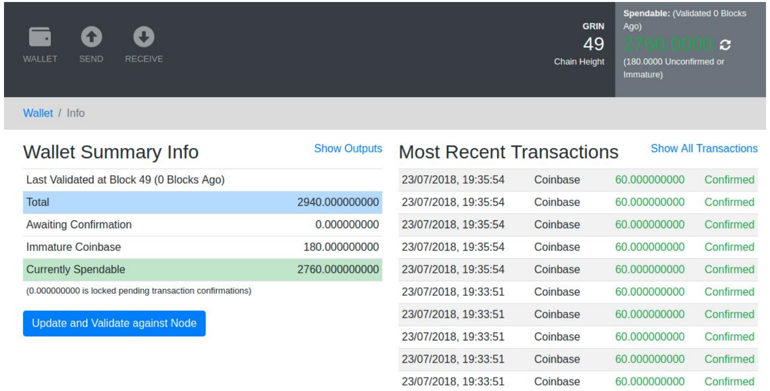


```
Grin Version 0.4.2

Basic Status        Current Status: Running
Peers and Sync      Connected Peers: 13
Mining              ------------------------
Version Info        Header Tip Hash: 41996f57
                    Header Chain Height: 68224
                    Header Cumulative Difficulty: 4579892020
                    ------------------------
                    Tip Hash: 41996f57
                    Chain Height: 68224
                    Cumulative Difficulty: 4579892020
                    ------------------------

-----------------
Tab/Arrow : Cycle
Enter     : Select
Q         : Quit
```

Web wallet



49
Chain Height

Spendable: (Validated 0 Blocks Ago)
2760.0000
(180.0000 Unconfirmed or Immature)

Wallet / Info

Wallet Summary Info

Show Outputs

Last Validated at Block 49 (0 Blocks Ago)	
Total	2940.000000000
Awaiting Confirmation	0.000000000
Immature Coinbase	180.000000000
Currently Spendable	2760.000000000

(0.000000000 is locked pending transaction confirmations)

Update and Validate against Node

Most Recent Transactions

Show All Transactions

23/07/2018, 19:35:54	Coinbase	60.000000000	Confirmed
23/07/2018, 19:35:54	Coinbase	60.000000000	Confirmed
23/07/2018, 19:35:54	Coinbase	60.000000000	Confirmed
23/07/2018, 19:35:54	Coinbase	60.000000000	Confirmed
23/07/2018, 19:35:54	Coinbase	60.000000000	Confirmed
23/07/2018, 19:33:51	Coinbase	60.000000000	Confirmed
23/07/2018, 19:33:51	Coinbase	60.000000000	Confirmed
23/07/2018, 19:33:51	Coinbase	60.000000000	Confirmed
23/07/2018, 19:33:51	Coinbase	60.000000000	Confirmed
23/07/2018, 19:33:51	Coinbase	60.000000000	Confirmed

More wallets in development, including at least 2 for mobile

When is Grin?

~January 15th, 2019

Just another step in development process

Grin is far from finished!

Many more future improvements possible

FlyClient, BLS, RSA accumulators, CA, LN ...

Participate in Grin (community)

- **Anyone** : download software, play with it, use it!
- **Anyone** : join gitter grin lobby, grin-forum.org, community subreddit, Telegram, Discords etc.
- **Miners** : grin-miner on Github
- **Designers**: join gitter grin/design
- **Devs** : look at open issues, join gitter grin/dev

https://github.com/mimblewimble/grin

https://grin-tech.org

Questions?

Github/gitter: jaspervdm
Twitter: @jaspervdmaarel