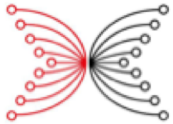


INPUT | OUTPUT

Lancaster University

A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence

Bingsheng Zhang

Lancaster University, UK & IOHK

Joint work with Roman Oliynykov (IOHK) and Hamed Balogun (Lancaster University)

25/02/2019 @ NDSS 2019

What is a treasury system?

Lancaster University

Who funds a cryptocurrency development/maintenance?

What is a treasury system?

Lancaster University

Patron organization donations

Initial Coin Offering (ICO)

Problem:
Lack of Sustainability

What is a treasury system?

Lancaster University

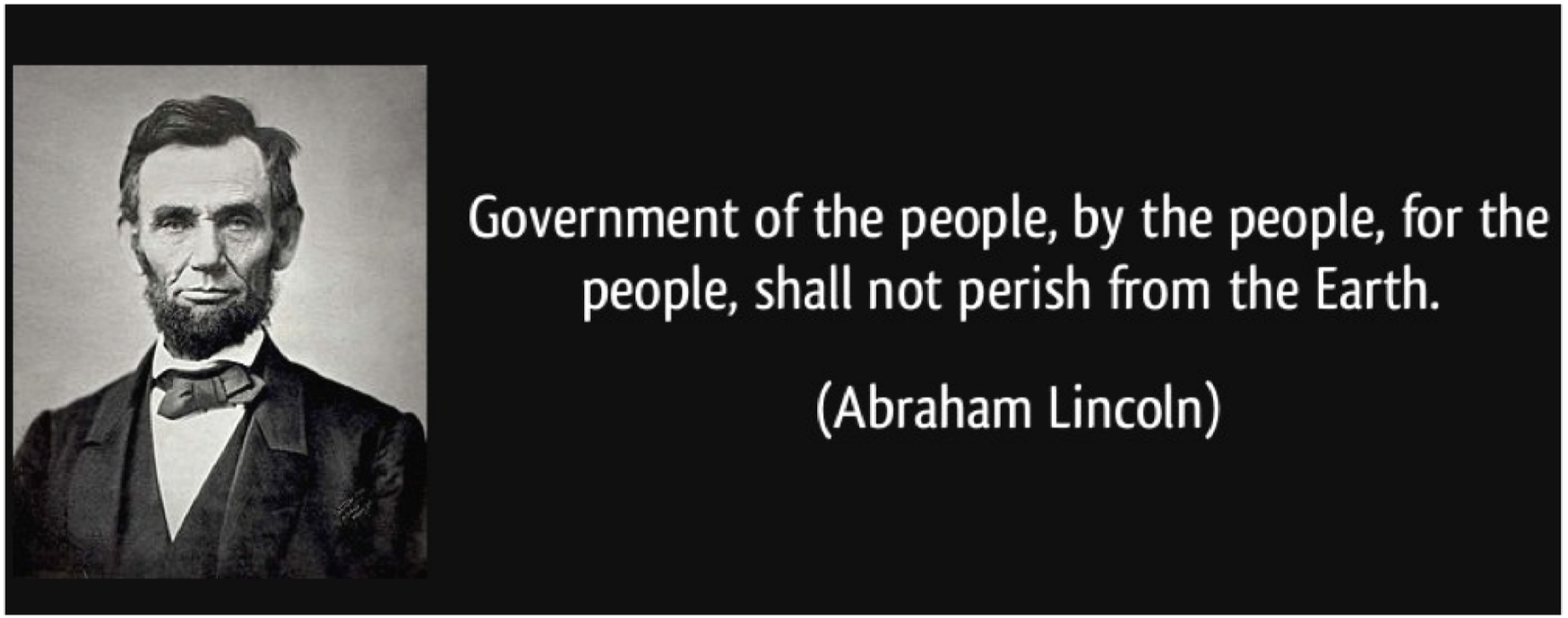
Alternatively:

Hair-cut/Tax of Block rewards



Who decides how the funds will be used?

Decision making



Who are the people?

Decision making

- What are the people?
  - Stakeholders
  - Anyone else? Developers? Researchers?

What is a treasury system?

Lancaster University

Treasury sources

Lancaster University

Mint coins

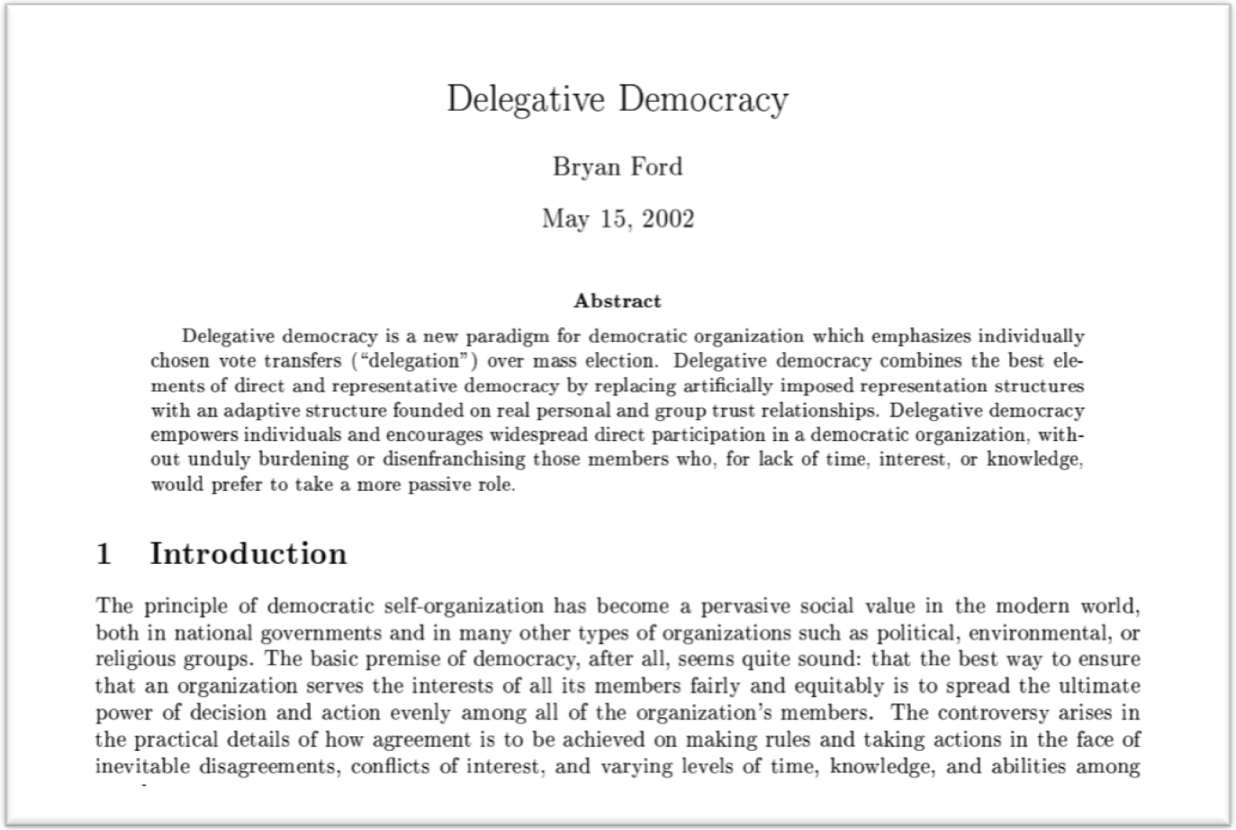
Taxation

Donation

Supporting liquid democracy

Lancaster University

- What is liquid democracy?



Delegative Democracy

Bryan Ford

May 15, 2002

Abstract

Delegative democracy is a new paradigm for democratic organization which emphasizes individually chosen vote transfers ("delegation") over mass election. Delegative democracy combines the best elements of direct and representative democracy by replacing artificially imposed representation structures with an adaptive structure founded on real personal and group trust relationships. Delegative democracy empowers individuals and encourages widespread direct participation in a democratic organization, without unduly burdening or disenfranchising those members who, for lack of time, interest, or knowledge, would prefer to take a more passive role.

1 Introduction

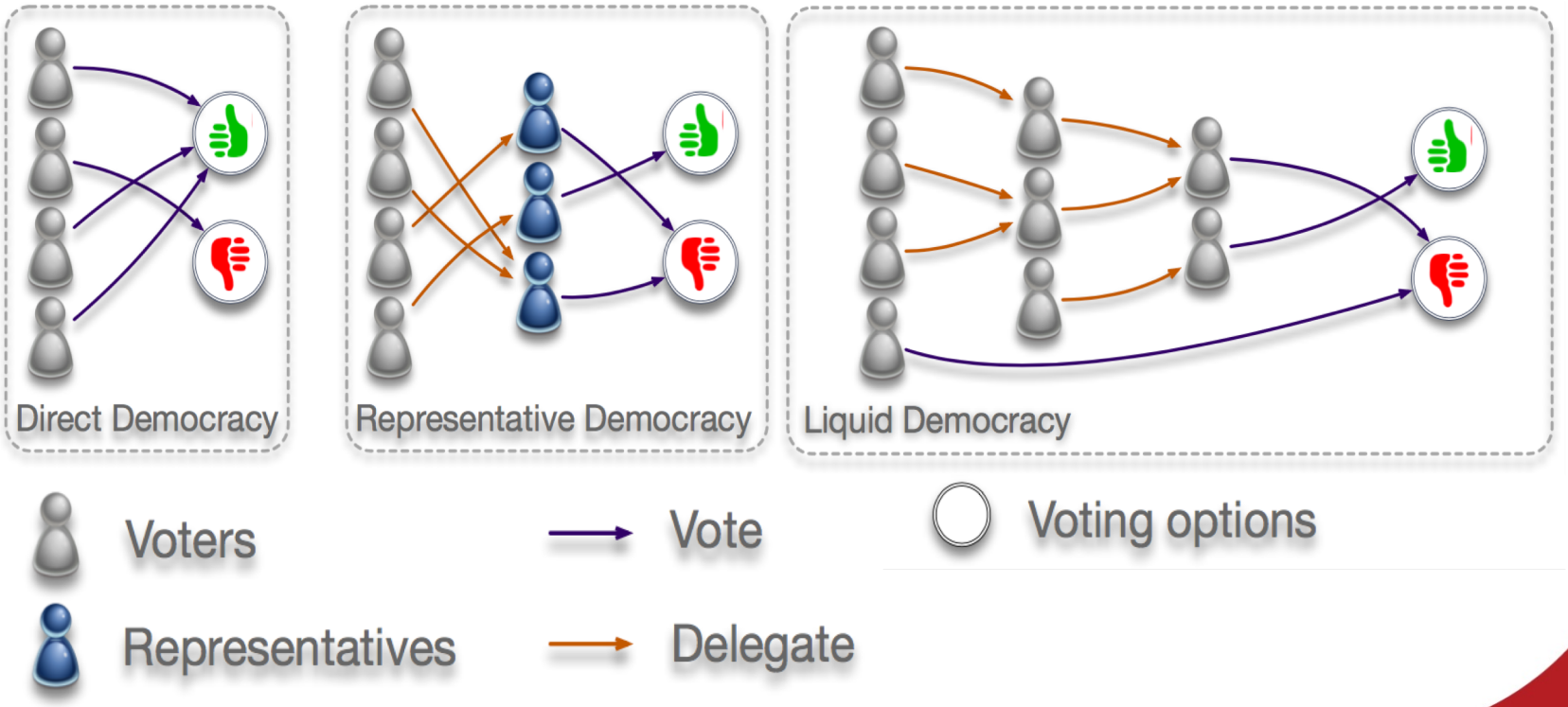
The principle of democratic self-organization has become a pervasive social value in the modern world, both in national governments and in many other types of organizations such as political, environmental, or religious groups. The basic premise of democracy, after all, seems quite sound: that the best way to ensure that an organization serves the interests of all its members fairly and equitably is to spread the ultimate power of decision and action evenly among all of the organization's members. The controversy arises in the practical details of how agreement is to be achieved on making rules and taking actions in the face of inevitable disagreements, conflicts of interest, and varying levels of time, knowledge, and abilities among

Source: https://bford.info/deleg/deleg.pdf

Supporting liquid democracy

Lancaster University

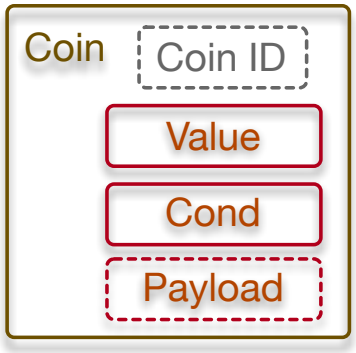
- Liquid democracy is a hybrid of direct democracy and representative democracy.

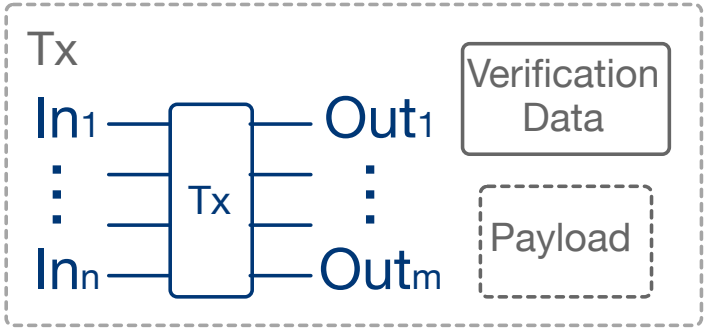


Cryptocurrency abstraction

Lancaster University

- Coin
  - Coin ID, value, condition, and payload
- Address
  - Generalized: spending condition the recipient intended
- Transaction
  - Inputs and outputs: s.t. $\sum_{i=1}^{n} \text{In}_i.\text{Value} \geq \sum_{j=1}^{m} \text{Out}_j.\text{Value}$

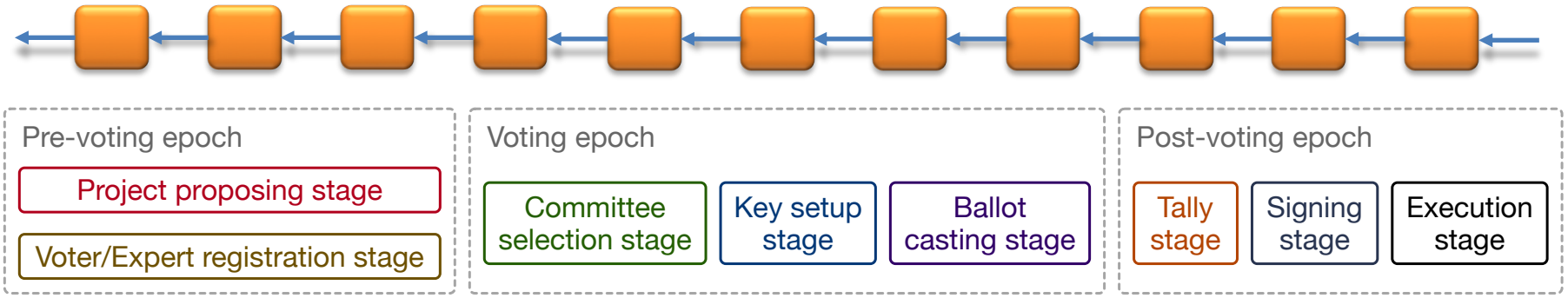




System overview

Lancaster University

- A treasury period consists of
  - Pre-voting epoch
  - Voting epoch
  - Post-voting epoch



Pre-voting epoch

- Project proposal
  - Open
  - Small cost: fee

- Voter registration
  - Minimum deposit
  - Voting power -- deposited stake
  - Reward -- deposited stake

Fine

- Expert registration
  - Fixed amount deposit
  - Voting power – delegations
  - Reward -- delegations

Voting epoch

Lancaster University

- Committee selection
  - Majority honest
  - Fixed deposit

- Key setup
  - Threshold PKE key generation
  - Robustness

- Ballot casting
  - See next page

Voting epoch

Lancaster University

- Ballot casting

Wait a minute. Where is delegation?

Conceptual barriers!

Answer: You vote your delegation

Voting epoch

Lancaster University

Unit vector

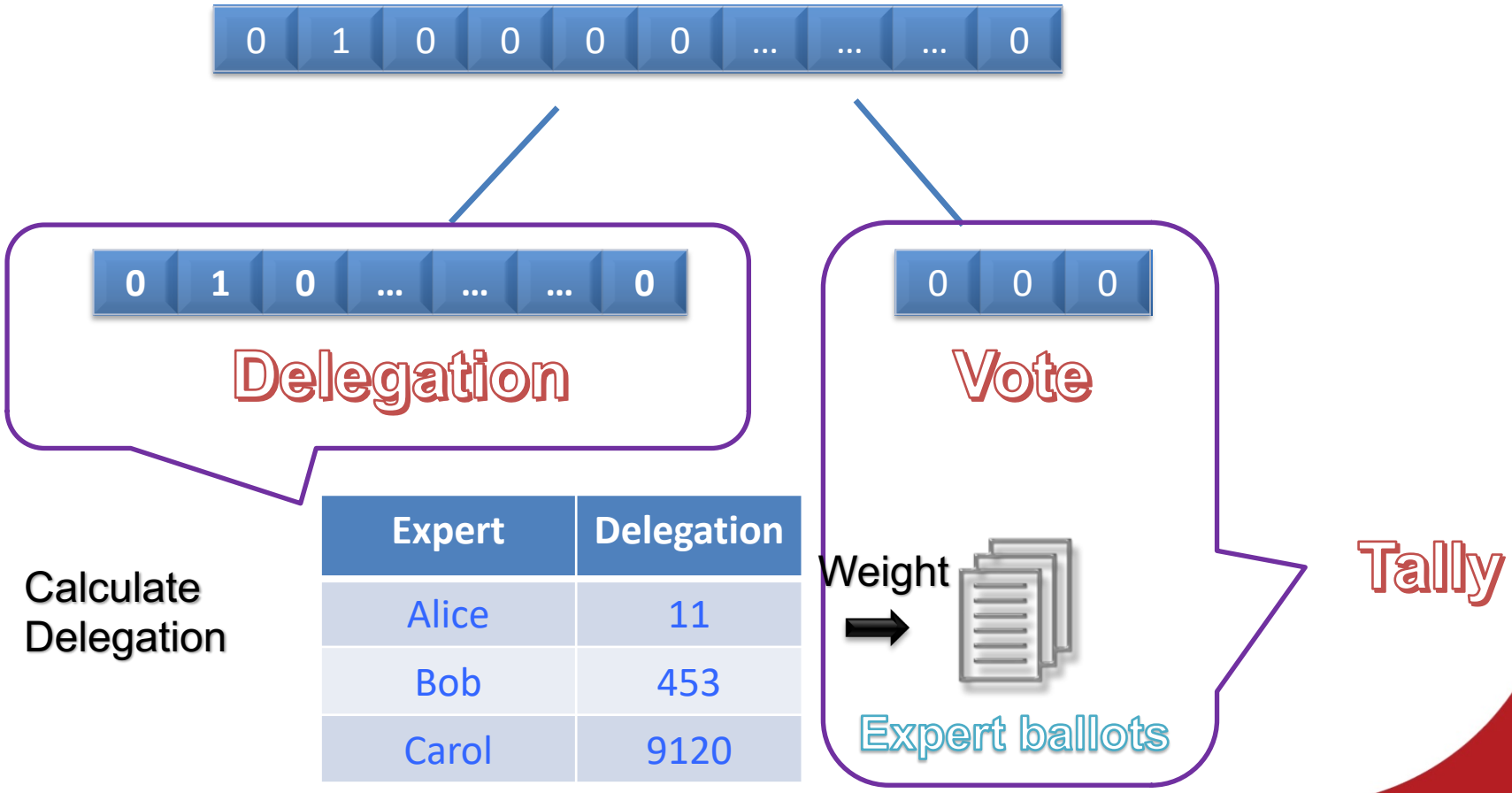
PROOF

Size: O(log n)

Post-voting epoch

Lancaster University

- Tally



Calculate Delegation

Expert	Delegation
Alice	11
Bob	453
Carol	9120

Post-voting epoch

Lancaster University

- Sign the decision
  - Tally results are signed by the voting committee and put on the blockchain
- Execution
  - Winning projects are funded
  - Voters and experts are rewarded: voters according to their deposit size, expert according to the level of delegation
  - Committee members are rewarded: fixed amount
  - [optional] Commit the next beacon

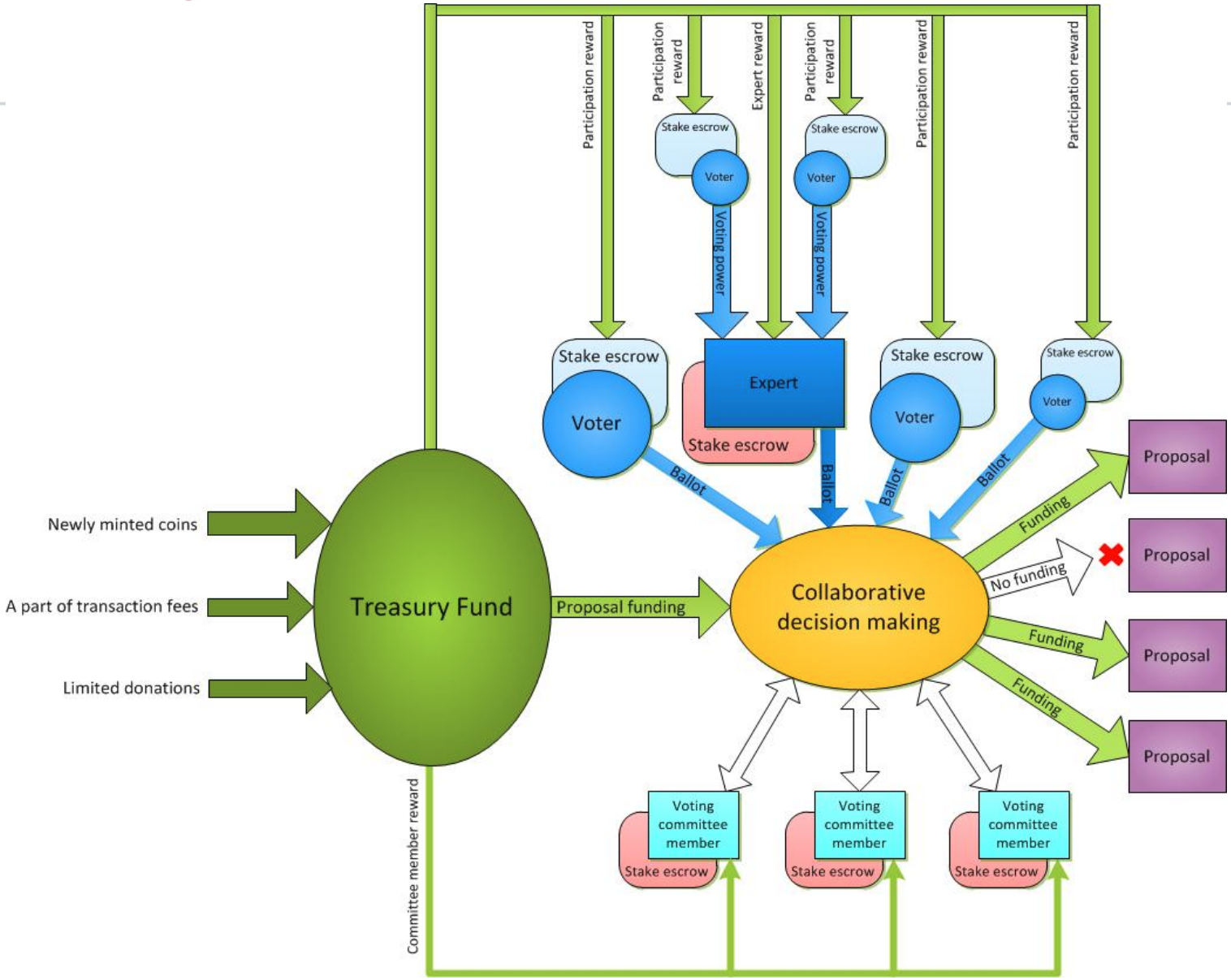
An example

Lancaster University

Title (listed by priority)	Monthly Amount	"Yes" Votes, stake	"No" Votes, stake	"Yes-No" difference	% of Votes
Core development (version 4.5.7)	12000	381800	12500	369300	95,45
Web portal and domain name maintenance (Feb-May 2018)	4000	362000	21000	341000	90,5
Design development for the new mobile client (version 17.4.8)	7000	349400	19100	330300	87,35
Marketing activity (ATM deployment)	3000	330300	29000	301300	82,575
Legal support (compliance analysis with respect to US/Nebraska legislation)	3000	327000	20100	306900	81,75
Cryptocurrency promotion at a FC conference	3000	273600	59100	214500	68,4
Fun challenge for Minecraft players	2000	180000	210100	-30100	-7,525
Total Budget	30 000 coins				
Total Number of Voting Stake	400000				

NB: 12000 + 4000 + 7000 + 3000 + 3000 = 29000 < 30000

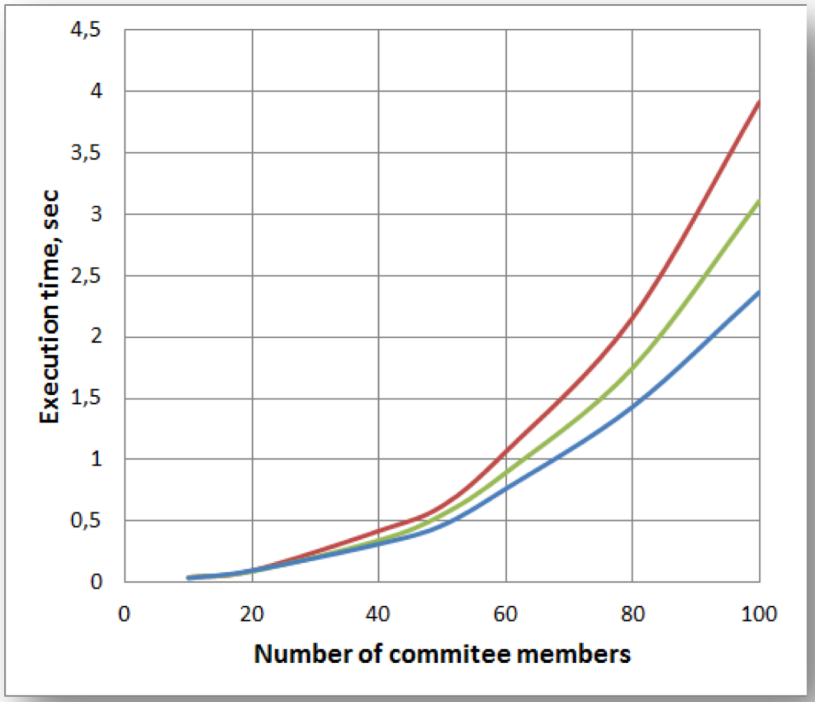
Put together



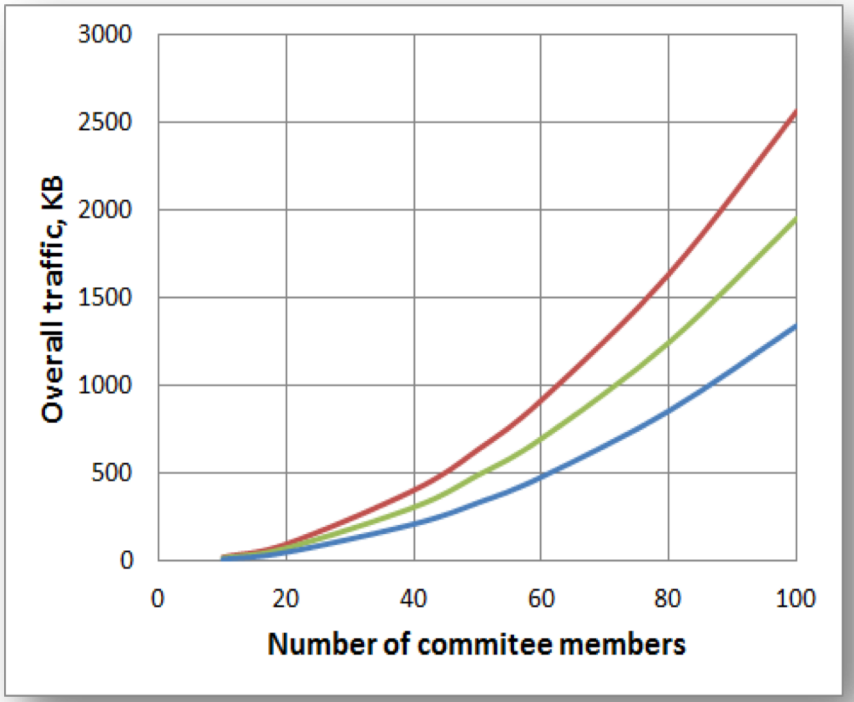
Performance (Setup)

Lancaster University

Time



Communication



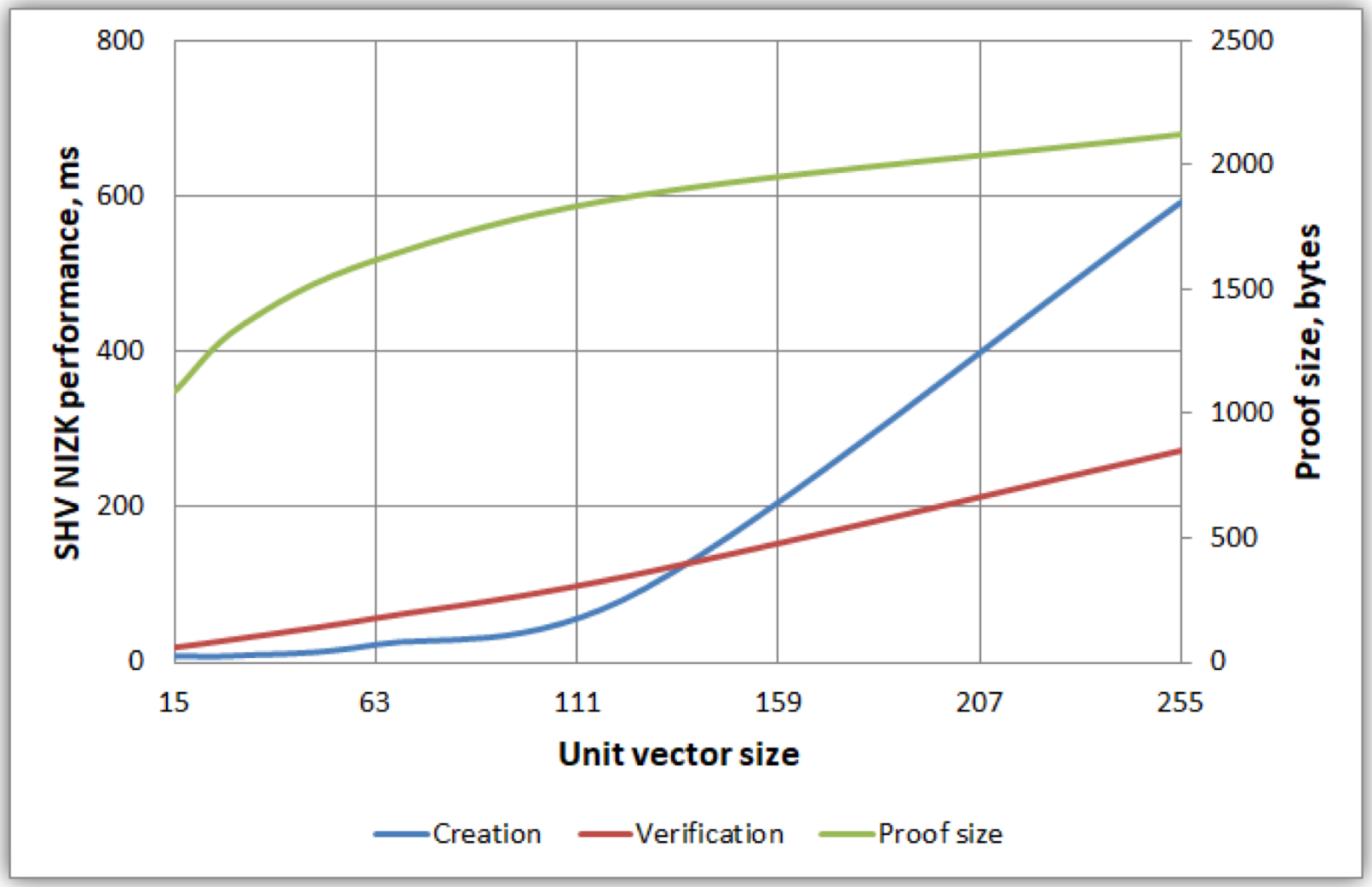
Malicious members ratio: 50%

Malicious members ratio: 25%

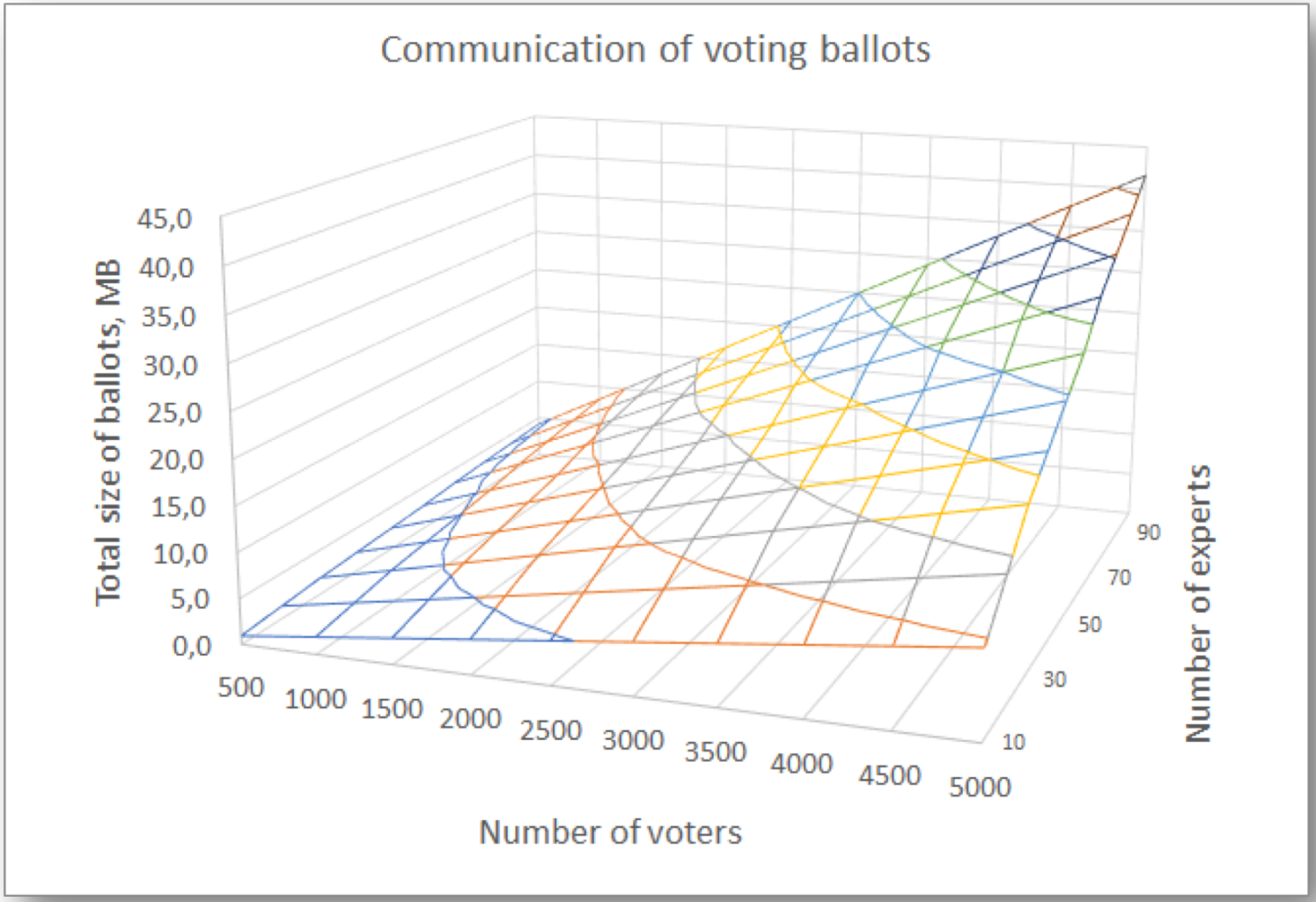
Malicious members ratio: 0%

Performance (Unit Vec NIZK)

Lancaster University



Performance (Overall)



Conclusion

Lancaster University

- Takeaways
  - Treasury system -- funding sustainability
  - It is currently adopted by Horizen
  - Support liquid democracy

- Future work
  - To support privacy preserving blockchains
  - Better project ranking schemes
  - Governance system

Full version: https://eprint.iacr.org/2018/435.pdf

Contact: b.zhang2@lancaster.ac.uk

Acknowledgement: This work is partially supported by IOHK