SybilQuorum:
Open Distributed Ledgers through Trust Networks

Authors
Alberto Sonnino*
George Danezis*

* University College London
and chainspace.io

January 2019
The Authors

Alberto Sonnino

George Danezis
Many challenges in blockchains

- Poor privacy
- Governance
- Scalability
- Security
Many challenges in blockchains

- Poor privacy
- Scalability
- Governance
- Security

Open systems need strong sybil defences
Our focus: bootstrapping an FBAS

Nodes do not have to be known ahead of time
Our focus: bootstrapping an FBAS

Nodes choose whom they trust
Our focus: bootstrapping an FBAS

How to achieve this with strong sybil resistance?
What are sybil attacks?

- Attacker creates multiple fake identities
What are sybil attacks?

- Attacker creates multiple fake identities

... and takes over the system
What should we do?

Cap the ability of the adversary to create multiple identities
What are sybil attacks?

- Traditional defences

  **Proof-of-Work**

  **Proof-of-Stake**
What are sybil attacks?

- Traditional defences
  
  Proof-of-Work
  
  Proof-of-Stake

Leverage scarce resources:

Money — by forcing to burn/lock it
What are sybil attacks?

- Traditional defences

The adversary needs to be rich
What are sybil attacks?

- Sometimes it is not enough...

Decentralised trading of financial products
( potentially worth $$$ )
What are sybil attacks?

- Sometimes it is not enough...

1. borrow a lot of money
2. turn it into tokens
3. subvert the system
4. payback the bank

What are sybil attacks?
What are sybil attacks?

- Can we strengthen existing mechanisms?

Leverage scare resources:

Money — by forcing to burn/lock it
What are sybil attacks?

- Can we strengthen existing mechanisms?

Leverage scarce resources:

- Money — by forcing to burn/lock it
- Trust — by penalising poor judgements
How do we make that happen?

**SybilQuorum**

Proof of Stake + Social network analysis

Lock stake on particular social links

Statistical analysis of nodes relationships
How to bootstrap an FBAS?

Step 1

Attribute weights to people you trust
An open system needs strong Sybil defences. Proof of Stake protocols: attackers can simply borrow a lot of money, turn it into tokens, and subvert the system. To defend against this, we use two-way stake wagers between entities, to build a social network of stake-weighted trust relationships.

We use social network theory to assess whether an entity is a Sybil. Poorly connected nodes to the main network see their stake attenuated.

**SybilQuorum: Step 1**

- **Stake-weighted trust relationships**
SybilQuorum: Step 1

- Stake-weighted trust relationships

Put money on links!
Both vertices can withdraw the money on the link
SybilQuorum: Step 1

- Stake-weighted trust relationships

Fraudsters can take the money and disappear

Poor judgement is penalised
SybilQuorum: Step 1

- Stake-weighted trust relationships

Bulk dishonesty protects against strategic dishonesty
How to bootstrap an FBAS?

Step 1
Attribute weights to people you trust

Step 2
Run social network analysis
An open system needs strong Sybil defenses. Proof of Stake protocols: attackers can simply borrow a lot of money, turn it into tokens, and subvert the system. To defend against this, we use two-way stake wagers between entities, to build a social network of stake-weighted trust relationships. (Academic paper 'Buffy' coming soon)

We use social network theory to assess whether an entity is a sybil. Poorly connected nodes to the main network see their stake attenuated.

SybilQuorum: Step 2

- Fast mixing assumption
An open system needs strong Sybil defences.

Proof of Stake protocols: attackers can simply borrow a lot of money, turn it into tokens, and subvert the system.

To defend against this, we use two-way stake wagers between entities, to build a social network of stake-weighted trust relationships. (Academic paper 'Buffy' coming soon)

We use social network theory to assess whether an entity is a sybil. Poorly connected nodes to the main network see their stake attenuated.

**SybilQuorum: Step 2**

- Fast mixing assumption

1. Fast integration of nodes into the network
An open system needs strong Sybil defences. Proof of Stake protocols: attackers can simply borrow a lot of money, turn it into tokens, and subvert the system. To defend against this, we use two-way stake wagers between entities, to build a social network of stake-weighted trust relationships. (Academic paper 'Buffy' coming soon)

We use social network theory to assess whether an entity is a sybil. Poorly connected nodes to the main network see their stake attenuated.

**SybilQuorum: Step 2**

- Fast mixing assumption

1. Fast integration of nodes into the network

2. Slow integration of sybils into the network
SybilQuorum: Step 2

- Each node performs a local judgement

Node’s view of the network
SybilQuorum: Step 2

- Each node performs a local judgement

Node’s view of the network

[Diagram showing a network node connected to a black box labeled 'Black Box']
SybilQuorum: Step 2

- Each node performs a local judgement

Node’s view of the network

Black Box

Map nodes to weights

...
SybilQuorum: Step 2

- Each node performs a local judgement

Node’s view of the network

Black Box

Map pk to weights

= SybilInfer, SybilGuard, SybilLimit, …
How to bootstrap an FBAS?

**Step 1**
Attribute weights to people you trust

**Step 2**
Run social network analysis

**Step 3**
Determine the quorum slices
SybilQuorum: Step 3

- Specify quorum slice for each node

![Diagram showing a set H with more than y members]
SybilQuorum: Step 3

- Specify quorum slice for each node

\[ > y \]

all subsets
\[ > \frac{2}{3} |H| \]
SybilQuorum: Step 3

- Specify quorum slice for each node

\[ y > \frac{2}{3} |H| \]
How to bootstrap an FBAS?

Step 1
Attribute weights to people you trust

Step 2
Run social network analysis

Step 3
Determine the quorum slices
Experimental evaluation

What to evaluate?

1. Number of sybil nodes?

2. Number of links/stake between sybils?

3. Number of links/stake between nodes and sybils?

4. Fraction of naïve nodes?
Conclusion

SybilQuorum: Sybil resistance mechanism
Conclusion

**SybilQuorum: Sybil resistance mechanism**

- **What?**

  Leverage Money by forcing to burn/lock it  
  Leverage Trust by penalising poor judgement
Conclusion

SybilQuorum: Sybil resistance mechanism

- What?
  - Leverage Money by forcing to burn/lock it
  - Leverage Trust by penalising poor judgement

- How?
  - Proof-of-Stake: build a stake-weighted graph
  - Social network analysis: determine sybil regions
Thank you for your attention
Questions?

Alberto Sonnino
http://sonnino.com