The IOTA Tangle: A Cautionary Tale

A presentation by A. Viscardi and T. Hollis

Plan

I) Introduction

II) IOTA Architecture
- A) The Tangle
- B) Consensus
- C) Incentive
- D) Stability & Smart Contracts

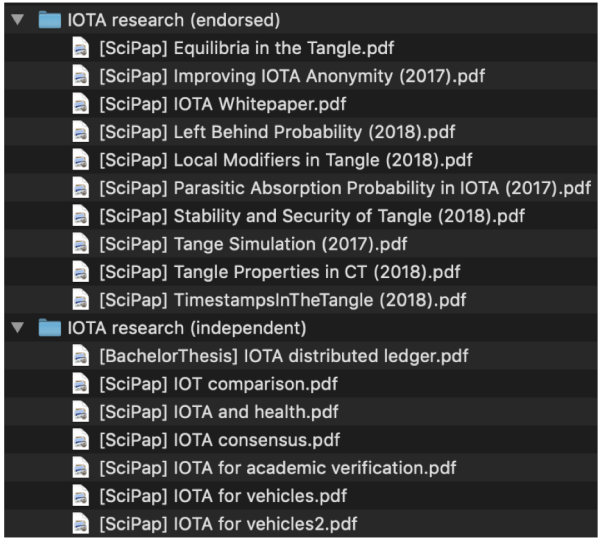
III) IOTA Performance
- A) Scalability & Decentralisation
- B) Protected Attacks
  1. Double Spending Attack
  2. Hash Collisions
  3. Quantum Computing
- C) Unprotected Attacks
  1. Parasitic Tangle
  2. Replay Attack
  3. Seed Gen Attack
  4. DDoS Attack
  5. Red Flags

IV) Conclusion

I) Introduction

- Available IOTA literature is **dense (20+ papers)**, actually mostly marketing

  Main goals:
  a. Microtransactions for IoT devices (Microsoft)
  b. Smart manufacturing (Fujitsu)
  c. Smart mobility (VW)
  d. Smart energy (Elaadnl)
  e. Smart health (IOTA MAM protocol)
  f. Data marketplace (store data in the Tangle)



- Like many other cryptocurrencies, IOTA is full of *buzzwords*, but has issues

II) IOTA Architecture
A) The Tangle

What is the main goal?

Support the rapidly increasing need for microtransactions by creating a scalable system that requires no fees.

What is IOTA’s solution?

The Tangle, a blockchain-less ledger system built on directed acyclic graph (DAG).

II) IOTA Architecture
A) The Tangle

Where is IOTA in the IEEE taxonomy of distributed ledger technology (DLT)?

1. Blockchains
    - **A. Traditional** - store transaction in a blockchain, simplest (e.g. Bitcoin)
    - **B. Offchain** – group transactions in local ledgers, better scaling (e.g. Lightning)
    - **C. Sidechain** – dynamically connect new sidechains to mainchain (e.g. LISK)
    - **D. Altchain** – alt blockchain with tokens/smart-contracts (e.g. ETH Namecoin)

2. Blockchainless DAGs
    - **A. BlockDAG** – blocks inside a DAG, usually has Tx fees (e.g. Conflux)
    - **B. TDAG** - transaction DAG, no total ordering (e.g. IOTA)

II) IOTA Architecture
A) The Tangle

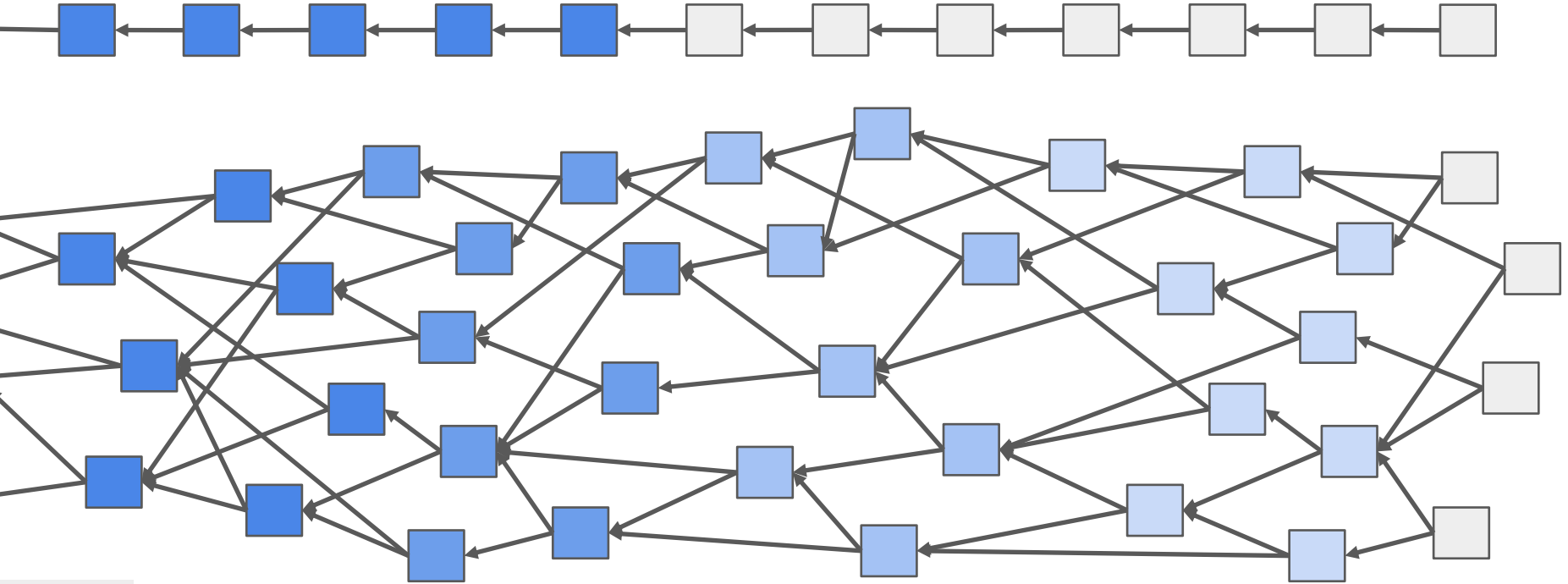
Where is IOTA in the IEEE taxonomy of distributed ledger technology (DLT)?

1. Blockchains
   - **A. Traditional** - store transaction in a blockchain, simplest (e.g. Bitcoin)
   - **B. Offchain** – group transactions in local ledgers, better scaling (e.g. Lightning)
   - **C. Sidechain** – dynamically connect new sidechains to mainchain (e.g. LISK)
   - **D. Altchain** – alt blockchain with tokens/smart-contracts (e.g. ETH Namecoin)

2. Blockchainless DAGs
   - **A. BlockDAG** – blocks inside a DAG, usually has Tx fees (e.g. Algorand)
   - **B. TDAG** - transaction DAG, no total ordering (e.g. IOTA)

II) IOTA Architecture
A) The Tangle

What does it mean?

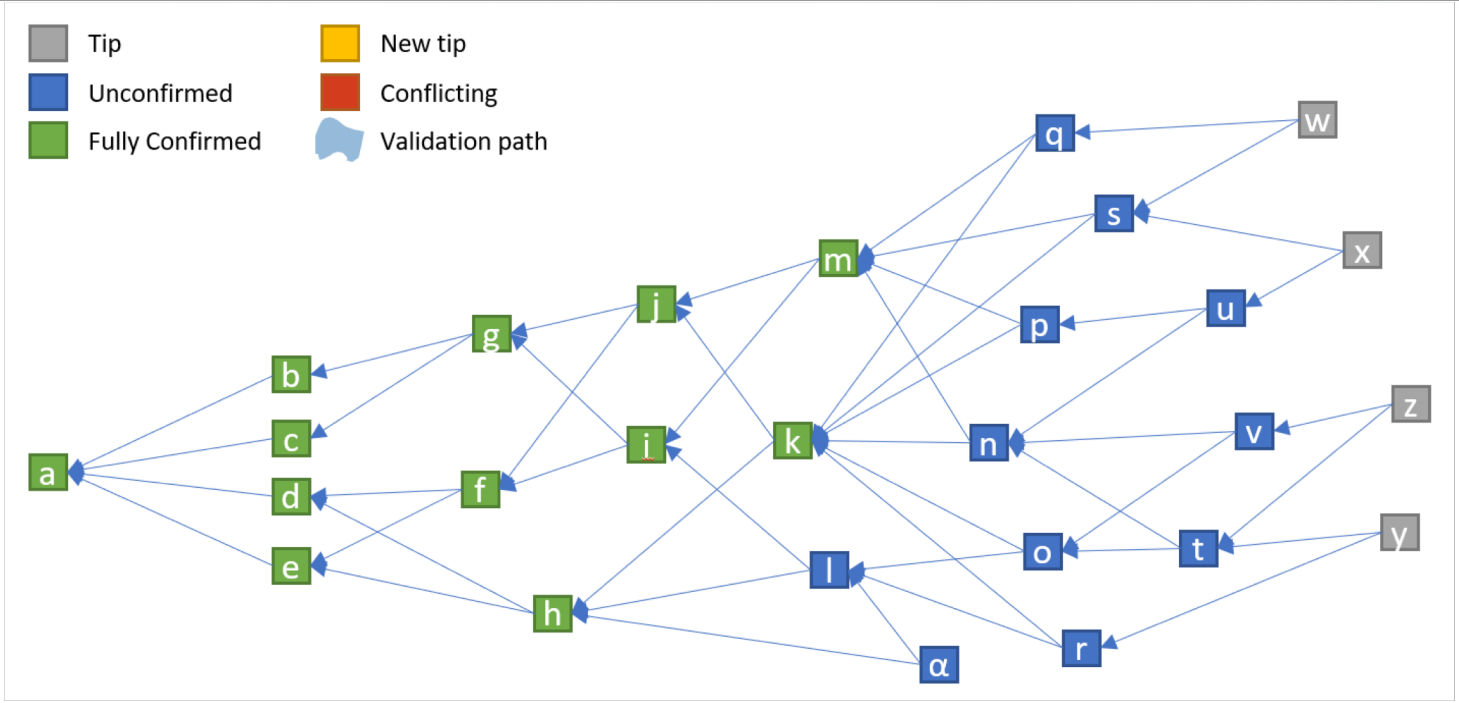


II) IOTA Architecture
B) Consensus

Homework Question:

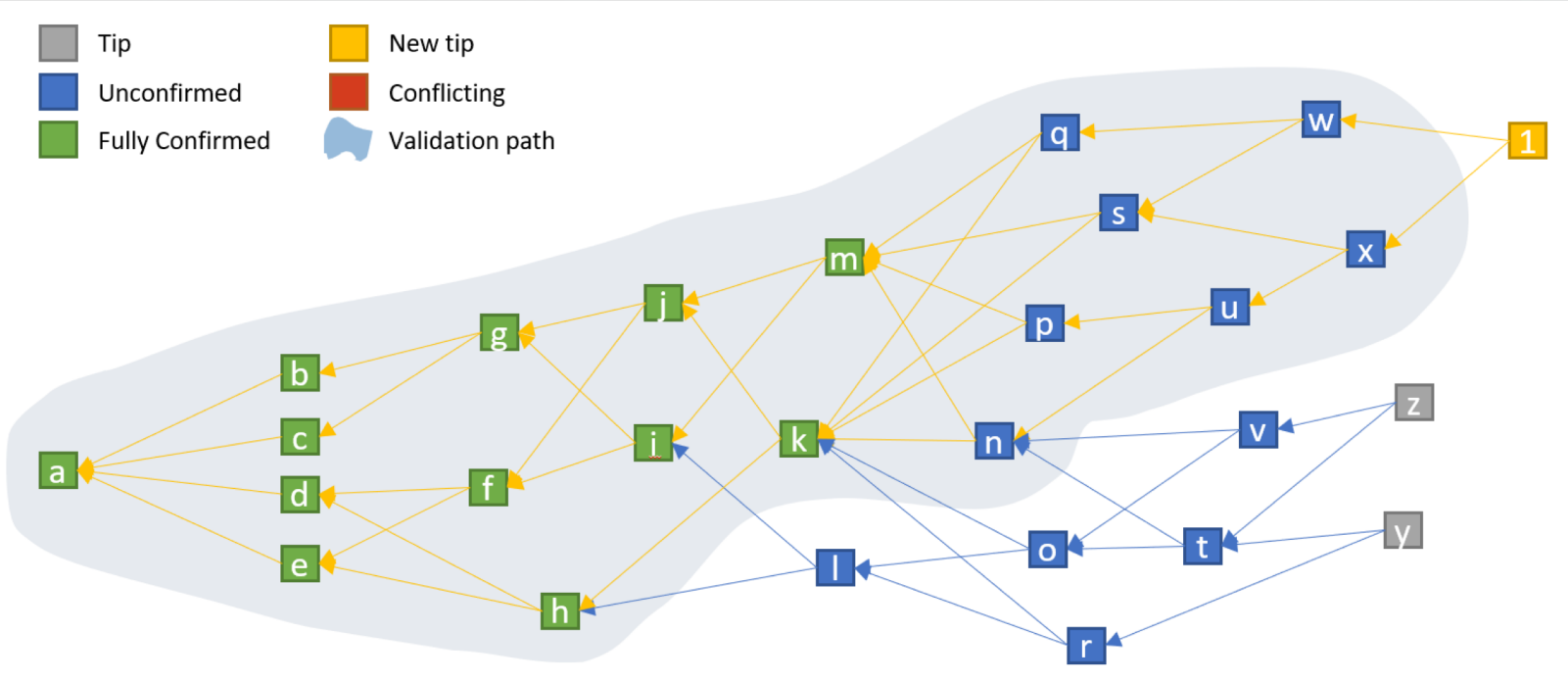
Are transaction confirmations guaranteed (like in Algorand) or probabilistic (like in Bitcoin)?

II) IOTA Architecture
B) Consensus



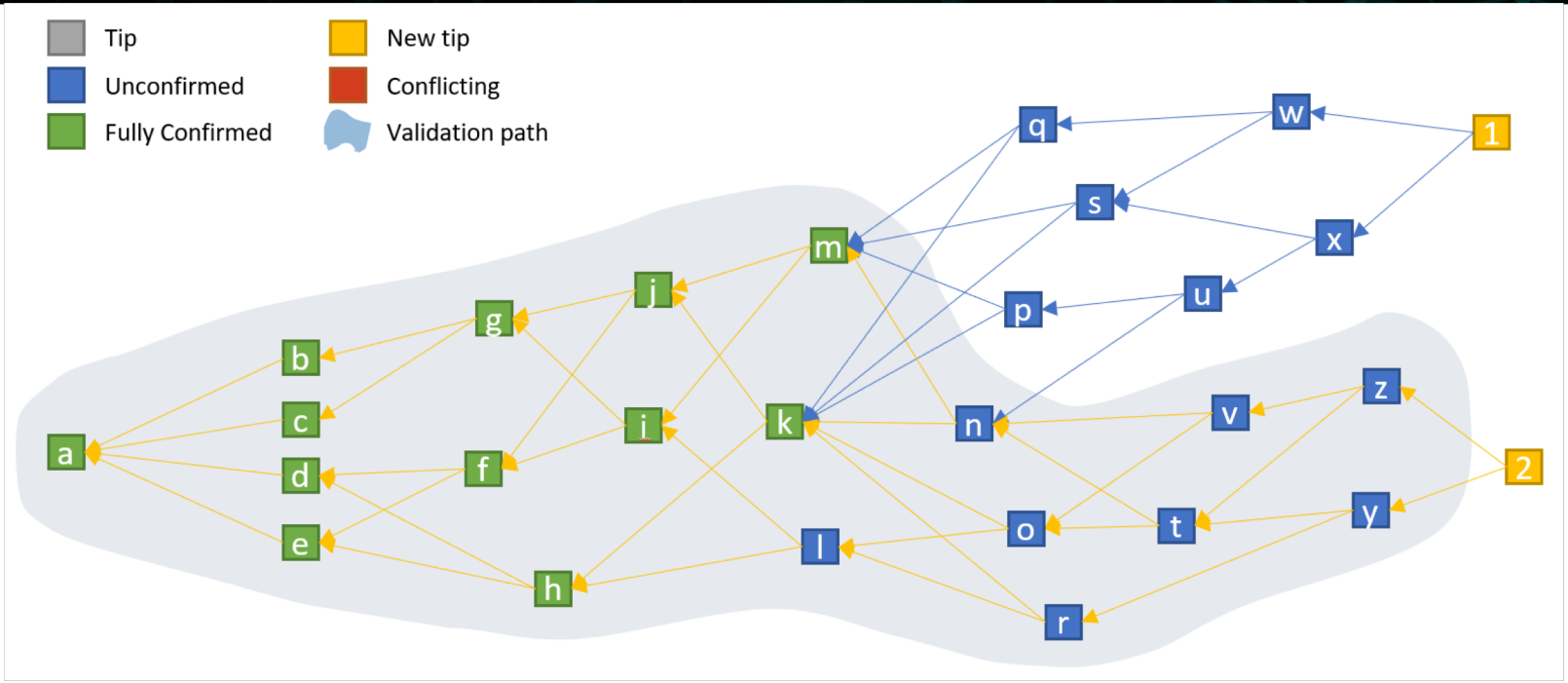
Credit: https://github.com/noneymous/iota-consensus-presentation

II) IOTA Architecture
B) Consensus



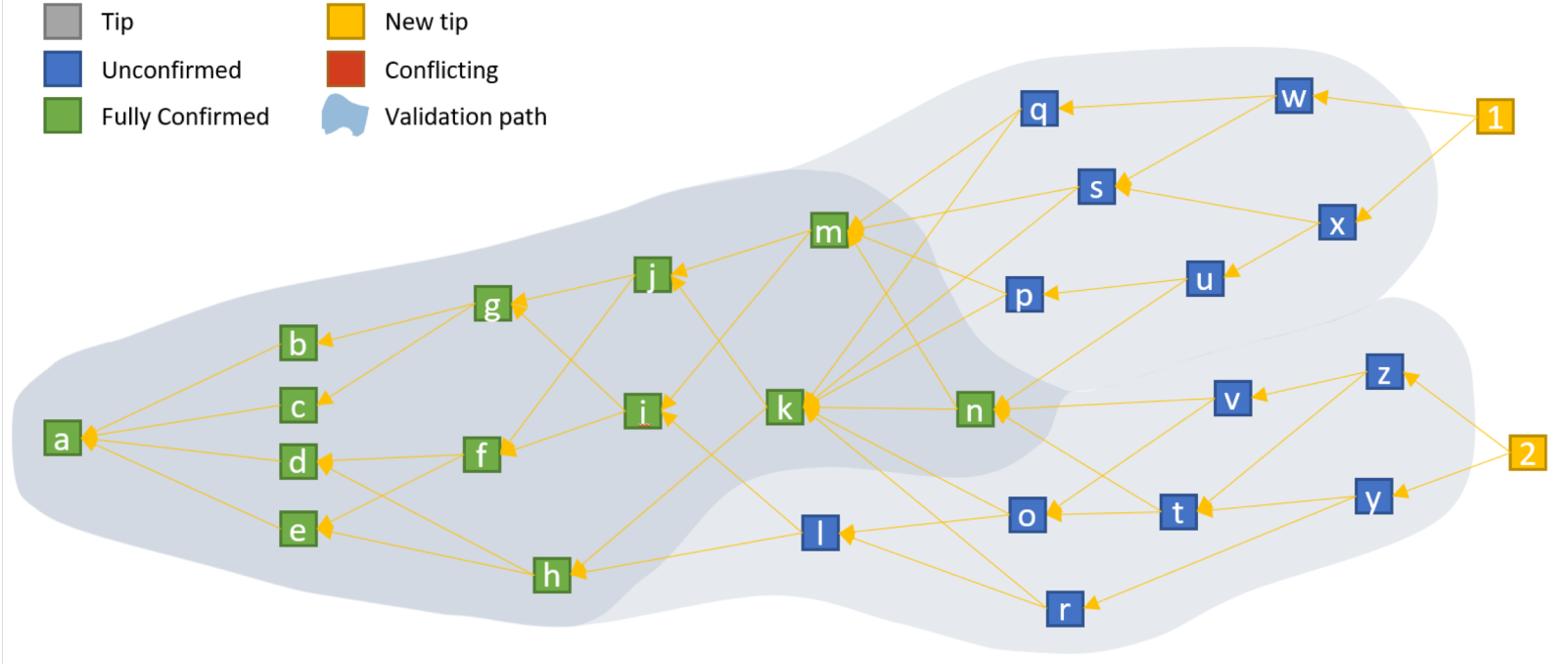
Credit: https://github.com/noneymous/iota-consensus-presentation

II) IOTA Architecture
B) Consensus



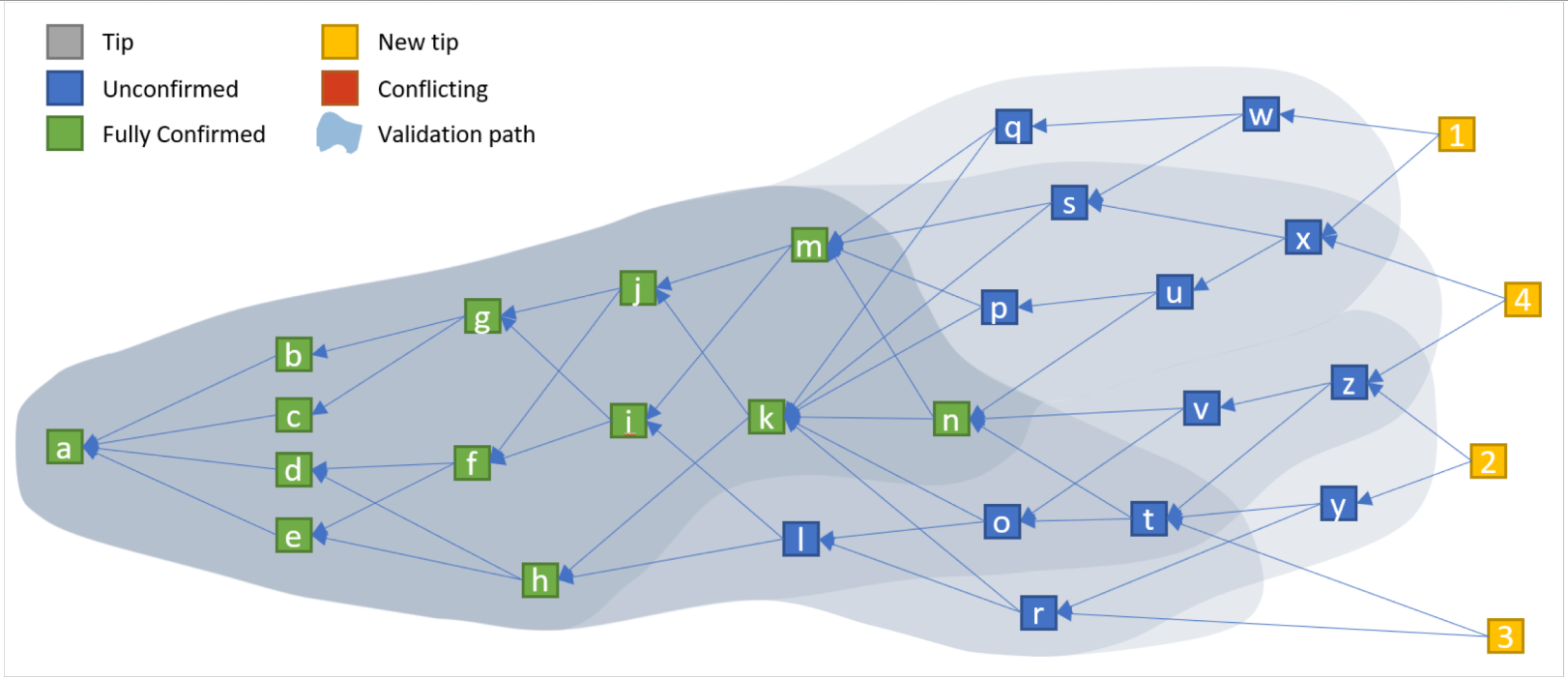
Credit: https://github.com/noneymous/iota-consensus-presentation

II) IOTA Architecture
B) Consensus



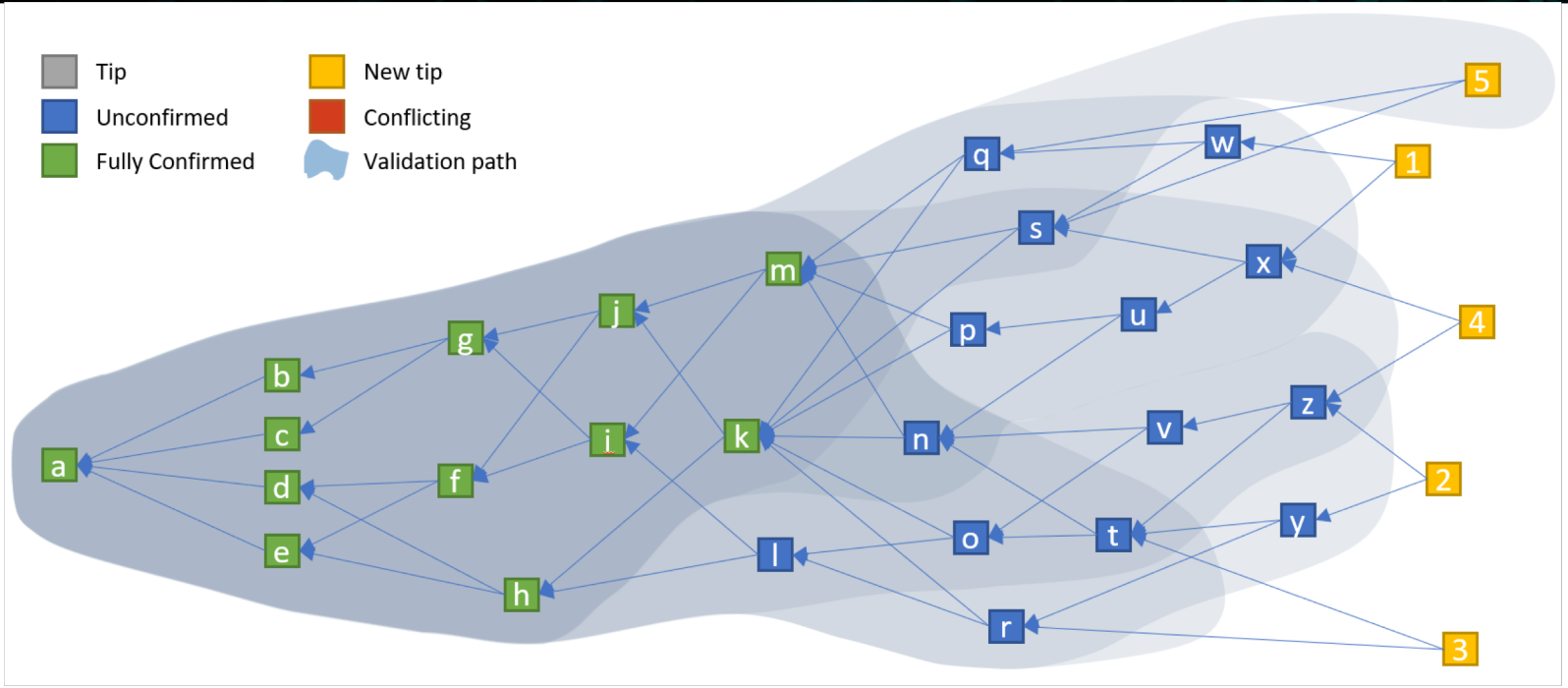
Credit: https://github.com/noneymous/iota-consensus-presentation

II) IOTA Architecture
B) Consensus



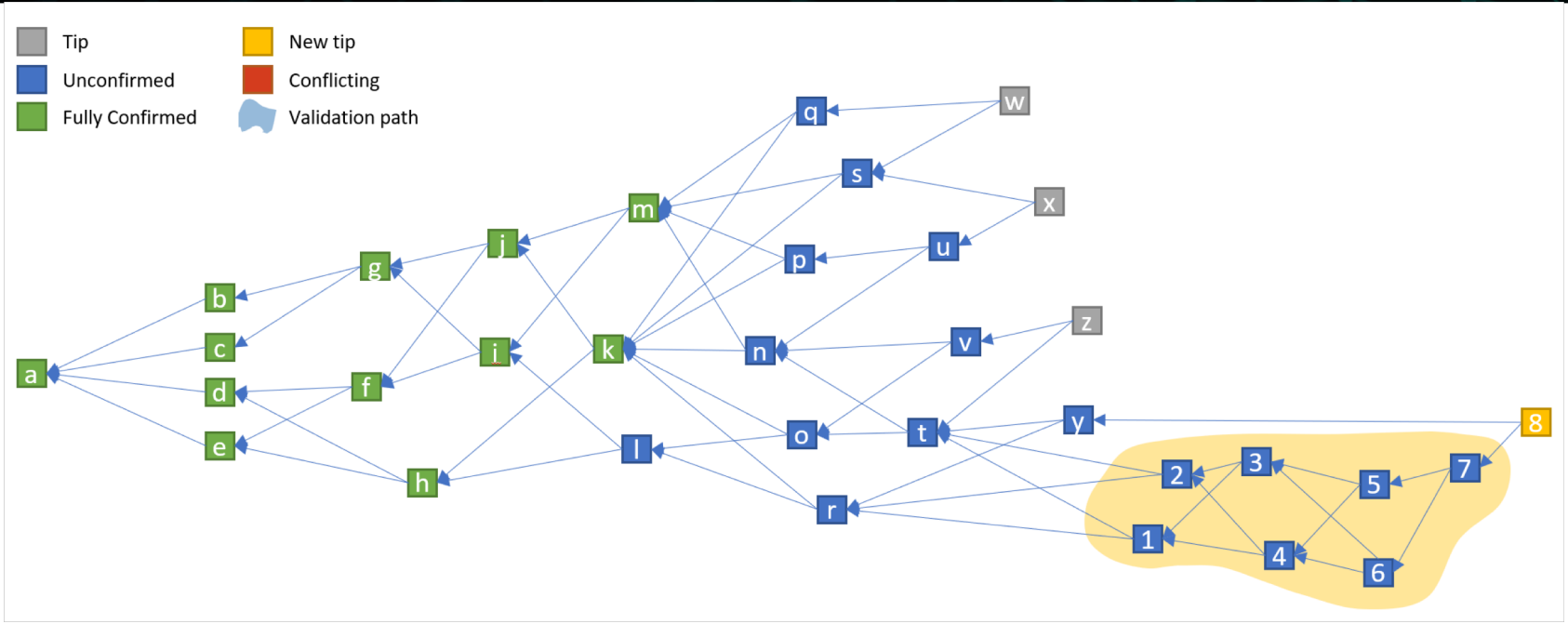
Credit: https://github.com/noneymous/iota-consensus-presentation

II) IOTA Architecture
B) Consensus



Credit: https://github.com/noneymous/iota-consensus-presentation

II) IOTA Architecture
B) Consensus



Credit: https://github.com/noneymous/iota-consensus-presentation

II) IOTA Architecture
C) Incentive

No fees!? What is the incentive then?

II) IOTA Architecture
C) Incentive

What is the problem here?

Why would anyone care **spending the resources** necessary to approve transactions if there is **no monetary reward**?

II) IOTA Architecture
C) Incentive

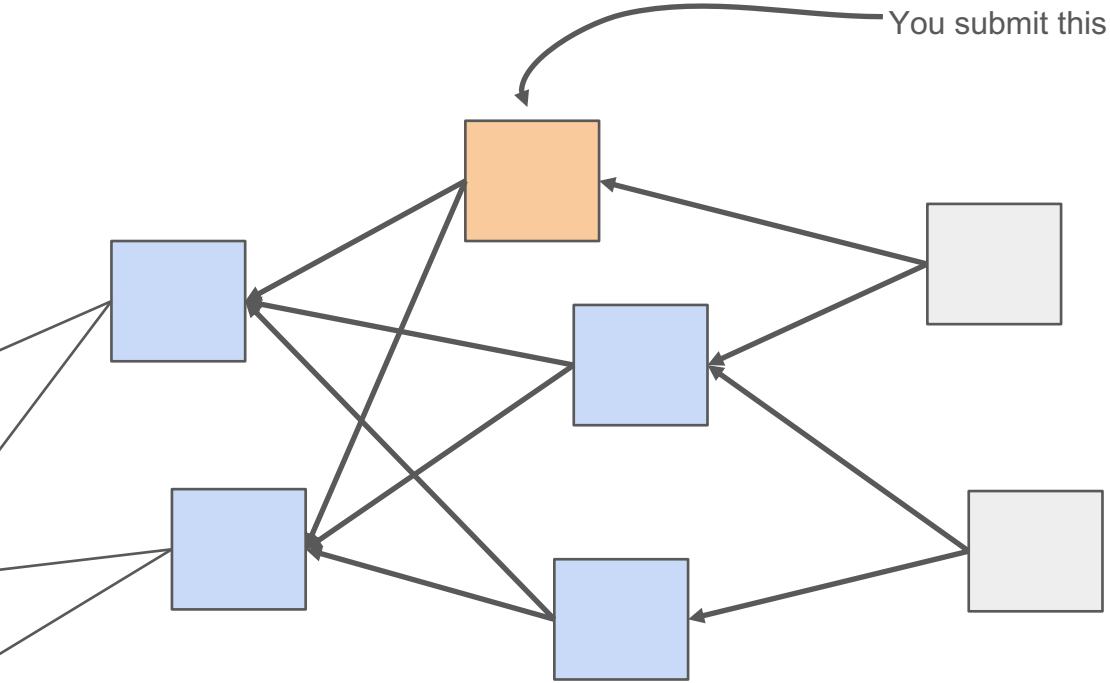
What is the problem here?

Why would anyone care **spending the resources** necessary to approve transactions if there is **no monetary reward**?

What if the transaction is **yours**?

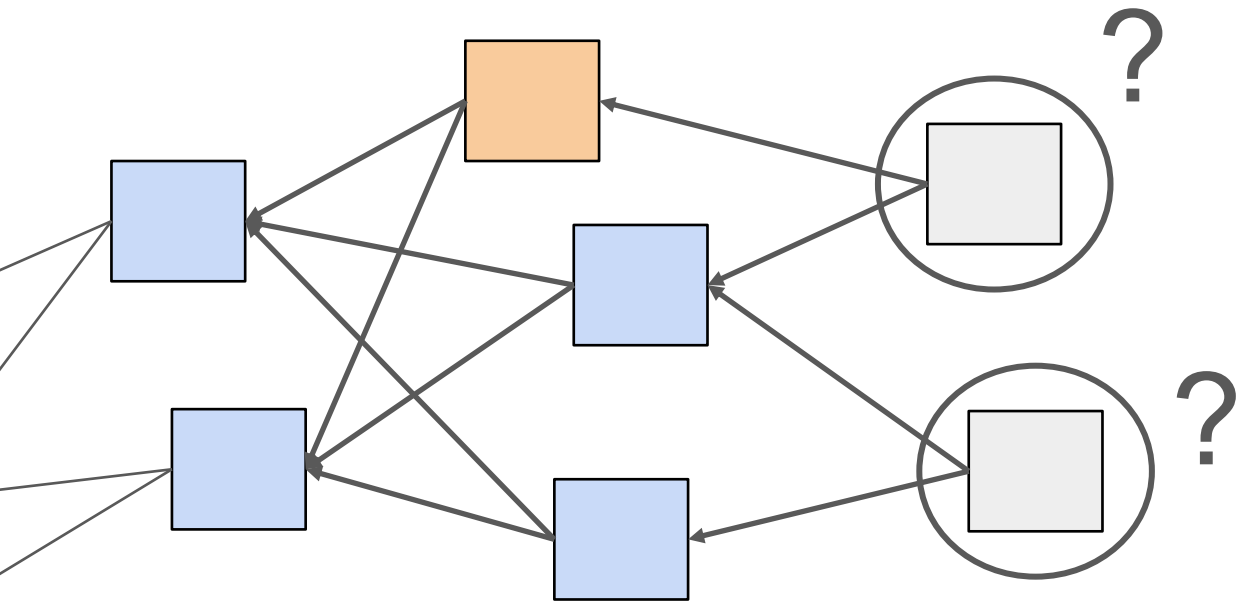
II) IOTA Architecture
C) Incentive

What is the problem here?



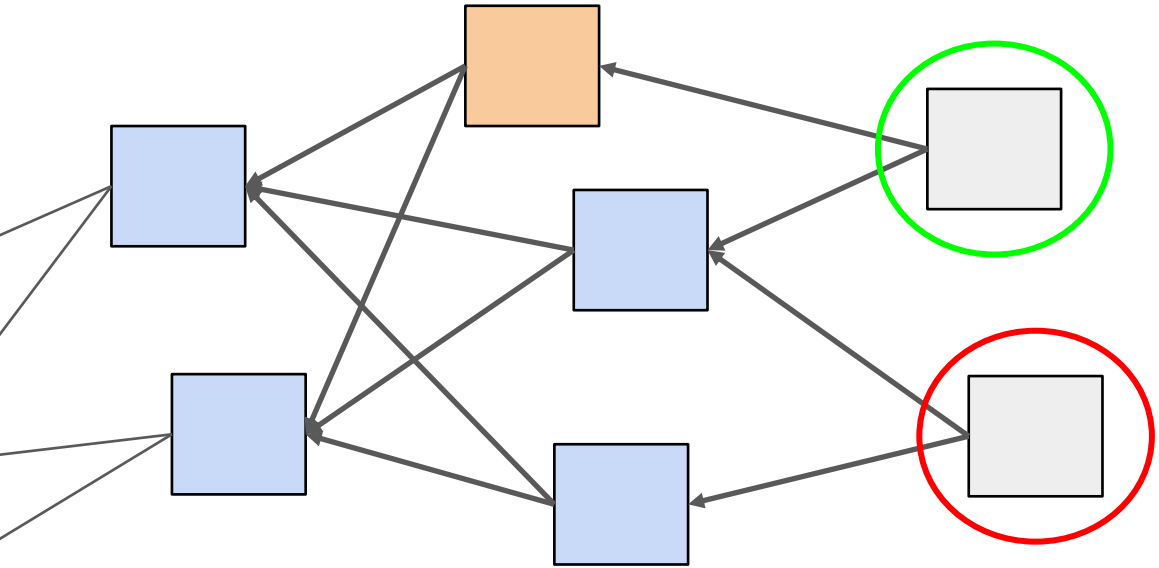
II) IOTA Architecture
C) Incentive

What is the problem here?



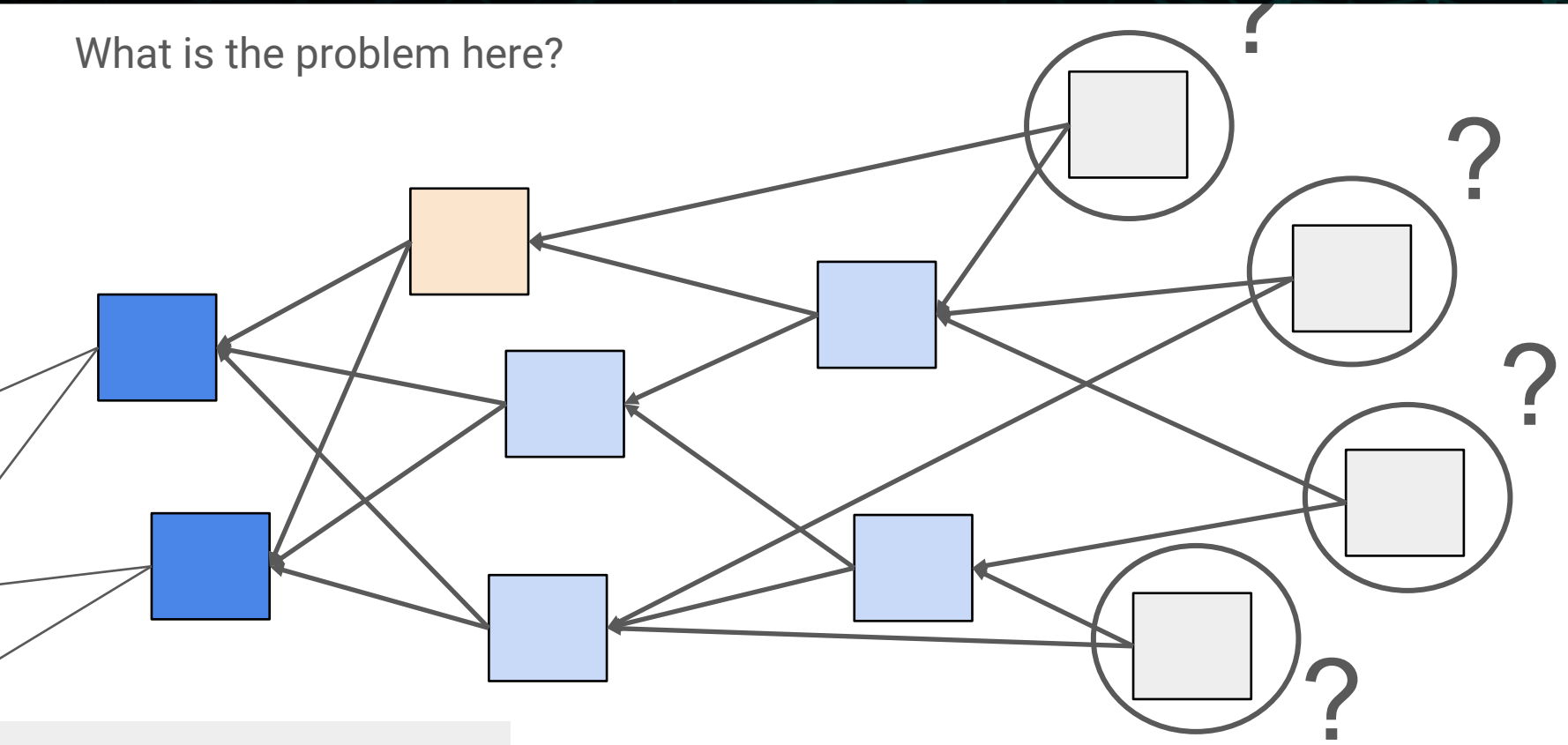
II) IOTA Architecture
C) Incentive

What is the problem here?



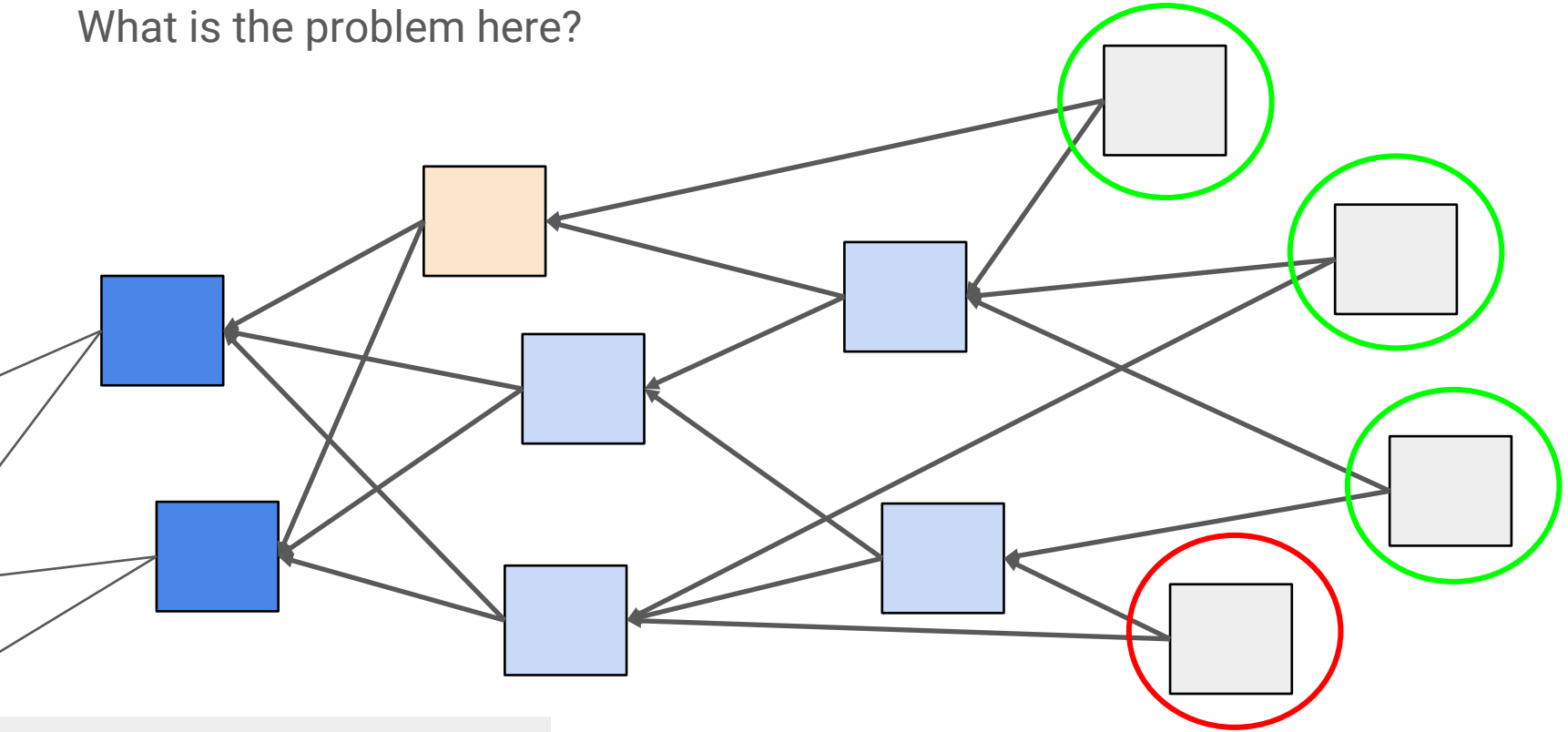
II) IOTA Architecture
C) Incentive

What is the problem here?



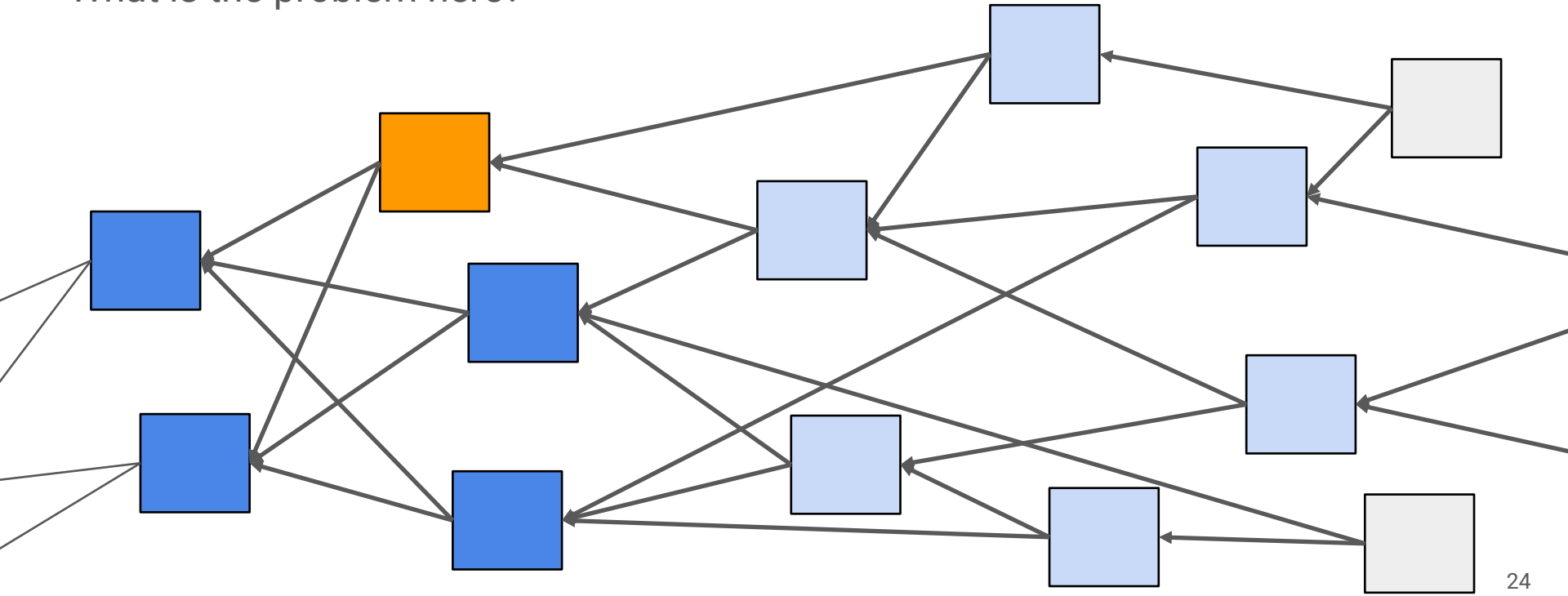
II) IOTA Architecture
C) Incentive

What is the problem here?



II) IOTA Architecture
C) Incentive

What is the problem here?



II) IOTA Architecture
C) Incentive

Unless you are constantly active in the network, your incentive fades away.

How do we fix that?

II) IOTA Architecture
C) Incentive

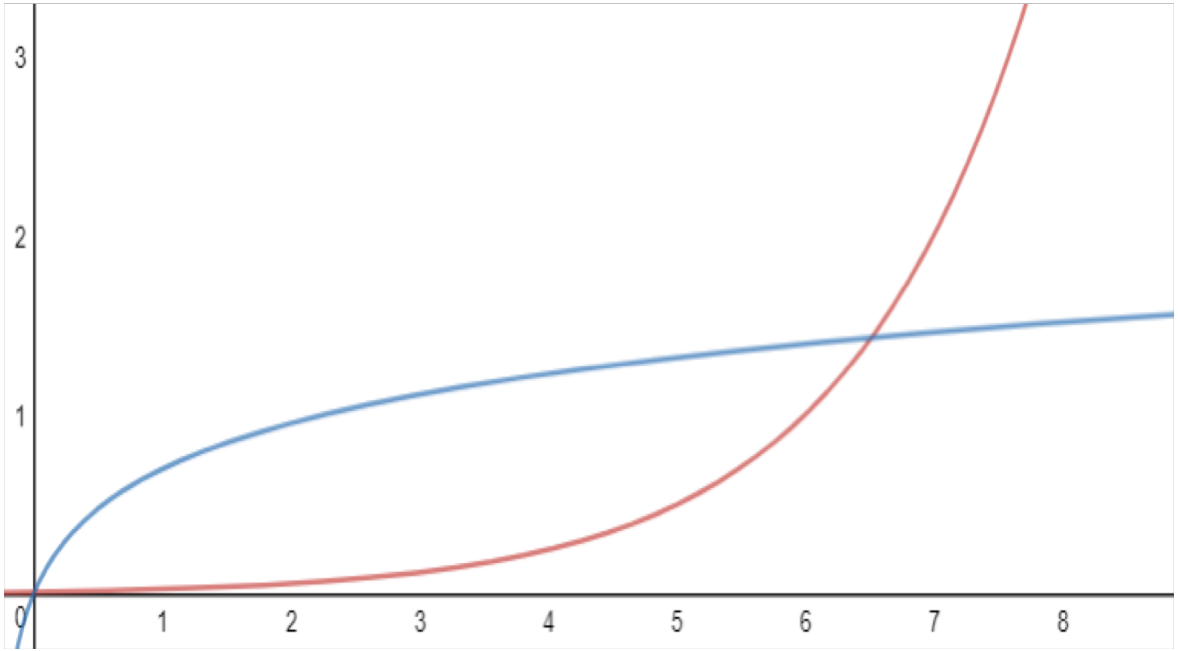
Unless you are constantly active in the network, your incentive fades away.

How do we fix that?

Lazy nodes get dropped.

II) IOTA Architecture
D) Stability & Smart Contracts

Is all this stable?



II) IOTA Architecture
D) Stability & Smart Contracts

We want to prove that the following exists and is positive.

$$\lim_{t \to \infty} P[L(t) = k]$$

II) IOTA Architecture
D) Stability & Smart Contracts

IOTA makes some assumptions:

1. The transactions are issued by a large number of **independent** entities. This can therefore be modeled as **Poisson point process**.
2. The rate **λ** of that process is **stable** in time.
3. All devices have roughly the same computing power and take a time **h** to do the computation required to issue a transaction.
4. Nodes select tips randomly.

II) IOTA Architecture
D) Stability & Smart Contracts

IOTA makes some assumptions:

5. A transaction attached to the tangle at time **t** becomes visible only at time **t + h**.
6. The number of tips remains roughly stationary in time around a number $\mathbf{L_0}$.
7. Typically, there are **r** revealed tips (visible to the network).

II) IOTA Architecture
D) Stability & Smart Contracts

We calculate $\mathbf{L_0}$ as a function of **λ** and **h** at some time **t**.

$$L_0 = r + \lambda h$$

II) IOTA Architecture
D) Stability & Smart Contracts

Because of our stationarity assumption, we can assume that at time **t** there are **λh** transactions that were tips at time **t - 1**.

$$L_0 = r + \lambda h$$

II) IOTA Architecture
D) Stability & Smart Contracts

New transactions approve tips with a probability of

$$\frac{r}{r + \lambda h}$$

Because it knows about **r** tips and **λh** transactions that it believes to be tips.

$$L_0 = r + \lambda h$$

II) IOTA Architecture
D) Stability & Smart Contracts

The mean number of approved tips is therefore,

$$\frac{2r}{r + \lambda h}$$

$$L_0 = r + \lambda h$$

$$\frac{r}{r + \lambda h}$$

II) IOTA Architecture
D) Stability & Smart Contracts

Now, because of our stationary assumption, new transactions should not change the number of tips.

That is, each transaction should validate one tip:

$$\frac{2r}{r+\lambda h} = 1$$

$$r = \lambda h$$

$$L_0 = 2\lambda h$$

$$L_0 = r + \lambda h$$

$$\frac{r}{r+\lambda h}$$

$$\frac{2r}{r+\lambda h}$$

II) IOTA Architecture
D) Stability & Smart Contracts

IOTA makes some assumptions:

1. The transactions are issued by a large number of **independent** entities. This can therefore be modeled as **Poisson point process**.
2. The rate **λ** of that process is **stable** in time.
3. All devices have roughly the same computing power and take a time **h** to do the computation required to issue a transaction.
4. Nodes select tips randomly.

II) IOTA Architecture
D) Stability & Smart Contracts

IOTA makes some assumptions:

5. A transaction attached to the tangle at time **t** becomes visible only at time **t + h**.
6. The number of tips remains roughly stationary in time around a number $\mathbf{L_0}$.
7. Typically, there are **r** revealed tips (visible to the network).

II) IOTA Architecture
D) Stability & Smart Contracts

Does it support smart contracts?

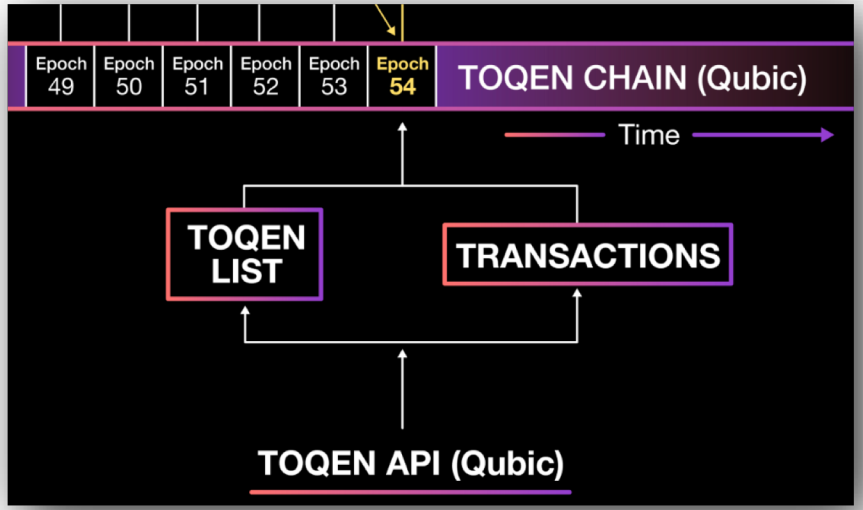
II) IOTA Architecture
D) Stability & Smart Contracts

Not directly.

We know: no total ordering of transactions → NO DIRECT SMART CONTRACTS

<u>However (PoC with questionable scaling)</u>:

- Layer 1: Data layer (IOTA)
- Layer 2: Consensus layer (QUBIC)
- Layer 3: Token layer (TOQEN)
- Layer 4: Application layer (MicroHash)



III) IOTA Performance

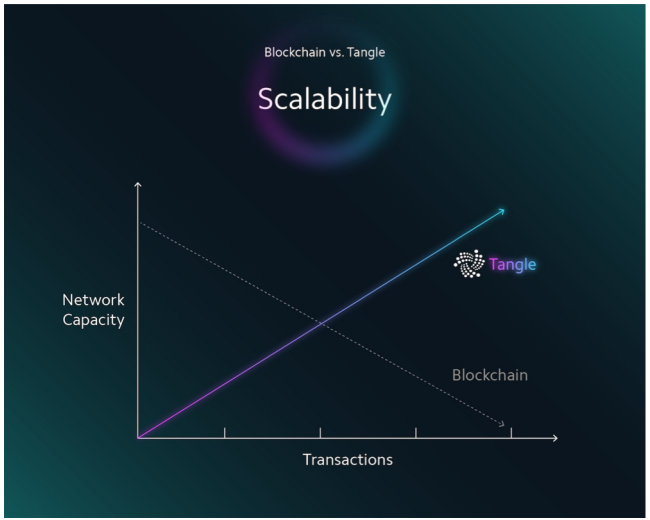
III) IOTA Performance
A) Scalability & Decentralisation

Does it scale?

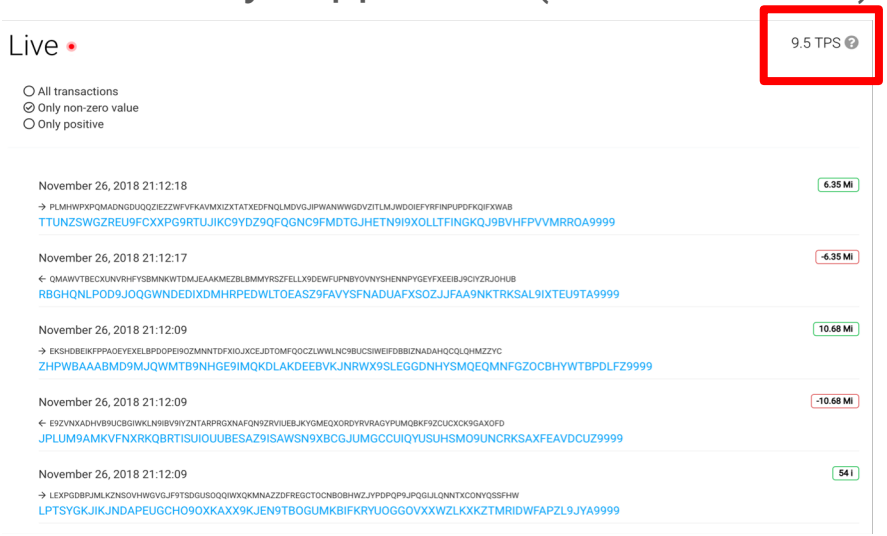
III) IOTA Performance
A) Scalability & Decentralisation

Not really…

What IOTA say:



What actually happens: (Tx size ~10KB)



III) IOTA Performance
A) Scalability & Decentralisation

Homework Question:

Is IOTA truly decentralised?

III) IOTA Performance
A) Scalability & Decentralisation

H_{att} = 13.5 TH/s *(One single Bitmain SHA256 ASIC, Antminer S9)*

$H_{att} > H_{honest}$ *(Condition for 51% attack)*

$H_{honest} > TPS \times H_{transaction}$ *($H_{transaction}$ estimated to be 60s x 2.5 MH/s, instead of 1s)*

Therefore:

$TPS > H_{att} / H_{transaction} = (13.5 \times 1'000'000) / (60 \times 2.5) =$ **90 000 TPS**

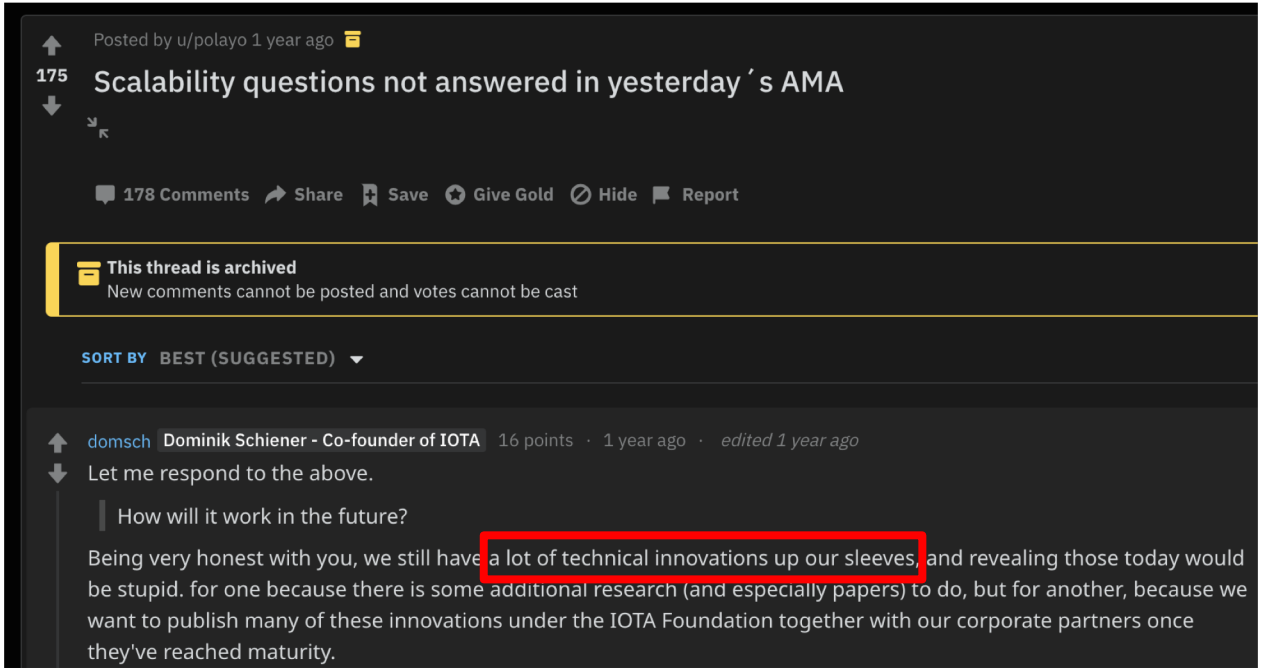
Note: 90k is a generous estimate, IOTA protocol breaks down after 33% malicious hashpower

III) IOTA Performance
A) Scalability & Decentralisation

Is IOTA decentralised?

Unlikely.

III) IOTA Performance
A) Scalability & Decentralisation

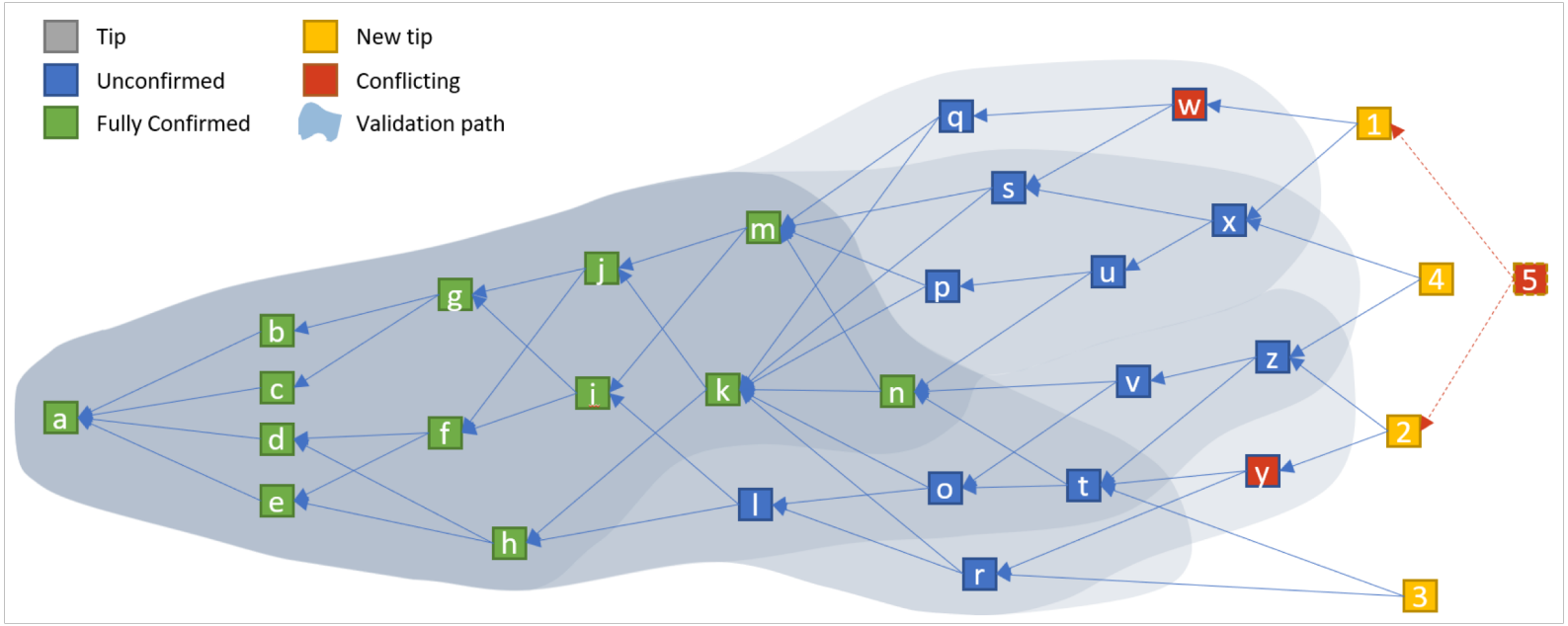


III) IOTA Performance
B) Protected Attacks - Double Spending Attack

Homework Question:

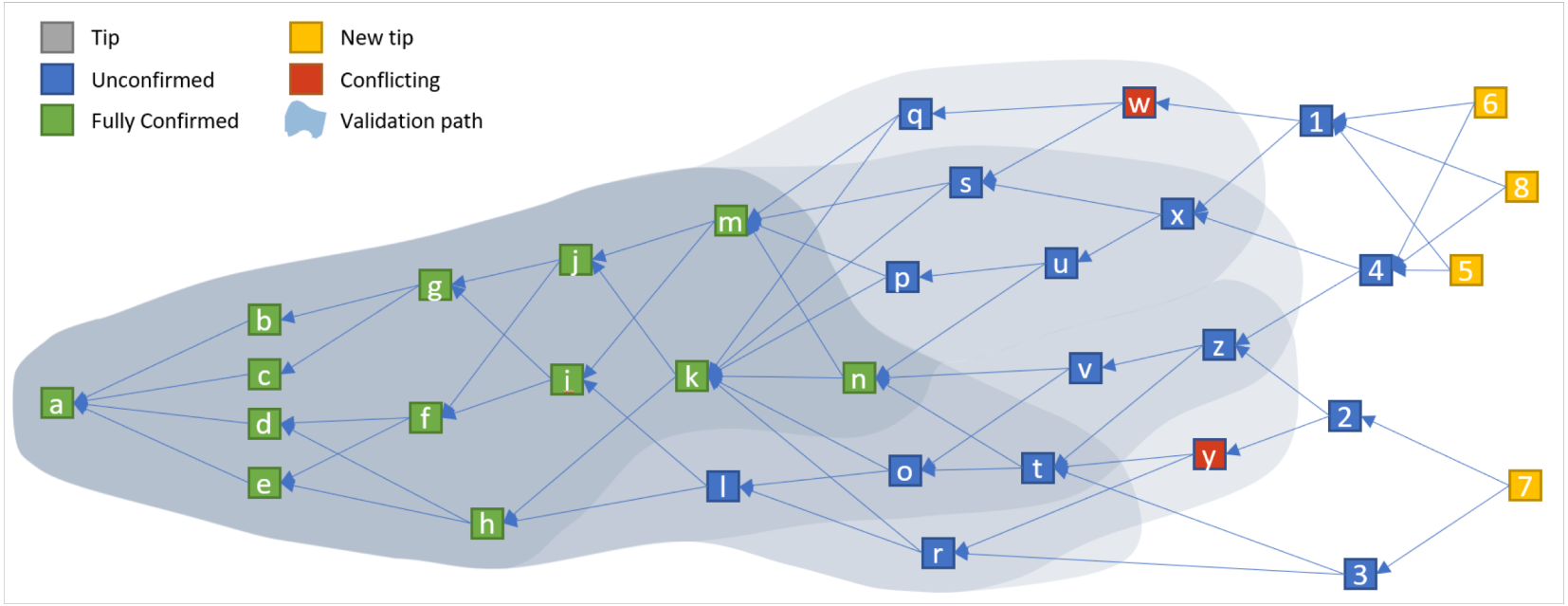
How does IOTA protect against a double spending attack?

III) IOTA Performance
B) Protected Attacks - Double Spending Attack



Credit: https://github.com/noneymous/iota-consensus-presentation

III) IOTA Performance
B) Protected Attacks - Double Spending Attack

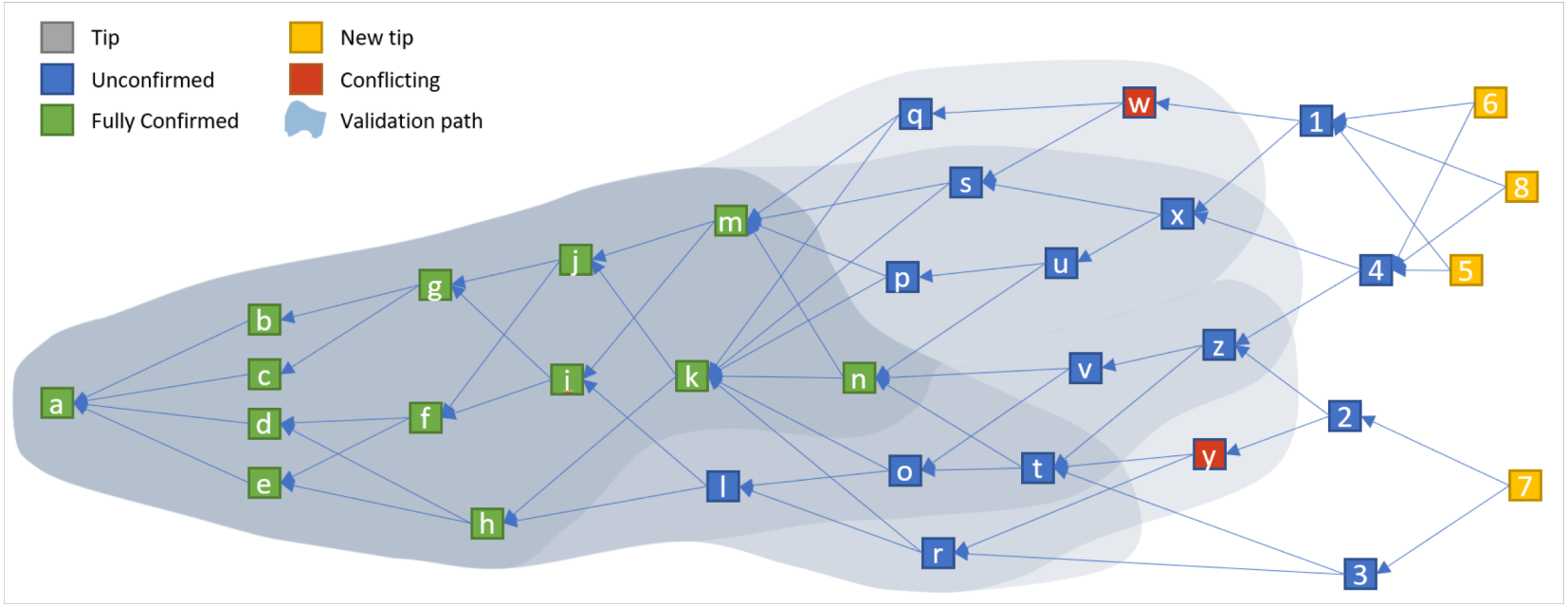


Credit: https://github.com/noneymous/iota-consensus-presentation

III) IOTA Performance
B) Protected Attacks - Double Spending Attack

What is wrong with a purely random tip selection approach?

III) IOTA Performance
B) Protected Attacks - Double Spending Attack



Credit: https://github.com/noneymous/iota-consensus-presentation

III) IOTA Performance
B) Protected Attacks - Hash Functions

Golden rule of cryptography: do not roll out your own!

III) IOTA Performance
B) Protected Attacks - Hash Functions

“CURL”

IOTA’s revolutionary custom-built hash function…

III) IOTA Performance
B) Protected Attacks - Hash Functions

It has hash collisions.

III) IOTA Performance
B) Protected Attacks - Hash Functions

IOTA forked, changed user addresses (inactive users lost funds) and…

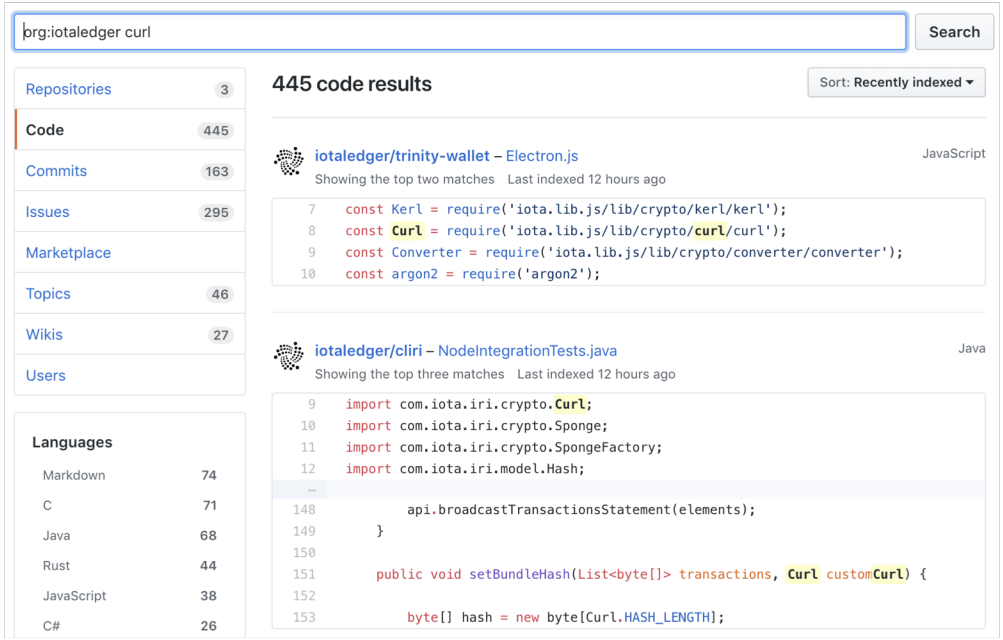
III) IOTA Performance
B) Protected Attacks - Hash Functions

IOTA forked, changed user addresses (inactive users lost funds) and…

Now they use SHA3.

III) IOTA Performance
B) Protected Attacks - Hash Functions

NB: IOTA replaced SHA3 in critical areas, our code review shows still full of CURL...

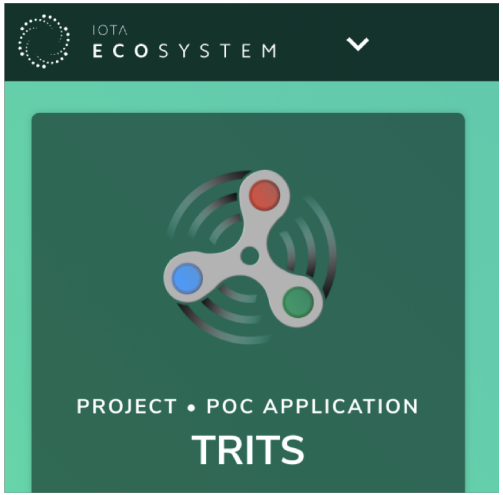


III) IOTA Performance
B) Protected Attacks - Quantum Computing

- White paper claims to be resistant
- Claim is that this is achieved with specialised “post-quantum” code (trits/trytes).

- Not sure if anyone believes this
- Little research has been done yet on the ternary security algos used

- Even MIT white hat hackers said they struggled to audit this in their paper



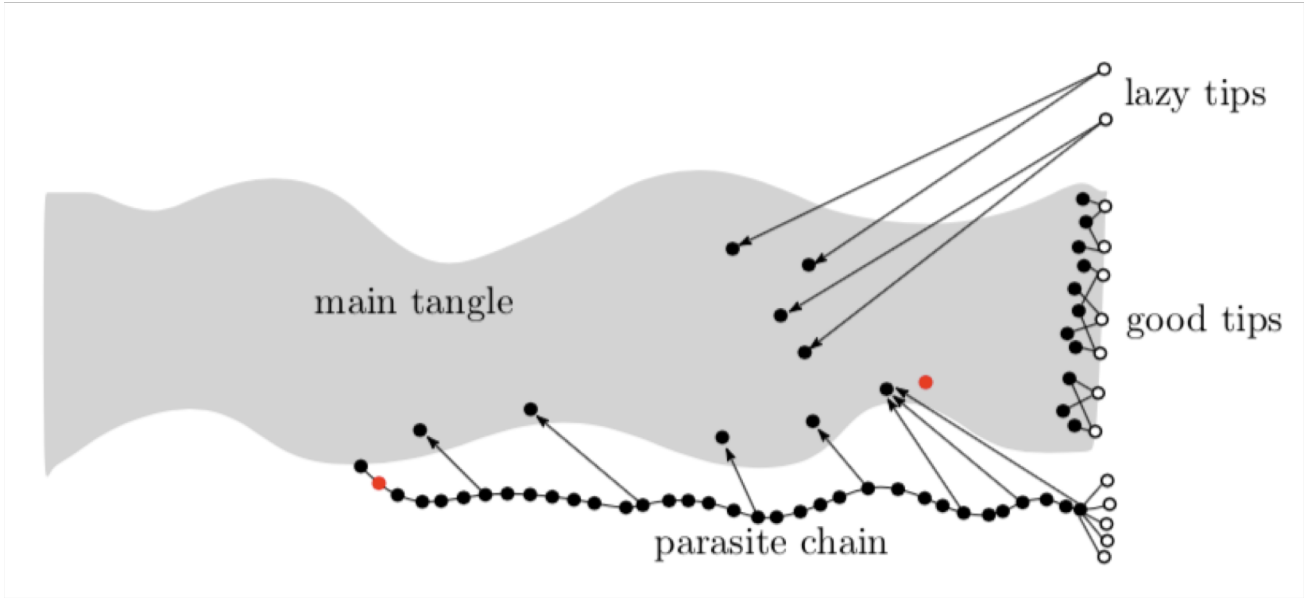
III) IOTA Performance
C) Unprotected Attacks - Parasitic Tangle

Homework Question:

What is a parasitic tangle and how can it be created? Is this a problem in IOTA?

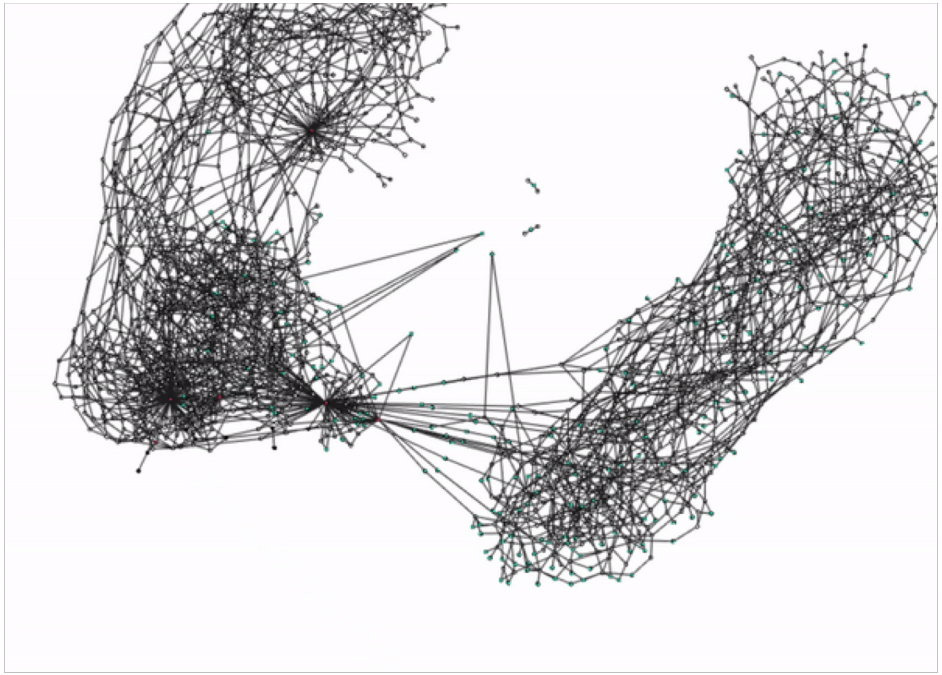
III) IOTA Performance
C) Unprotected Attacks - Parasitic Tangle

In theory (from original IOTA whitepaper):

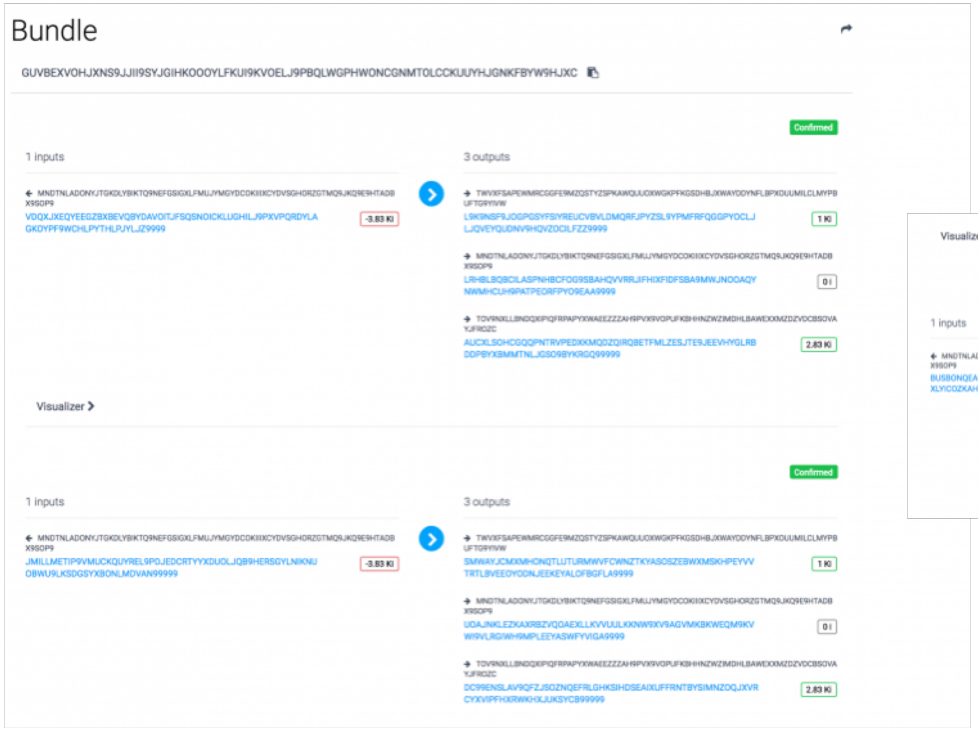


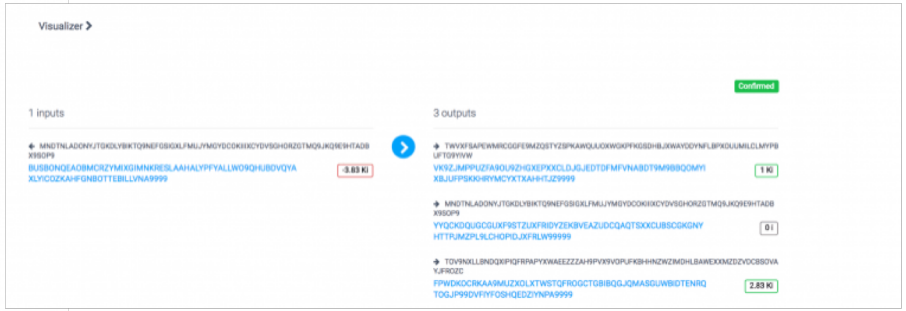
III) IOTA Performance
C) Unprotected Attacks - Parasitic Tangle

In practice:

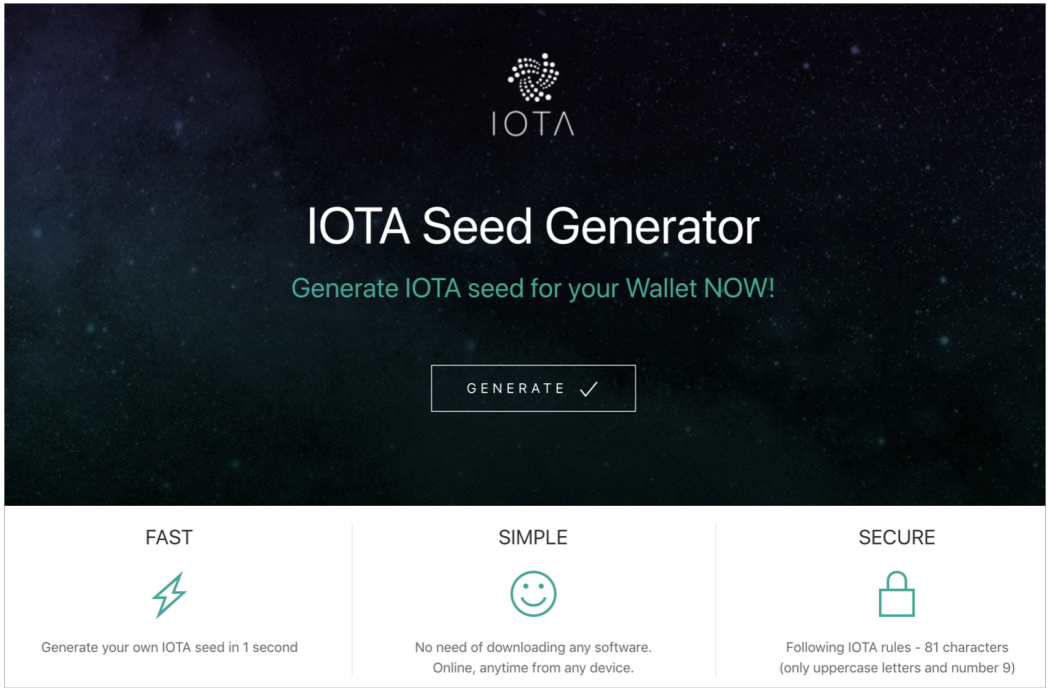


III) IOTA Performance
C) Unprotected Attacks - Replay Attack





III) IOTA Performance
C) Unprotected Attacks - Seed Gen Attack



https://www.iotaseedgenerator.online/

III) IOTA Performance
C) Unprotected Attacks - DDoS Attack

IOTA claim:

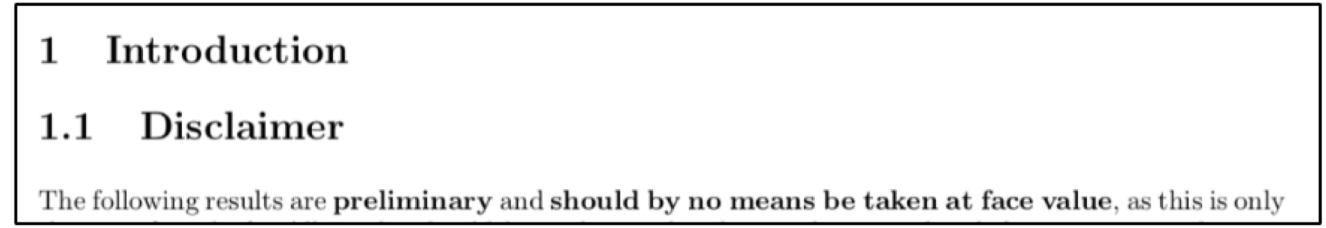
“DDoS makes IOTA stronger”

III) IOTA Performance
C) Unprotected Attacks - Red Flags

- Whitepaper is pretty poorly written (“assume” on 17/28 pages, 27 times total)
- Fairly ludicrous assumptions have been made (as discussed earlier)
- Fully transparent Tx, 0 privacy - recommends off-ledger-mixing (bad for IoT)
- IOTA source code mostly written in JAVA instead of C++ like other cryptos
- IOTA owners own 0.8% of all IOTA (they cashed out - unlike 60% in Ripple, #2)

III) IOTA Performance
C) Unprotected Attacks - Red Flags

- Some publication gems:



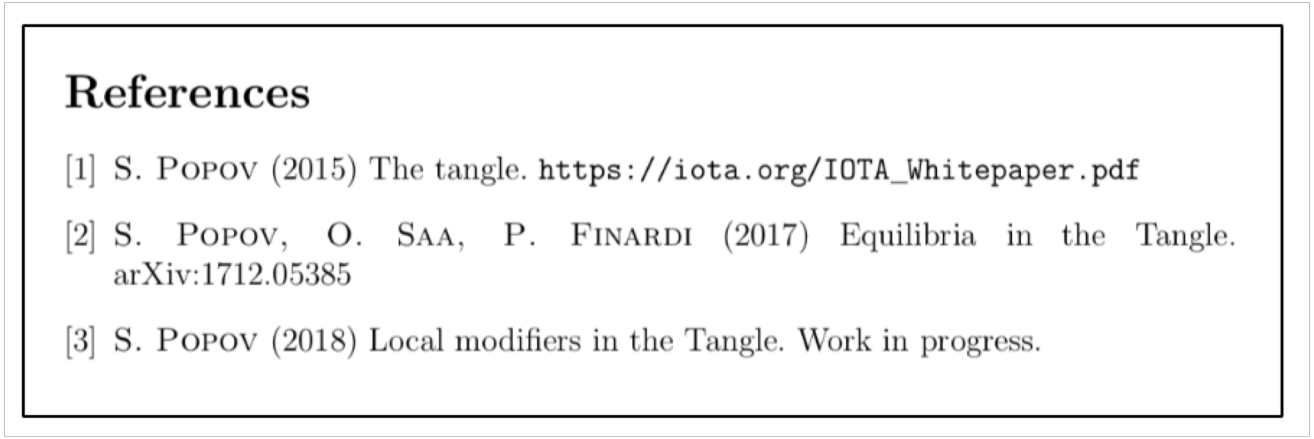
1 Introduction

1.1 Disclaimer

The following results are **preliminary** and **should by no means be taken at face value**, as this is only

III) IOTA Performance
C) Unprotected Attacks - Red Flags

- Some publication gems:



References

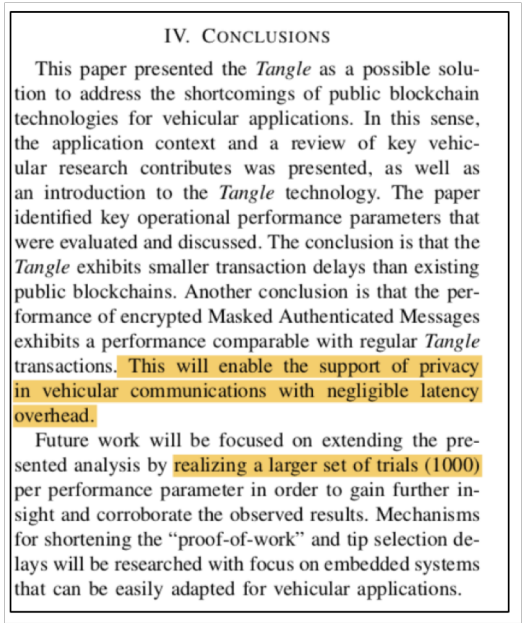
[1] S. Popov (2015) The tangle. https://iota.org/IOTA_Whitepaper.pdf

[2] S. Popov, O. Saa, P. Finardi (2017) Equilibria in the Tangle. arXiv:1712.05385

[3] S. Popov (2018) Local modifiers in the Tangle. Work in progress.

III) IOTA Performance
C) Unprotected Attacks - Red Flags

- Some publication gems:



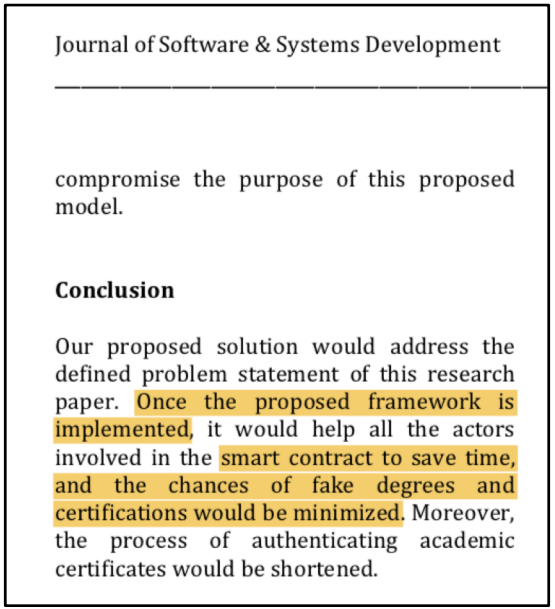
IV. CONCLUSIONS

This paper presented the *Tangle* as a possible solution to address the shortcomings of public blockchain technologies for vehicular applications. In this sense, the application context and a review of key vehicular research contributes was presented, as well as an introduction to the *Tangle* technology. The paper identified key operational performance parameters that were evaluated and discussed. The conclusion is that the *Tangle* exhibits smaller transaction delays than existing public blockchains. Another conclusion is that the performance of encrypted Masked Authenticated Messages exhibits a performance comparable with regular *Tangle* transactions. This will enable the support of privacy in vehicular communications with negligible latency overhead.

Future work will be focused on extending the presented analysis by realizing a larger set of trials (1000) per performance parameter in order to gain further insight and corroborate the observed results. Mechanisms for shortening the "proof-of-work" and tip selection delays will be researched with focus on embedded systems that can be easily adapted for vehicular applications.

III) IOTA Performance
C) Unprotected Attacks - Red Flags

- Some publication gems:



Journal of Software & Systems Development

compromise the purpose of this proposed model.

Conclusion

Our proposed solution would address the defined problem statement of this research paper. Once the proposed framework is implemented, it would help all the actors involved in the smart contract to save time, and the chances of fake degrees and certifications would be minimized. Moreover, the process of authenticating academic certificates would be shortened.

IV) Conclusion

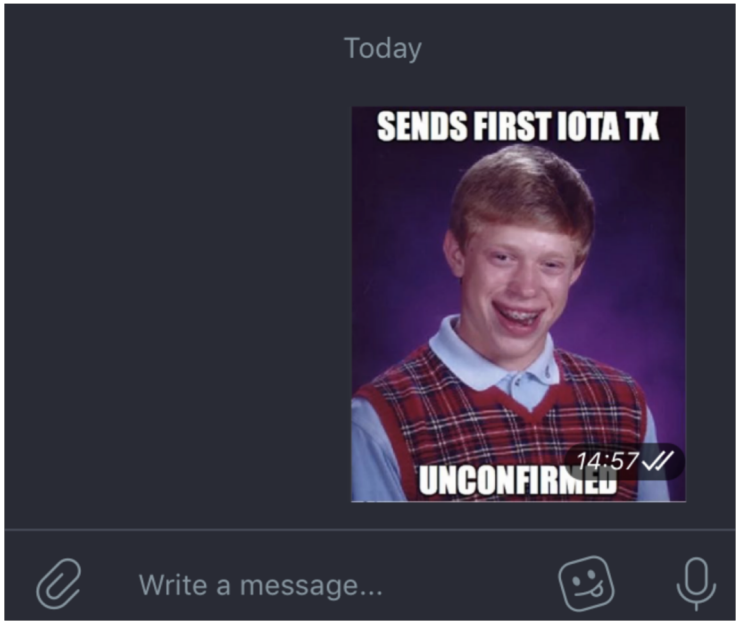
IOTA concepts covered:

- The Tangle Architecture
- Incentive
- Consensus
- Stability
- Smart Contracts
- Scalability
- Decentralisation
- Attacks, Vulnerabilities & Privacy

IV) Conclusion

So… has our ‘free’ transaction gone through in one hour?

IV) Conclusion




IOTA
Questions?