

Second year review

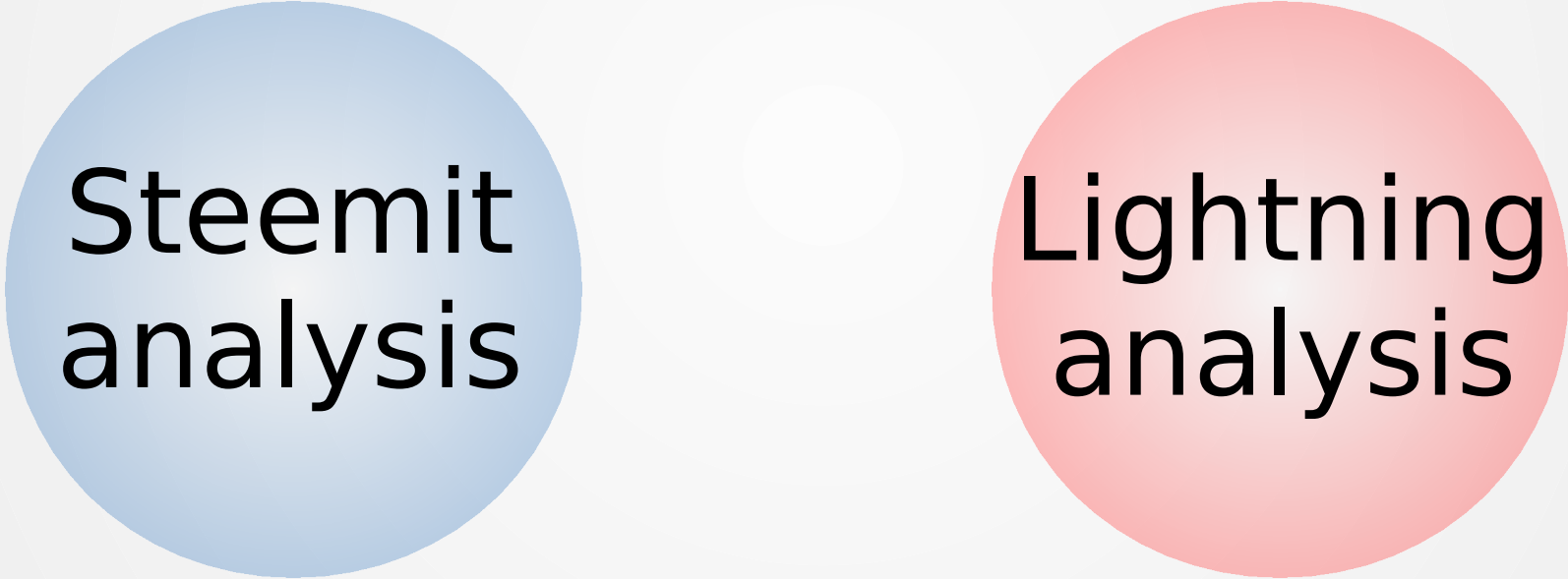
PhD student for Cryptography and Blockchains

Orfeas Stefanos
Thyfronitis Litos

Edinburgh University
5/6/2019



Past year



Steemit
analysis

Lightning
analysis



A Puff of Steem

- Steemit
 - Social media platform
 - Lives on Steem blockchain



A Puff of Steem

- Steemit
 - Social media platform
 - Lives on Steem blockchain
 - Posting & Voting
 - Voted creators gain \$\$
 - Trend-setting voters gain \$\$
 - Decentralised content curation



Player

- Voting power $\in [0, 1]$
 - Vote - \downarrow
 - Wait - \uparrow
- Coins > 0



Vote count

- Vote scaled, weighted by coins
- Voting power reduced



Vote count

- Vote scaled, weighted by coins
- Voting power reduced

$$i = a \cdot VP \cdot w + b$$
$$\text{score}' = \text{score} + i \cdot SP$$
$$VP' = VP - i$$



Our model

- System of ITMs
 - Input: post list, params
 - Output: reordered post list
- Player ITMs vote best of top n posts, list reordered – m rounds
- Output compared to ideal list



Our results

- “When is curated = ideal guaranteed?”
answered analytically
 - Steemit params → Up to 70 posts
- “How do collusions influence order?”
answered with simulation
 - A single selfish player ruins order

Blockchains are slow

- High latency ($\sim 3\text{min}$)
- Low throughput ($< 30 \text{ tx/s}$)

Blockchains are slow

- High latency ($\sim 3\text{min}$)
- Low throughput ($< 30\text{ tx/s}$)

Why?

- All nodes handle all transactions!

Solution:

- Do most txs off-chain
- Resolve disputes on-chain

Solution:

- Do most txs off-chain
- Resolve disputes on-chain

Names:

- Layer 2
- Payment Networks
- Payment Channels
- State Channels
- ...

Lightning Network



- Protocol specification for Bitcoin¹
- Contains BTC worth ~\$8,600,000²
- Beta implementation

¹<https://github.com/lightningnetwork/lightning-rfc/>

²<https://1ml.com/statistics>

Lightning Network Security



- UC framework
- We define $\mathcal{F}_{\text{PayNet}}$
- We “implement” LN in pseudocode: Π_{LN}
- We prove Π_{LN} UC-realizes $\mathcal{F}_{\text{PayNet}}$
- Concrete security

Decentralised markets

I planned to define a “market” functionality, but needed more:

- Game Theory
- Economics

Future projects

- $\mathcal{G}_{\text{ledger}}$ simplification
- Virtual Payment Channels for Bitcoin
- New PCN-enabled blockchain
- Privacy & Payment Networks
- Steemit on channels
- Content Curation classification
- Dec. Content Curation with ML

Future projects

- $\mathcal{G}_{\text{ledger}}$ simplification
- Virtual Payment Channels for Bitcoin
- New PCN-enabled blockchain
- Privacy & Payment Networks
- Steemit on channels
- Content Curation classification
- Dec. Content Curation with ML

Q&A