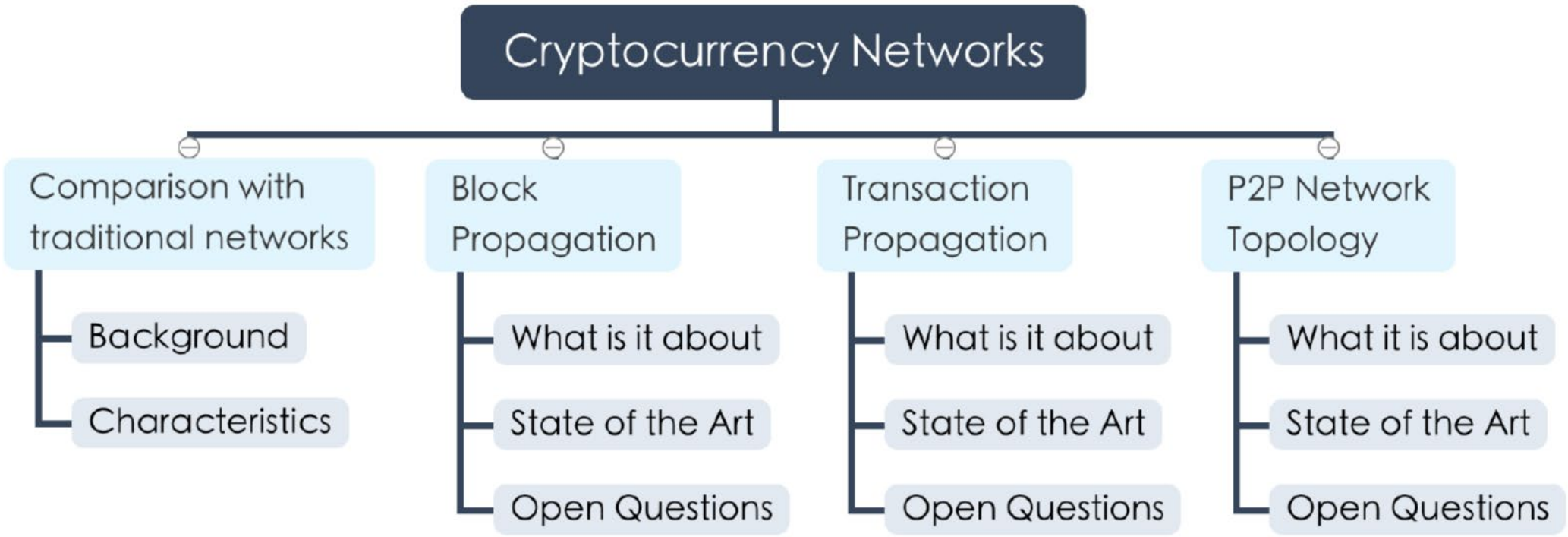
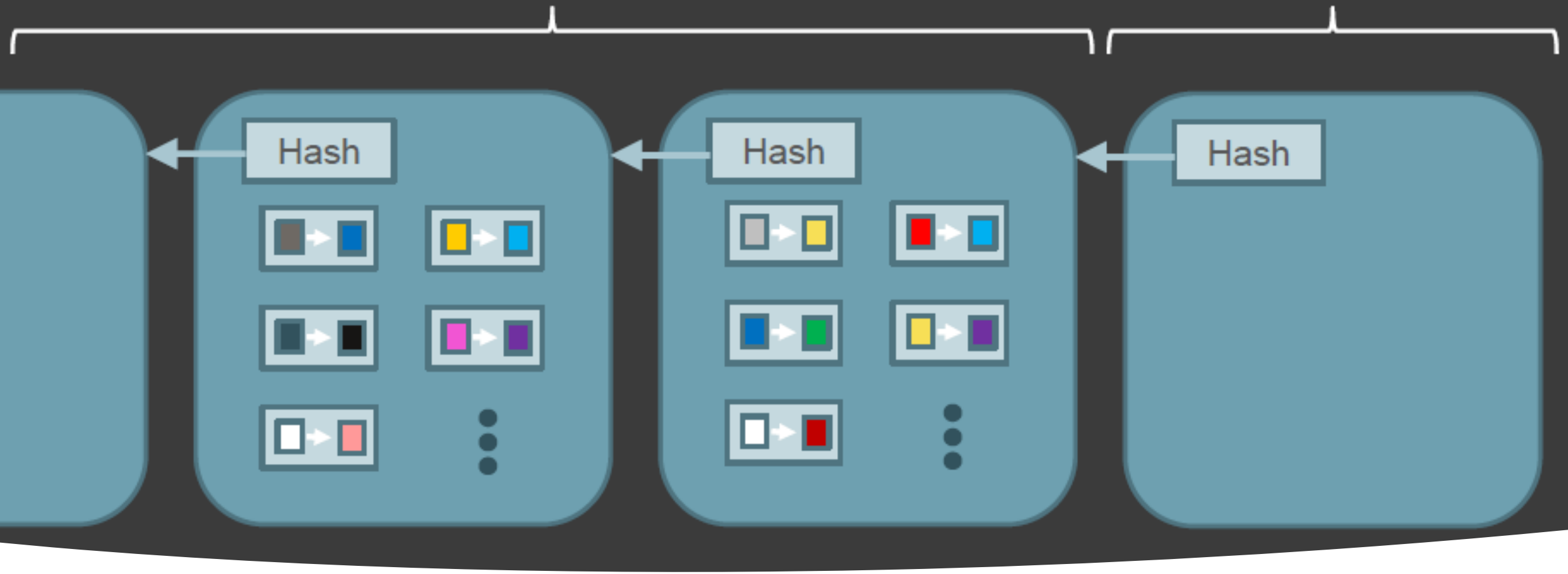
Cryptocurrency Networking: Context, State-of-the-Art, Challenges

Maya Dotan[1]
Yvonne-Anne Pignolet[2]
Saar Tochner[1]
Stefan Schmid[3]
Aviv Zohar[1]

[1] The Hebrew University of Jerusalem, [2] DFINITY, [3] Faculty of Computer Science, University of Vienna

Agenda


Cryptocurrency Networks
Comparison with traditional networks
Background
Characteristics
Block Propagation
What is it about
State of the Art
Open Questions
Transaction Propagation
What is it about
State of the Art
Open Questions
P2P Network Topology
What it is about
State of the Art
Open Questions

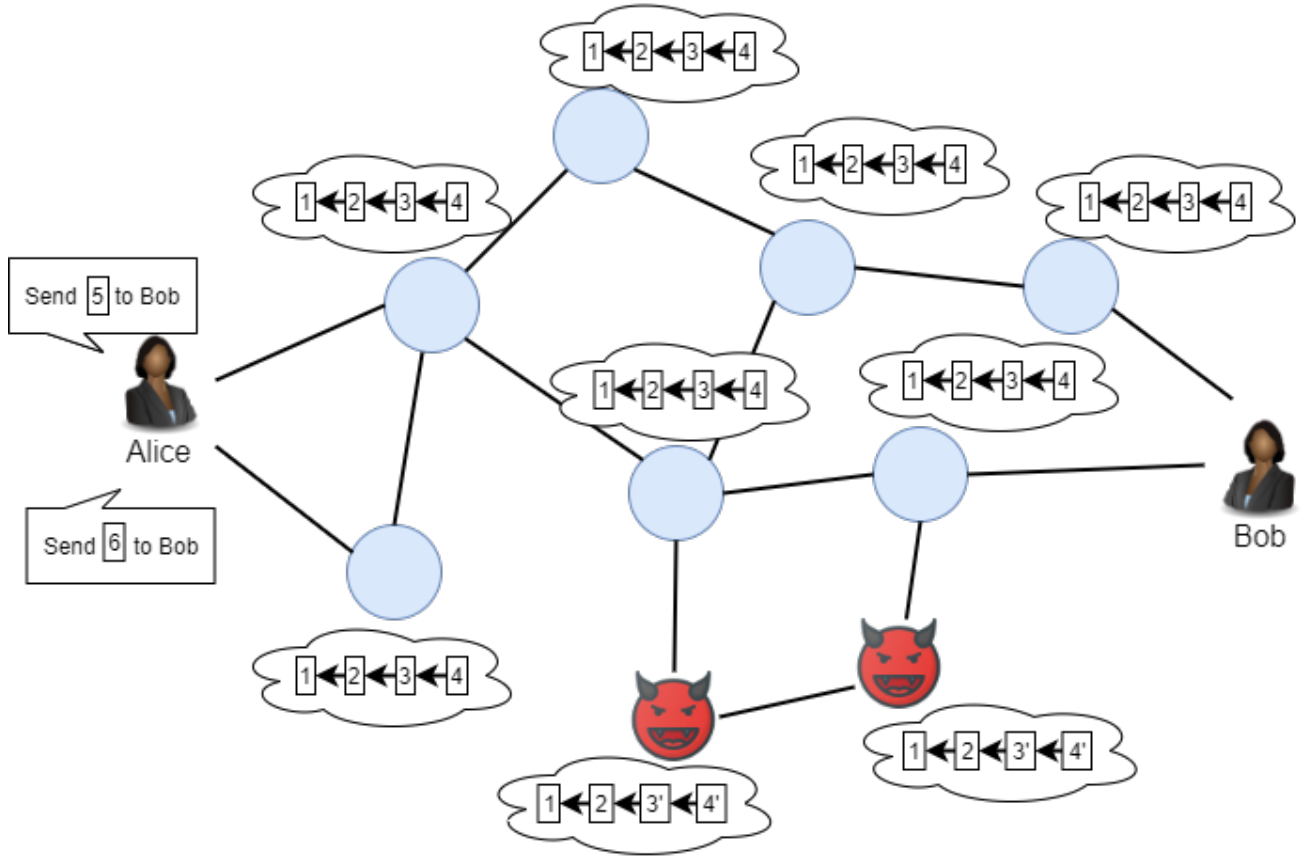


The Blockchain

- Transactions are stored in Blocks
- Every block is labeled with a cryptographic hash of the previous block
- Block size and rate are bounded (Bitcoin -~1MB, Block ~ 10 min)
- block size is small → Limited throughput

P2P

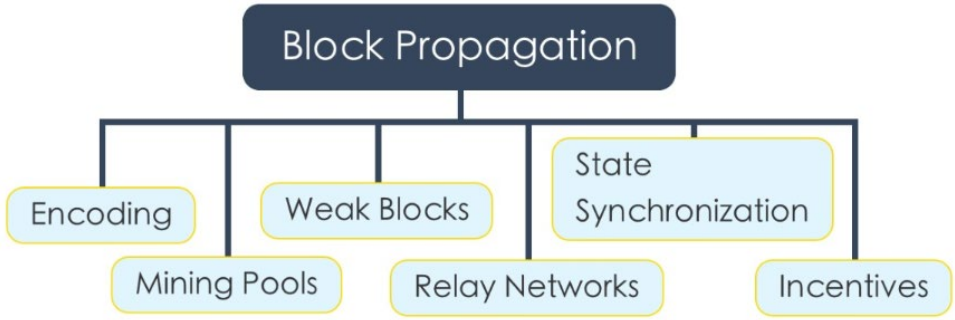
- Users:
  1. create and propagate transactions
  2. validate blocks
- Miners:
  1. Create Blocks
  2. Include Tx's in Blocks for a fee
  3. Propagate block to entire network.



Characteristics of Cryptocurrency Networks

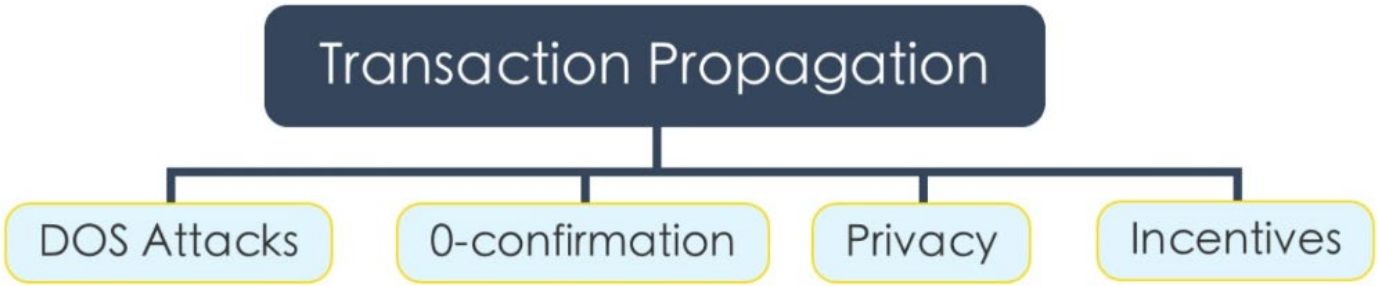
- Incentives – trustless system thus need to incentivize nodes to follow the protocol
- Communication pattern – Bursts of information (Block), Repetitive
- Network topology – Built incrementally vs. dictated
- Security – Depends on fast propagation
- Performance – network in scale (Benchmark: Visa – 2000 tx/s)

BLOCK PROPAGATION



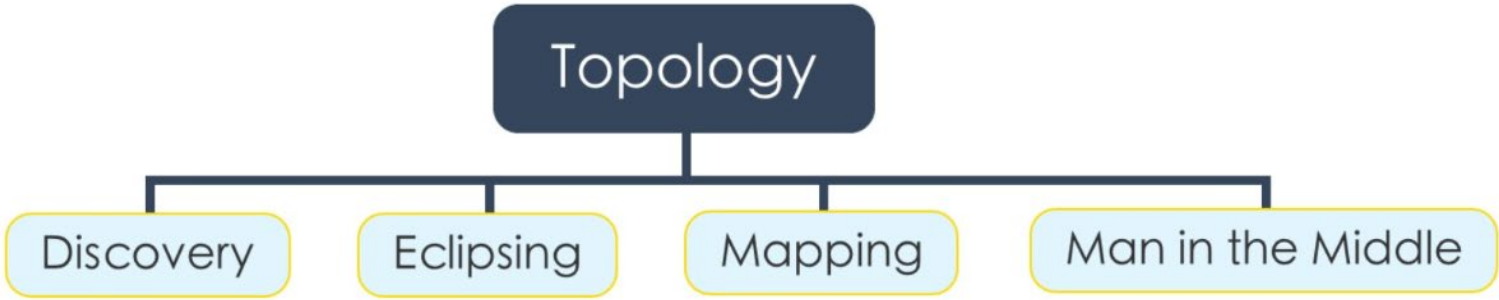
- How to accelerate block propagation?
- How to incentivize mining blocks with many valid transactions?
- How to broadcast blocks within a pool?
- How to get headers to miners quickly (topology-wised)?
- How to monitor pools?

TRANSACTION PROPAGATION



- How to avoid transaction floods?
- How to balance DOS prevention and 0-confirmation requirement?
- How to model and analyze cryptocurrencies?
- How to implement a suitable reward system?

TOPOLOGY OF THE P2P NETWORK



- Should the topology be hidden? How to balance routing efficiency and prevent eclipse/hijacking attacks?
- How to create a single component of all the honest nodes?
- How to model link failures?

Conclusion

Open Question	Methodologies
How to accelerate block propagation?	PROT, ALG, GAME, SEC, CRYPTO
How to incentivise mining blocks with many valid transactions?	GAME
How to broadcast blocks within a pool?	ALG, PROT
Efficient network design for mining pools	PROT, ALG
Should pools be allowed?	GAME
How to avoid transaction floods?	SEC, GAME
How to balance DOS prevention and 0-confirmation requirements?	PROT, GAME, ALGP
How to model and analyse crypto currency?	PROT, GAME
How to implement a suitable reward system?	GAME
Topology information hiding	SEC, CRYPT, ALG
Giant honest component	ALG
Link failure models	PROT, ALG

Thanks!