CS 731: Blockchain Technology And Applications

Sandeep K. Shukla

IIT Kanpur

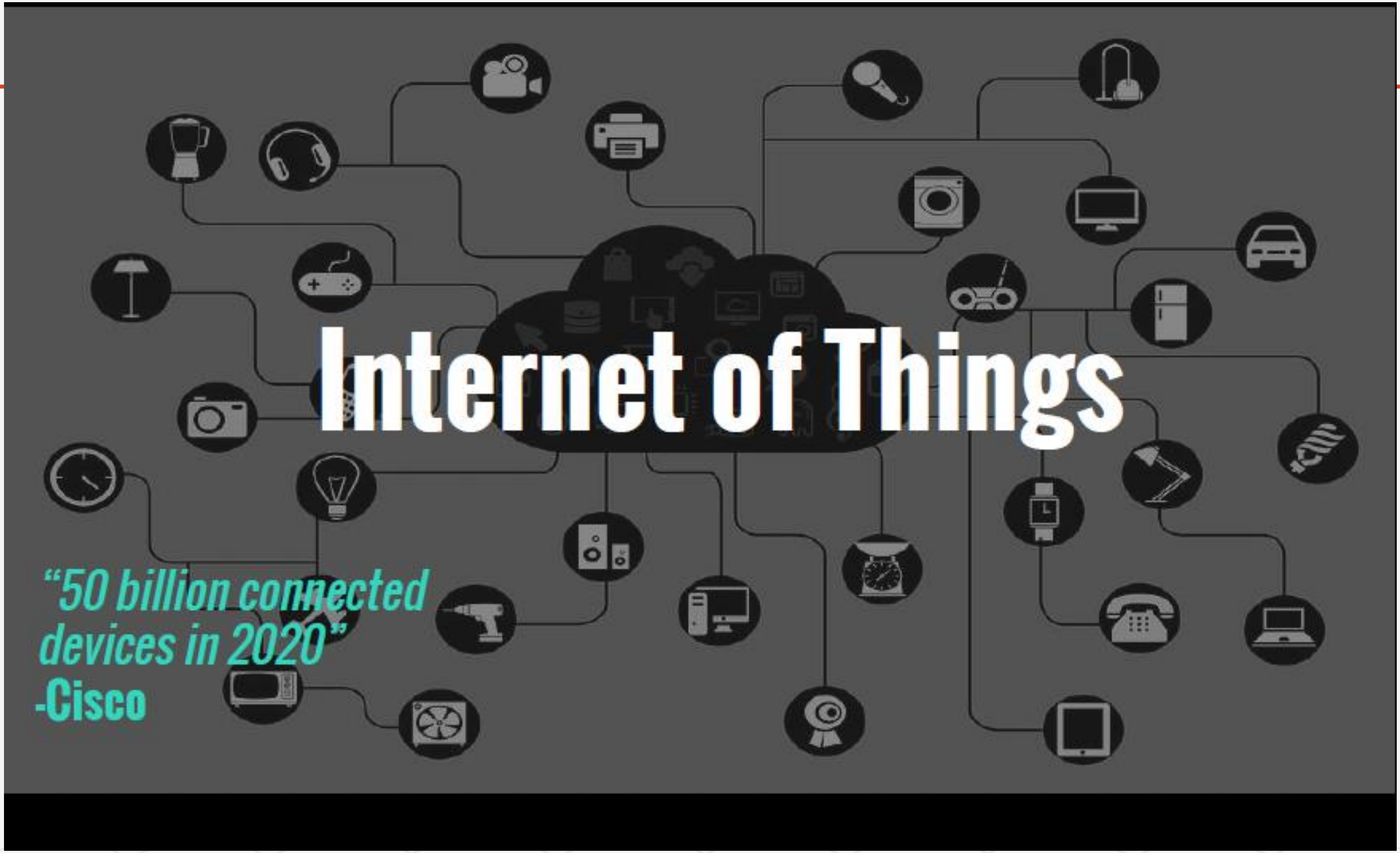
C3I Center

Acknowledgements

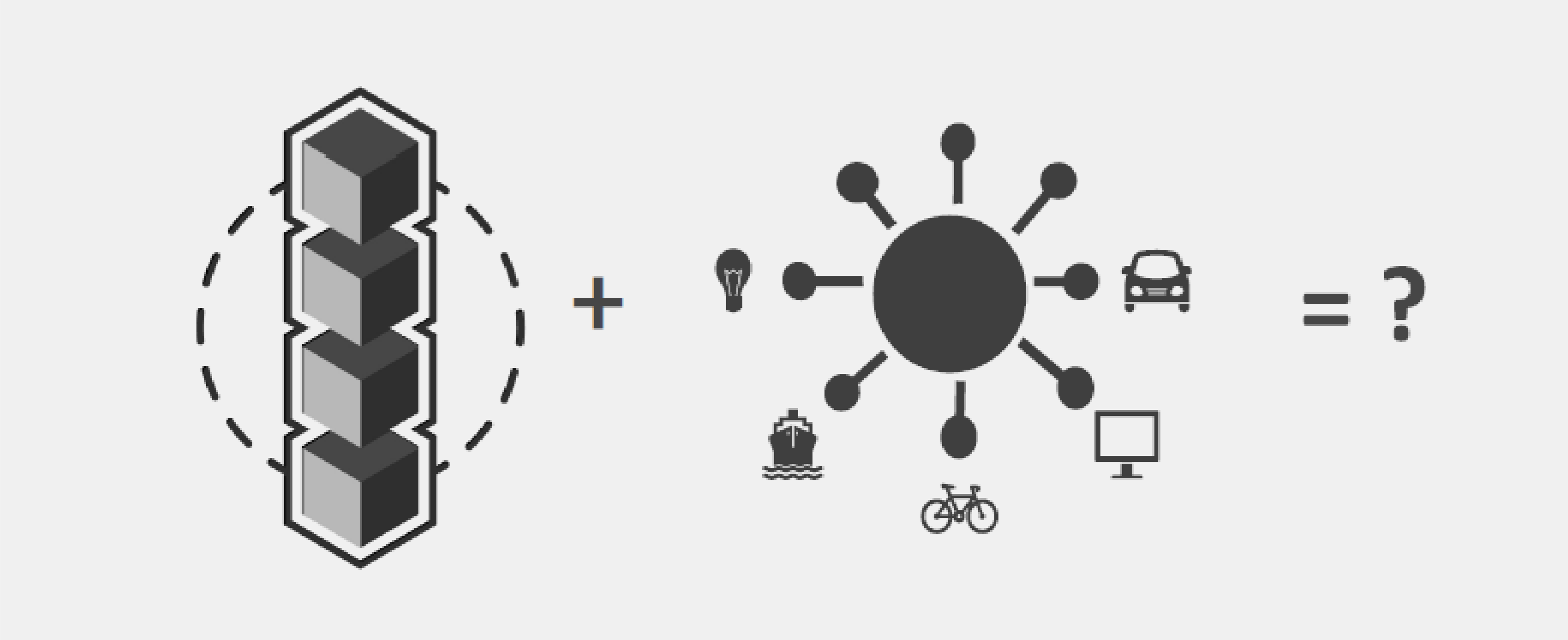
- Bennet Breier, TUM
- IOTA Foundation
- Alon Gal

IOTA

Transactions, Confirmation And Consensus


Internet of Things
“50 billion connected devices in 2020”
-Cisco

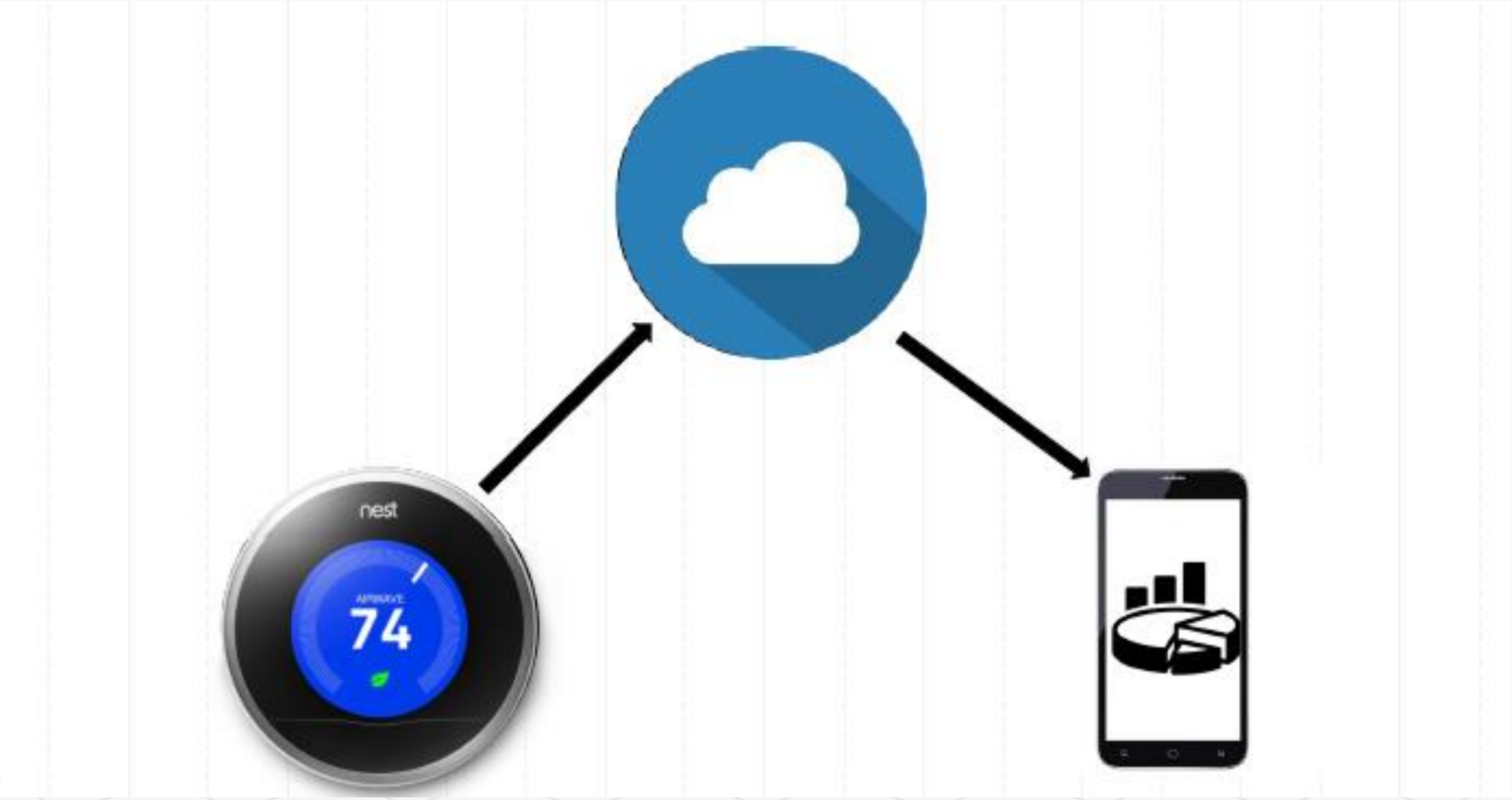
Blockchain and IoT



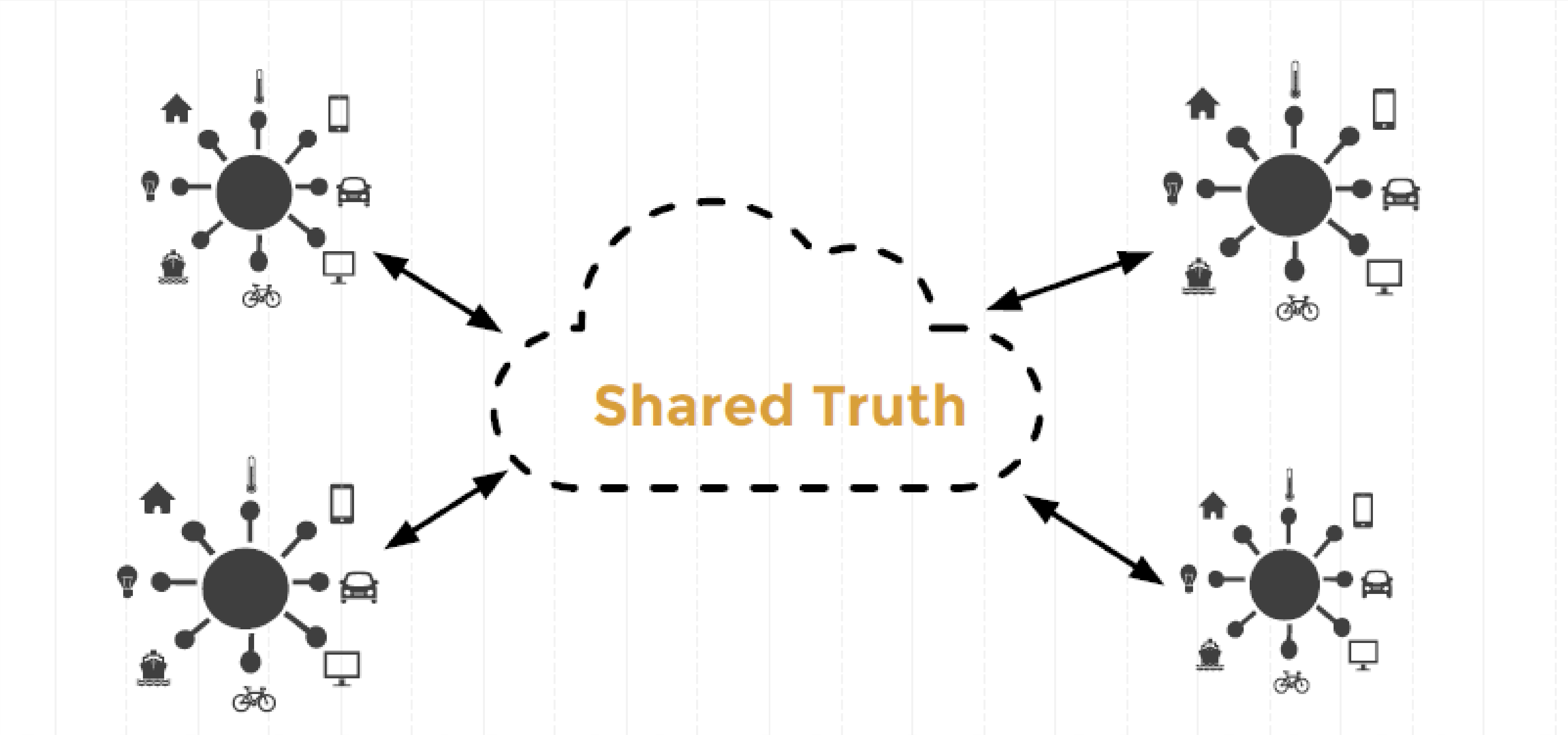
IoT – Internet of Things

- Examples
  - Smart City
  - Smart Home
  - Smart Grid
  - Smart Transportation
- What is enabling information technology?
  - IoT components must talk to each other M2M to share information
  - Visibility of the State of the system or subsystem as a whole for autonomous decision making
  - Cloud based IoT ecosystem proposed by many companies
  - All IoT devices communicate to the cloud and get global state info from the cloud
  - Often communicate via cloud

Cloud + IoT



Single Shared Truth for Everyone



What’s the problem with Cloud + IoT

- Single point of failure
- Data Integrity and confidentiality at stake
- Cyber attack on the cloud
- Cloud infrastructure provider gets enormous power and data
- Can we decentralized this?
  - Blockchain anyone?

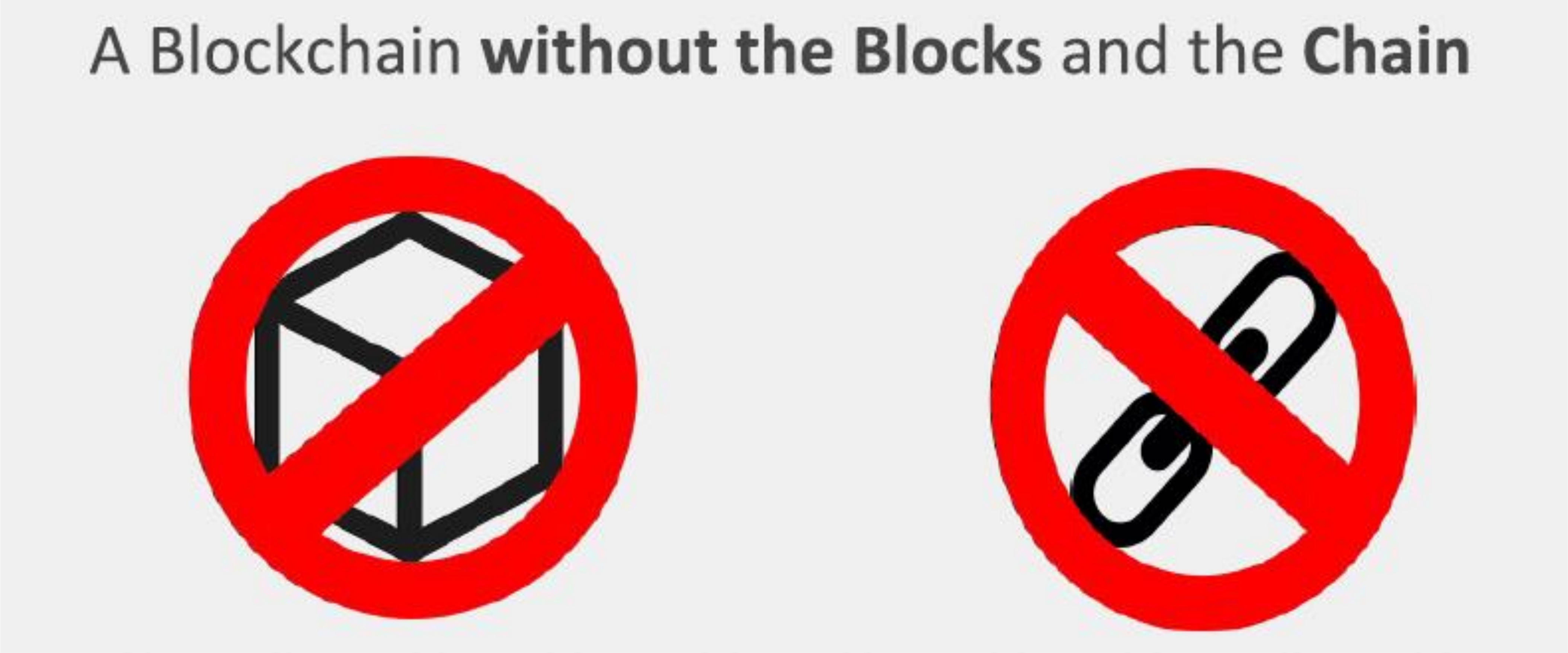
IoT + Blockchain

- Existing Blockchain (Bitcoin, Ethereum etc)
  - Scalability issues
  - PoW computational requirement
  - Centralization by powerful miners
  - Cost of transactions
  - All guarantees of integrity is probabilistic
  - Privacy requires a bit more thought
- IoTA foundation claims to have a solution
  - Replace Blockchain by Tangle
  - It borrows a lot of ideas from Blockchain
    - But not exactly a blockchain

Requirements of IoT

- Low Resource Consumption
- Widespread Interoperability
- Billions of Nano-transactions
- Data Integrity

The Tangle



A Blockchain **without the Blocks** and the **Chain**

Tangle

- No block – individual transactions are tangled together
- What is Tangling
  - Construct Directed Acyclic Graphs (DAGs) connecting transactions
- Self Regulating
- Very Scalable
- Still use PoW – but a long overhead PoW
  - Prevent spamming

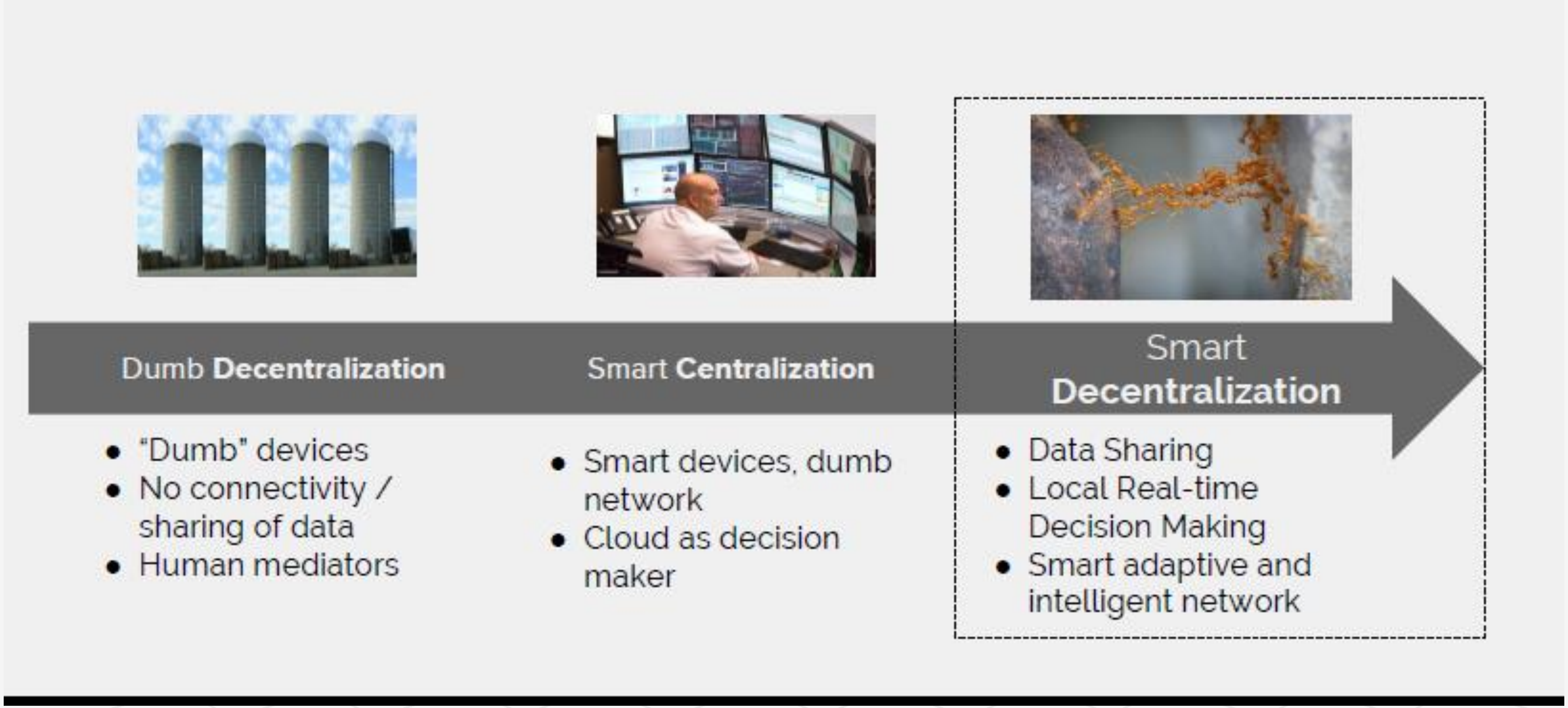
What we get out of Tangle in place of Blockchain?

- CAP
  - Consistency
  - Availability
  - Partition-Tolerance
- No Fees
- Scalable
- Modular
- Lightweight
- Offline allowed
- Quantum Proof

Envisioned Use cases

- Complete M2M communication
  - Anything which has computational resource (Chip) can be leased by another machine autonomously
  - Devices can share resources by coordinating – bandwidth sharing for example
  - Supply Chain
  - Smart Grid to coordinate production of energy without human dispatching
  - On-demand API access
  - Sensor Data Selling and Data Market Place
  - ….

Towards Smart Decentralization



Dumb **Decentralization**

- "Dumb" devices
- No connectivity / sharing of data
- Human mediators

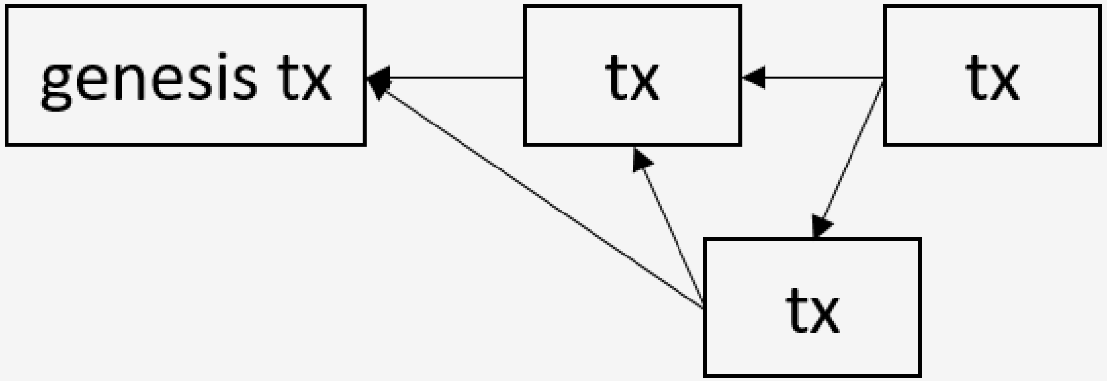
Smart **Centralization**

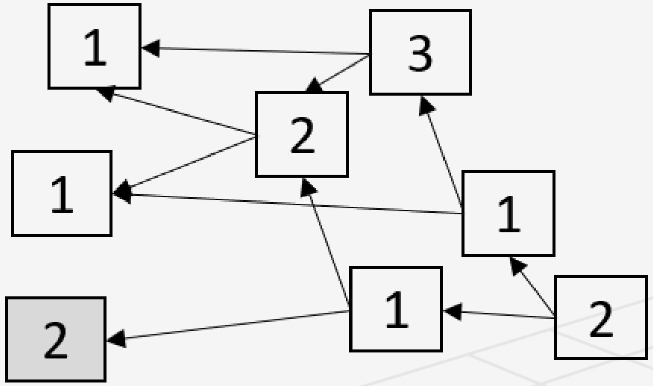
- Smart devices, dumb network
- Cloud as decision maker

Smart **Decentralization**

- Data Sharing
- Local Real-time Decision Making
- Smart adaptive and intelligent network

Tangle Initialization & Transaction Issuance





Cumulative Weight = 5

https://public-rdsdavdrpd.now.sh/

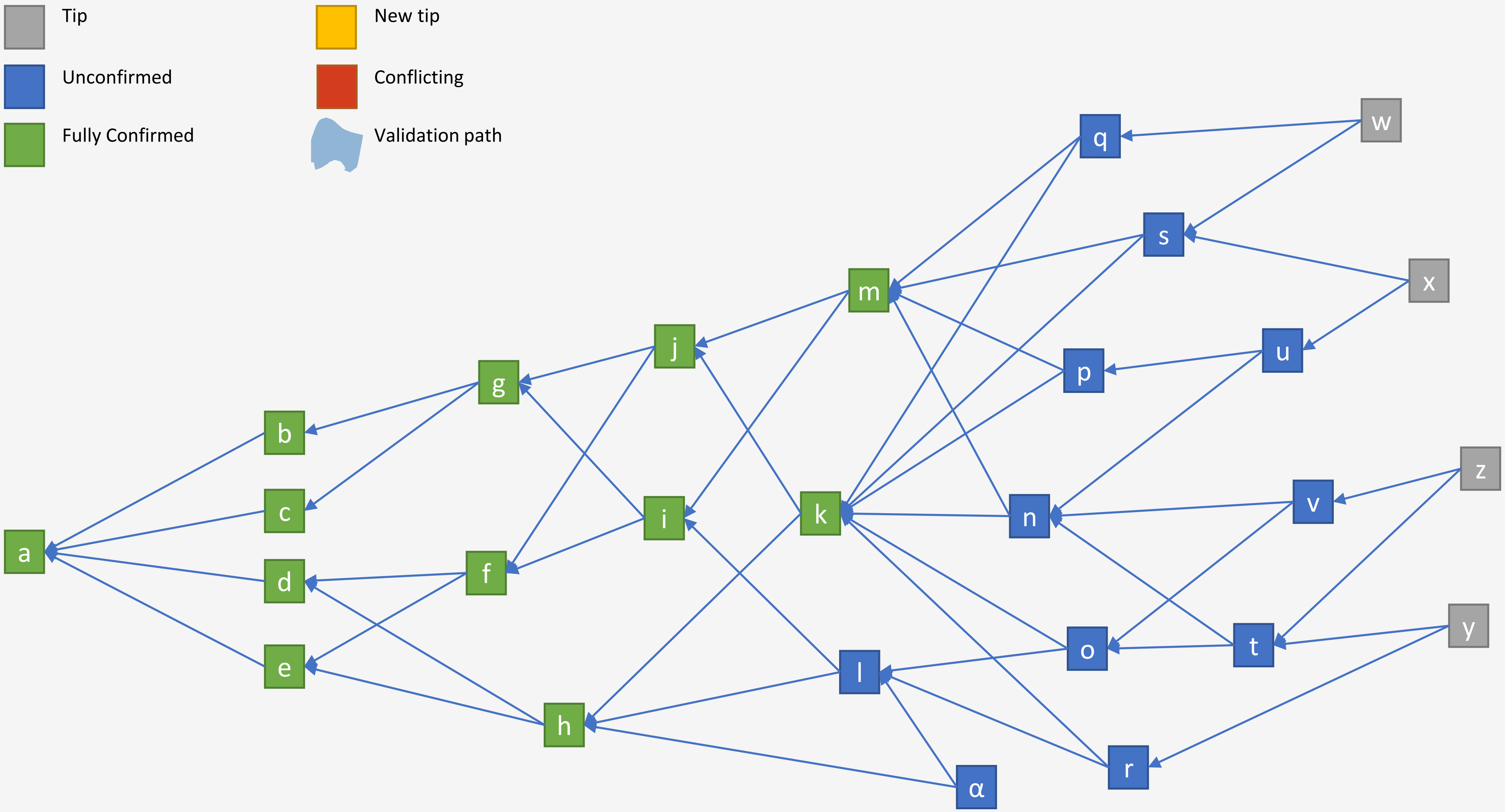
Issuing a Transaction

1. Bundling & Signing
2. Tip Selection
3. Validation
4. Proof-of-Work (PoW)
5. Publishing

Simulations

- Simulation by varying λ (transaction arrival rate – Poisson process)
  - https://public-rdsdavdrpd.now.sh/
- Simulation of unweighted random walk based tip selection
  - https://public-xnmzdqumwy.now.sh/
- Simulation of weighted random walk based tip selection
  - https://public-qnbiiqwyqj.now.sh/
- Simulation of Confirmation Confidence Computation
  - https://public-krwdbaytsx.now.sh/
  -

Initial Tangle State



Adding A Transaction

⬜ Tip

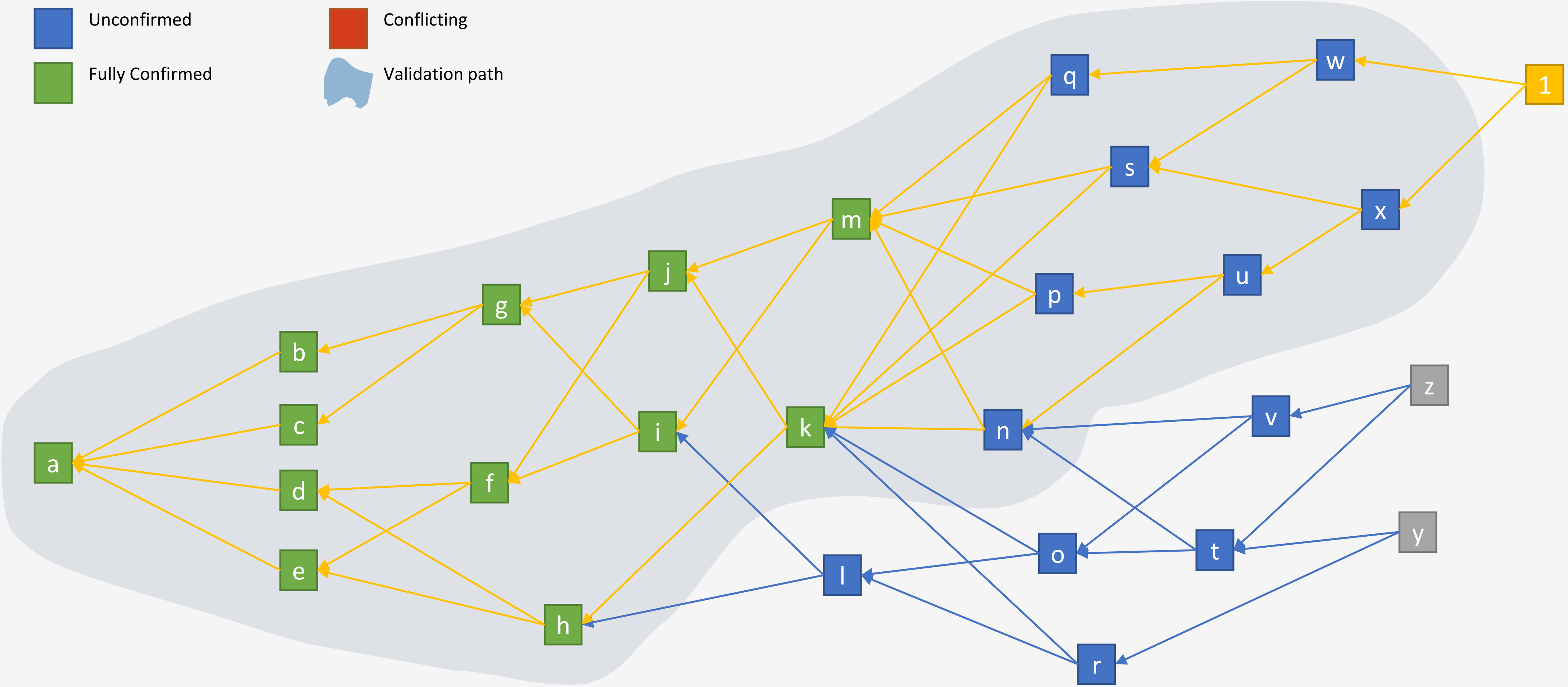
🟦 Unconfirmed

🟩 Fully Confirmed

🟨 New tip

🟥 Conflicting

Validation path



Another Transaction

⬜ Tip

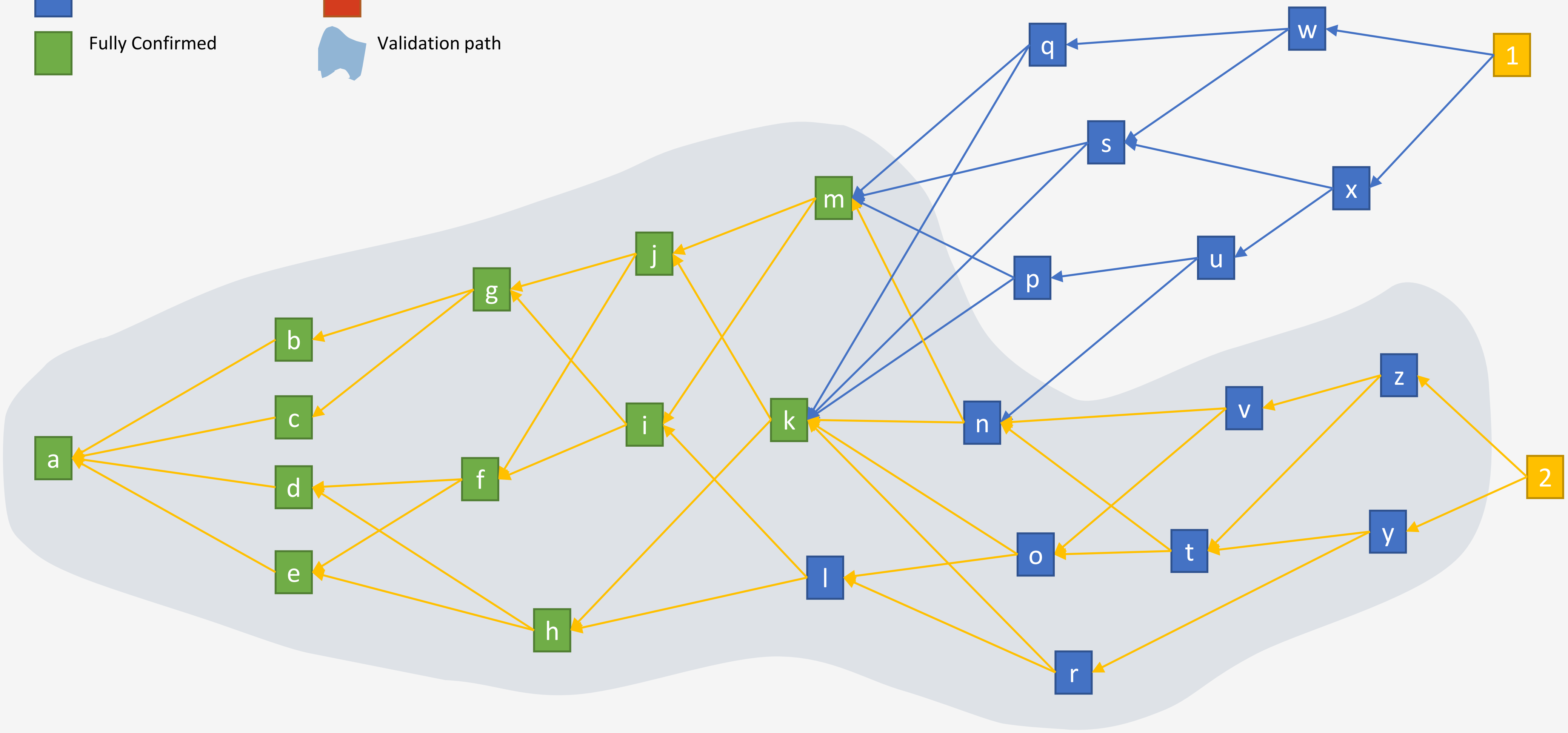
🟨 New tip

🟦 Unconfirmed

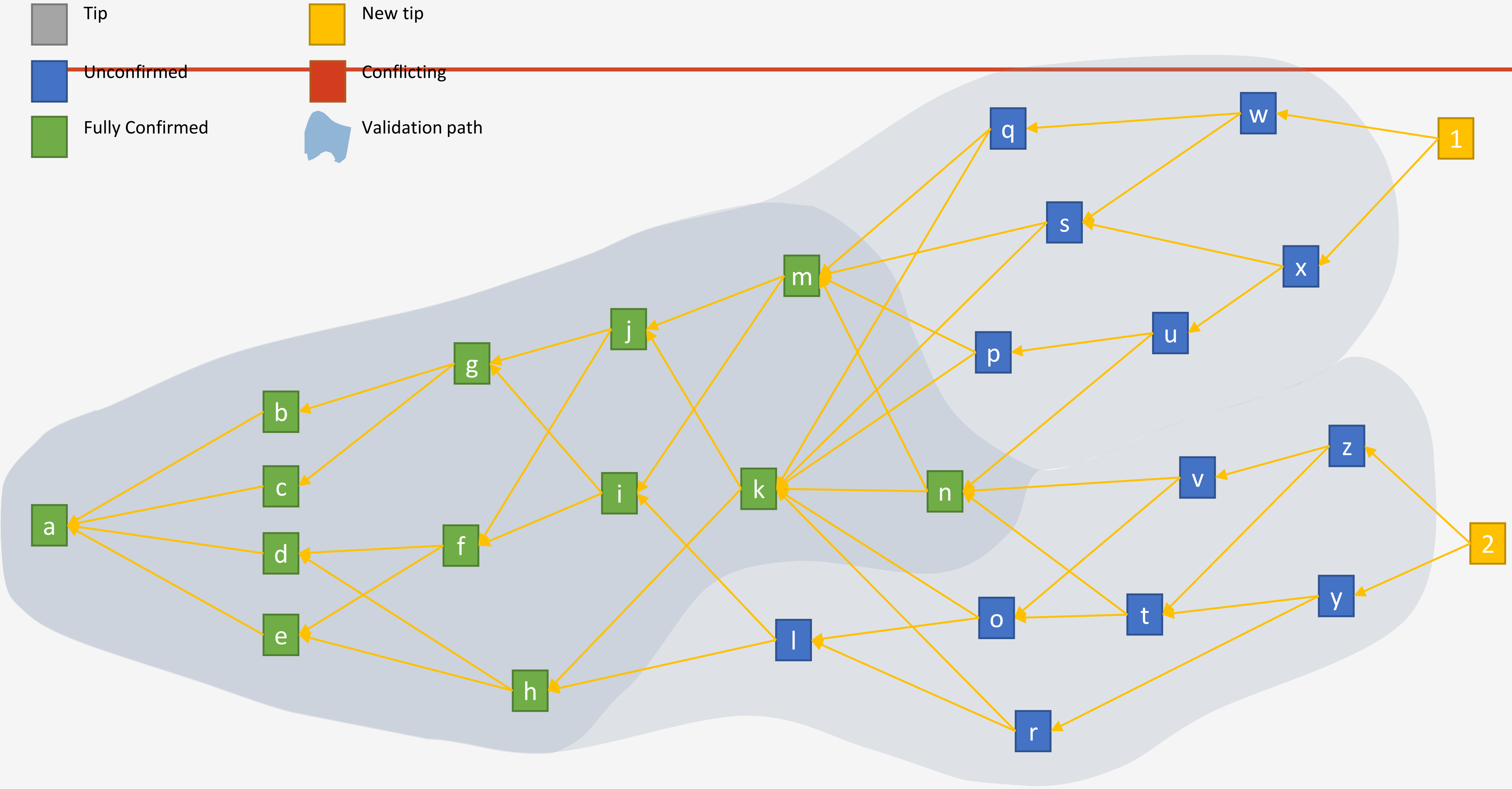
🟥 Conflicting

🟩 Fully Confirmed

Validation path



New Tangle State



⬜ Tip

🟨 New tip

🟦 Unconfirmed

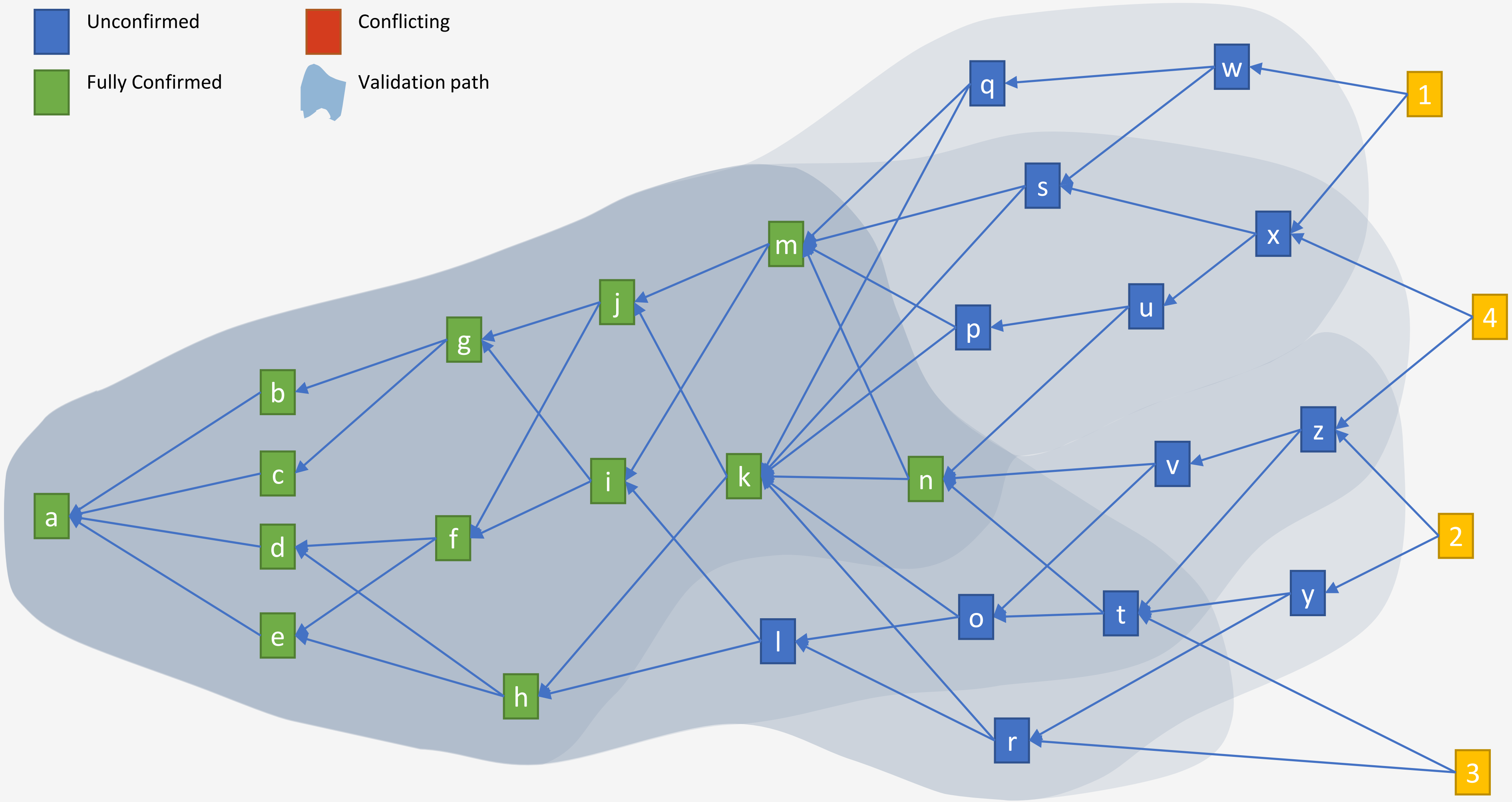
🟥 Conflicting

🟩 Fully Confirmed

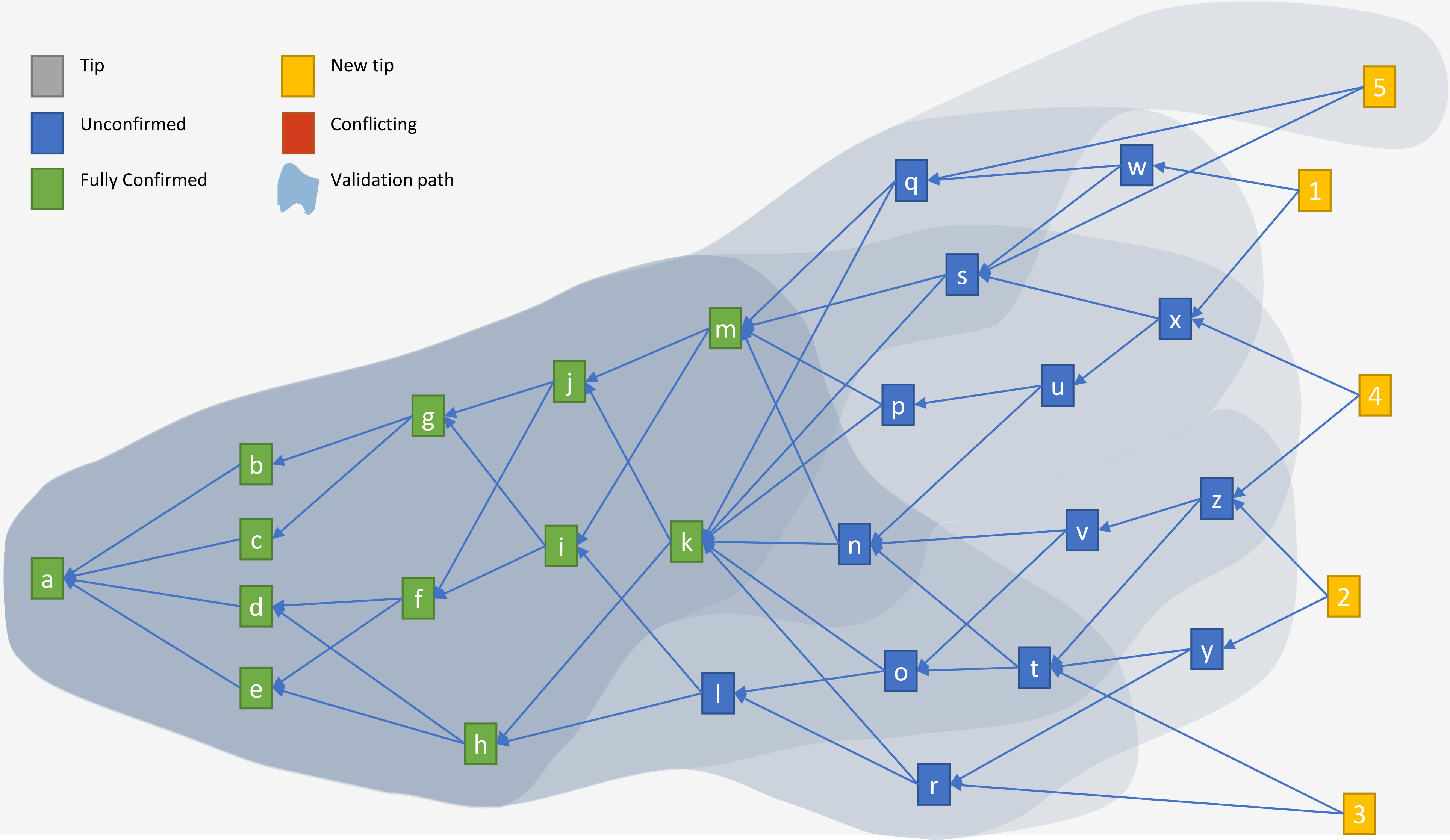
▨ Validation path

Confirmation Levels

- ⬜ Tip
- 🟦 Unconfirmed
- 🟩 Fully Confirmed
- 🟨 New tip
- 🟥 Conflicting
- Validation path



Propagation Delay



- ⬜ Tip
- 🟦 Unconfirmed
- 🟩 Fully Confirmed
- 🟨 New tip
- 🟥 Conflicting
- ▨ Validation path

Double Spend

⬜ Tip

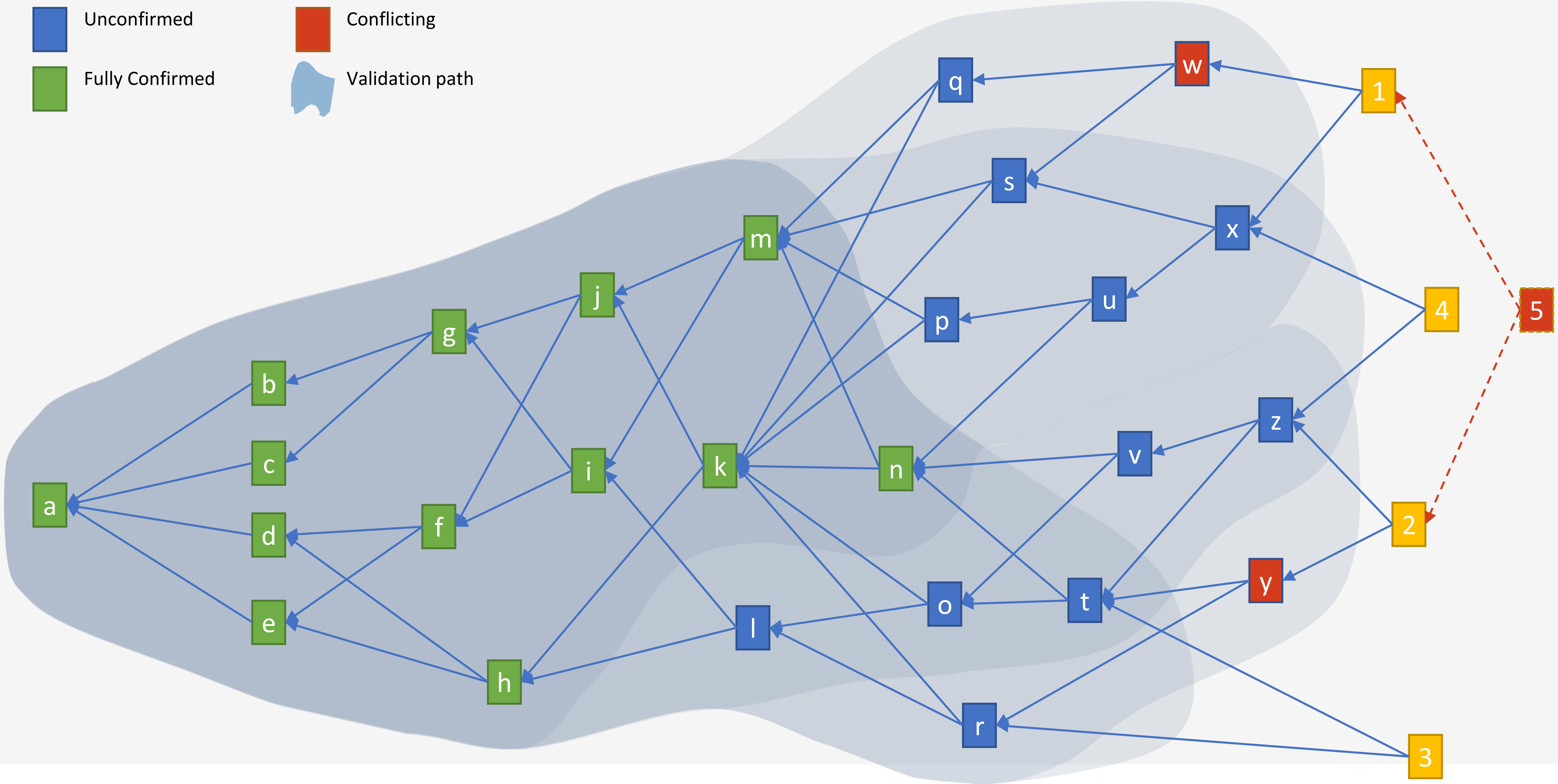
🟨 New tip

🟦 Unconfirmed

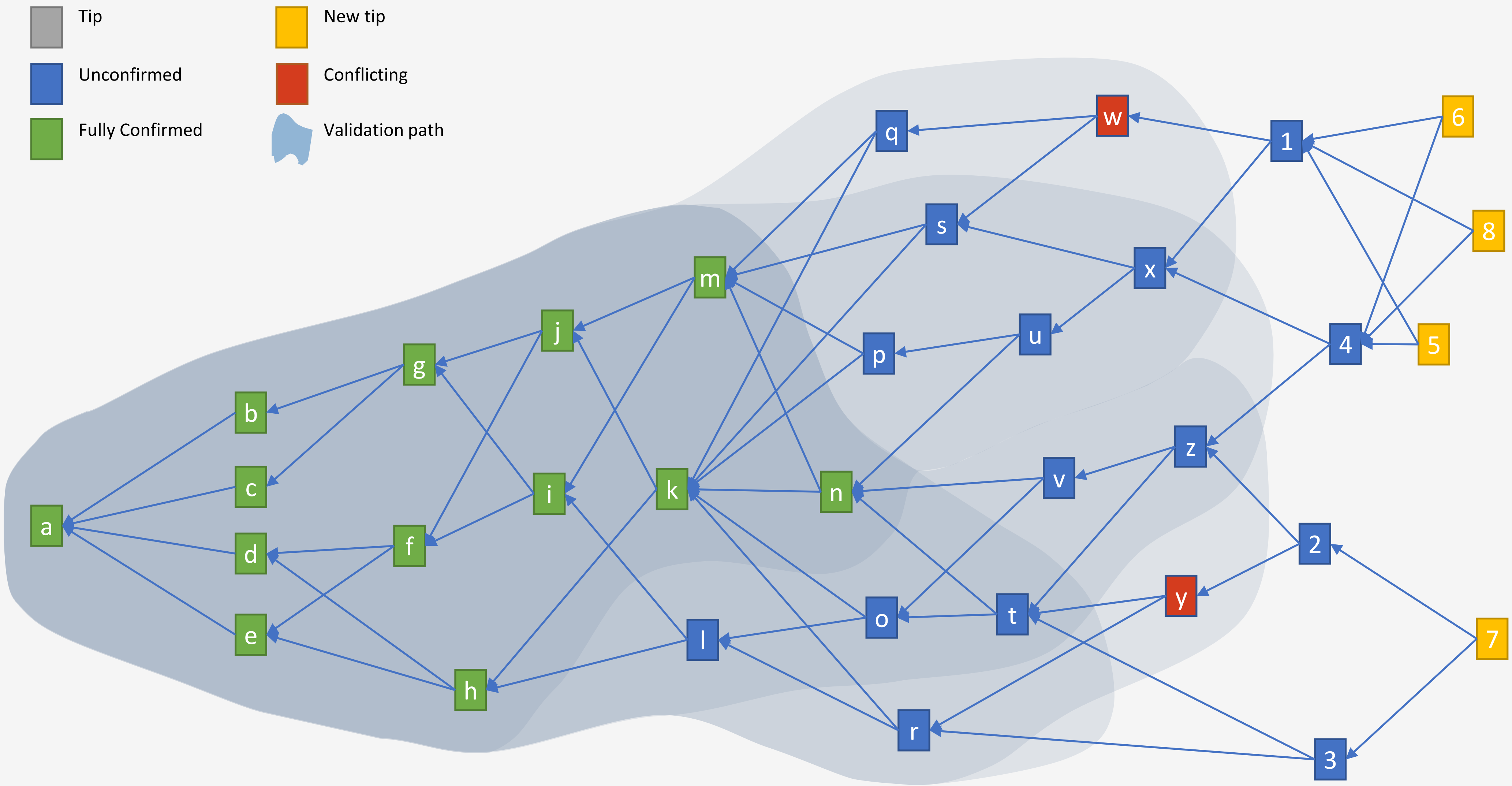
🟥 Conflicting

🟩 Fully Confirmed

▨ Validation path

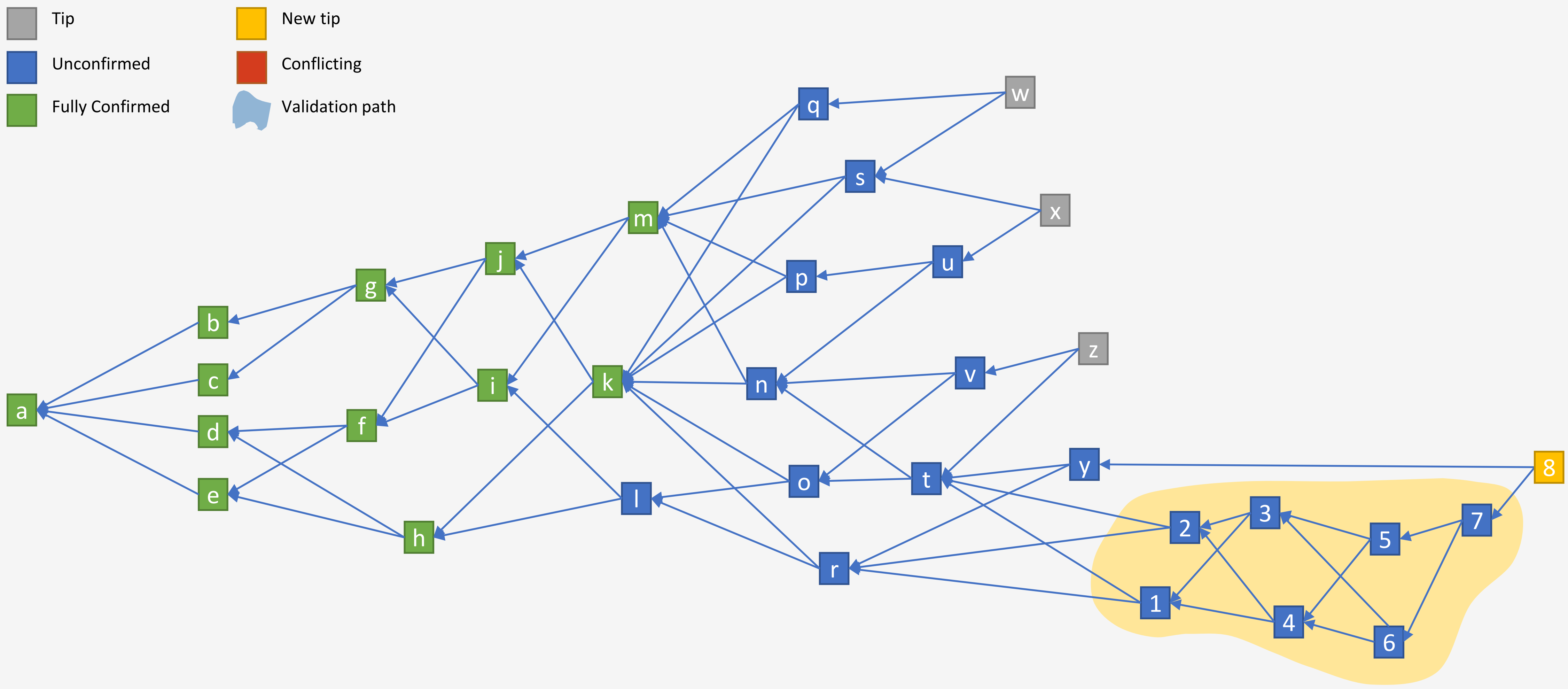


Double Spend Resolution



- ⬜ Tip
- 🟦 Unconfirmed
- 🟩 Fully Confirmed
- 🟨 New tip
- 🟥 Conflicting
- Validation path

Offline Tangle



⬜ Tip

🟦 Unconfirmed

🟩 Fully Confirmed

🟨 New tip

🟥 Conflicting

Validation path