Mimblewimble & Grin

privacy by default

@i1skn

What would be in this talk?

- Mimblewimble (MW)
- Grin as an implementation of MW
- Monetary policy
- Mining
- Where is Grin now
- How to get involved

A short history MW

- 2 Aug 2016, an anonymous person using the name **Tom Elvis Jedusor** dropped a document onto a Bitcoin research IRC channel called MimbleWimble.

- 6 Oct 2016, **Andrew Poelstra** published revised document of **MimbleWimble**.

- 20 Oct 2016, an anonymous person using the name **Ignotus Peverell** published the first commit in github.com/mimblewimble/grin repository.

What is MW?

- Complete fungibility
- Scales mostly with number of users, not transactions.
- Elliptic Curve Cryptography
- Interactive TX building

Confidentail Transactions

- Alice wants to send N grin to Bob
- Alice take her **unspent output** and create a new one for Bob
- To do that, Alice needs Bob to cooperate
- After output was created:
    - It is **impossible** to distinguish this output from others
    - It is **impossible** to find matching input for this output
    - It is **impossible** to observe the amount in this output

Scalability

1.Check that now new coins were created in the block does not require a history of transactions

2. Node needs only a few full blocks with full guarantee

Cut through

1. Alice sends 10 grins to Bob

2. Bob sends 10 grins to Carol

3. Do weed need to know, that Bob was involved?

Alice → Bob, Bob → Carol <=> Alice → Carol

4. Outputs, created and spent in the same block can be eliminated

Grin as an implementation of MW

- Implemented in Rust
- Bulletproofs
- Fast-sync by default
- Dandelion

More technical talk by @yeastplume at Grincon0 https://youtu.be/11Li5Zy2cKk

Short FAQ

- No ICO
- No ‘Founders reward’
- No Premine
- No Pre-allocation

Dandelion

- Network layer anonymity solution that was originally proposed in 2017 to help improve on Bitcoin's P2P network privacy
- Purpose: hide who created the transaction
- Amazing talk by @quentinlesceller from Grincon0 - https://youtu.be/Q1XWFcHiwQA

Monetary policy

- Block reward is **fixed over time** - 60 Grin
- Supply is **unlimited**
- Fee is proportional to number of outputs and back-proportional to number of inputs

⛏ Mining ⛏

- Two algorithms (*ASICS Friendly, ASICS Resistant*)
- Day 1 - **10%** goes to ASICS **Friendly**
- In 2 years - **100%** goes to ASICS **Friendly**
- **ASICS Resistant** Mining on GPU is memory heavy (7Gb+)
- OpenCL implementation still in progress

For more details @tromp talk at Grincon0 https://youtu.be/CLiKX0nOsHE

Where is Grin now?

- **2,6k** ★, 85 contributors on Github
- Today - Floonet, **15 January - Mainnet**
- **1.3k** people in gitter

Get involved

- Know some Rust? https://github.com/mimblewimble/grin
- Design/UX skills? https://gitter.im/grin_community/design
- Frontend dev? Web wallet needs some love
- Mobile dev? iOS/Android is still in development
- Know how to write? Documentation!1!!1!1!!1!
- Very smart? Confidential assets currently is not available
- Other? https://gitter.im/grin_community/Lobby

Thanks

- **The** document - https://github.com/mimblewimble/grin/blob/master/doc/intro.md
- Videos from Grincon0 - https://grincon.info/
- Gitter - https://gitter.im/grin_community/Lobby
- Forum - https://www.grin-forum.org
- My Gitter/Twitter/Telegram: @i1skn