Distributed Ledger Architecture Paradigms

How distributed ledger technology can solve real problems.

KING'S College LONDON

Moritz Platt, moritz.platt@kcl.ac.uk

Solutions Engineering Team Lead, R3

PhD Student, King's College London

Agenda

1. **I see what you see**—Any implementation of distributed ledger technology (DLT) or blockchain serves the purpose of state machine replication.

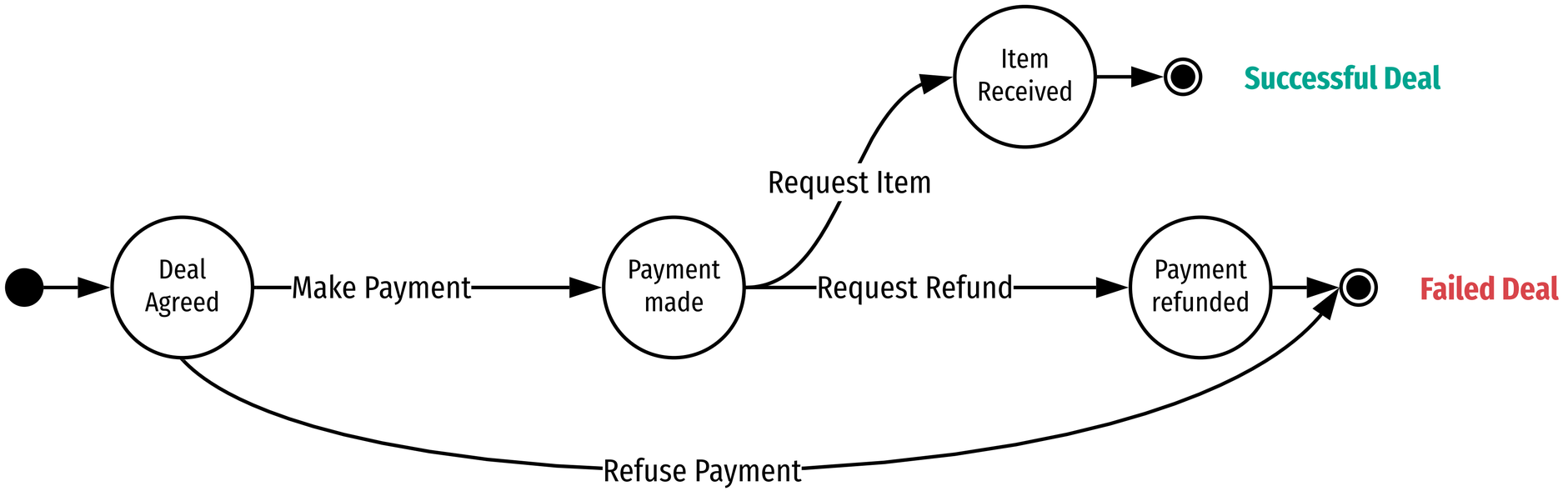
2. **Horses for Courses**—Do you need a blockchain? Mapping business cases to architectural paradigms and why it's important to get it right at the beginning.

3. **Network Performance**—There are different measures for system performance in distributed systems. Counterintuitively, privacy can benefit network-level throughput.

4. **Academia and Industry on DLT Innovation**—The research agenda in permissioned and permissionless systems and the demand seen in the industry.

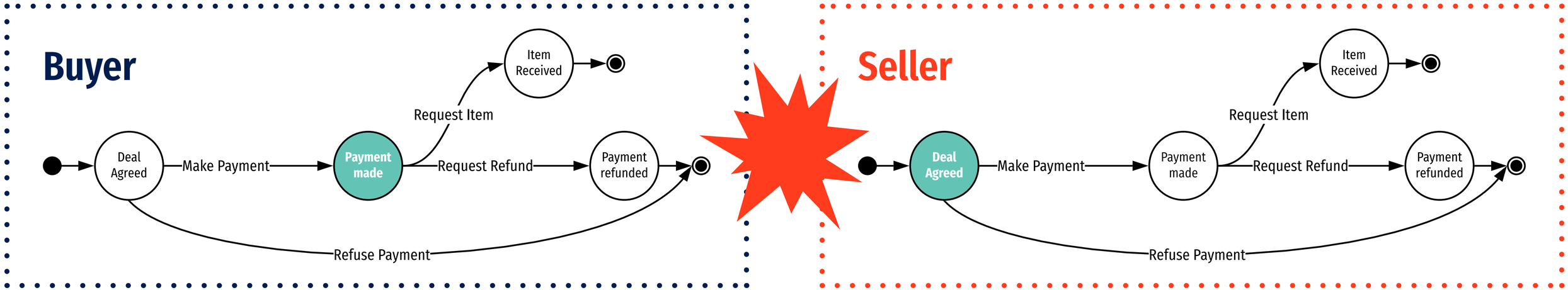
Finite State Machines

- In automata theory, *a machine, or a model of a machine, that is capable of assuming only a finite number of **states** and **transitions** between these states.* *[Weik2017]*
- This helps a formal understanding of the allowed states a computer system can be in.
- Interactions—such as the buyer-seller relationship—can be modelled as state machines:



State Machine Replication

- State machines help to model isolated systems
- Can they explain distributed systems too?



- Synchronising transistions between (distrusting) systems is the core problem DLT solves
- Is the actor *allowed* to perform an action?
- How do we *synchronise* this state change with everyone who needs to know?

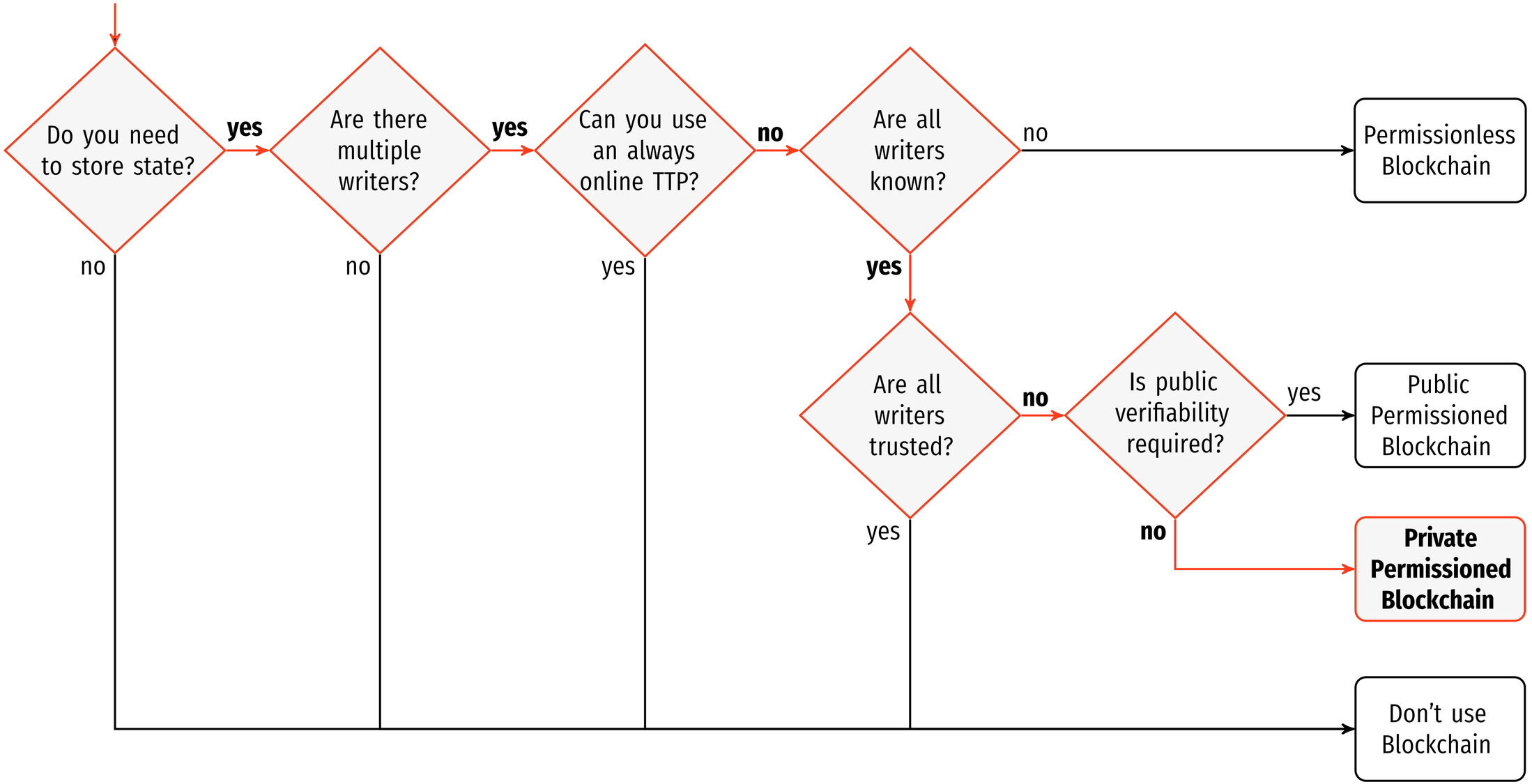
State Machine Replication

- Different DLT platforms implement SMR in different ways. Key differences are:
  - **Smart Contract Implementation:** How can participants encode what constitutes a legal transition?
  - **Consensus Protocol:** How is a joint understanding on whether a transition was legal is reached?
  - **Network:** Who needs to evaluate a given transition for validity.
  - **Synchronisation:** How is it ensured that at all times participants have a correct/up-to-date view of all relevant states.

The Two Dimensions of DLT

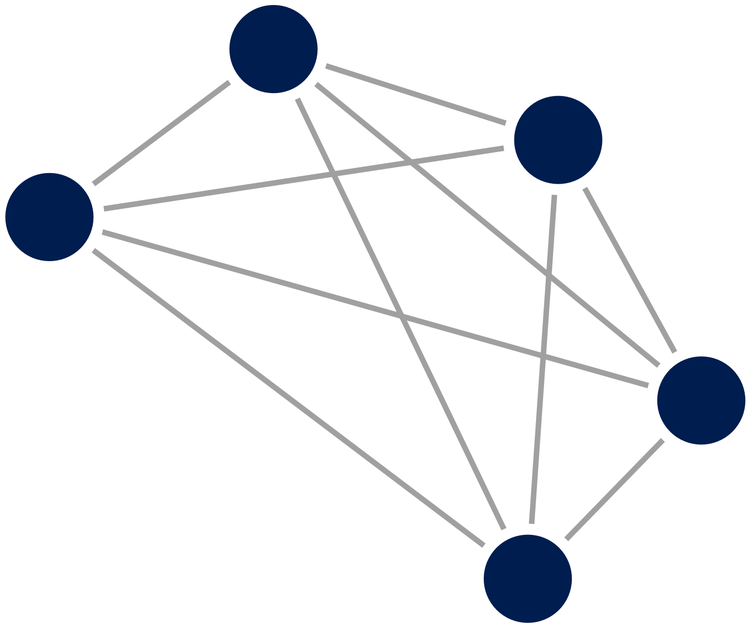
- Permissioned versus Permissionless (Consensus)
  - In a permissionless system anyone can *contribute to network consensus*
  - Most prominent approach: ‘Proof-of-Work’
  - In a permissioned system an approved group validates transactions
- Public versus Private (Participation)
  - A public DLT system is open for everyone to participate in
  - A private system only allows invited parties to participate

Do you need a blockchain? [Wuest2018]



Public Permissionless Blockchains

- Bitcoin, Ethereum
- Based on **Satoshi Nakamoto**'s original idea of a peer-to-peer electronic cash system that hashes transactions into an ongoing chain using hash-based proof-of-work [Nakamoto2008]
- ⊞ **Truly permissionless**: No need for participants with special positions
- ⊟ **Waste of Resources**: Mining Bitcoin/Bitcoin Cash has a significant energy footprint by causing 0.13% of global energy consumption [Jenkinson2017].

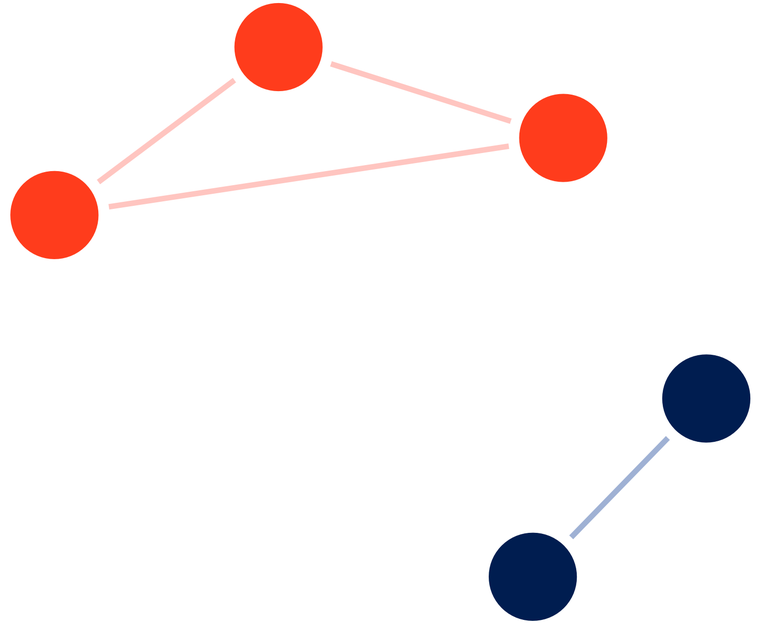


Public Permissionless Blockchains

- **Network inefficiency**: Experimental analysis shows that existing 'Proof-of-Work' blockchains are limited to throughputs of ~60 transactions per second [Gervais2016] even using optimal configurations.
- **Poor Privacy**: Behavior-based clustering techniques can unveil profiles of users, even if they try to enhance their privacy by manually creating new addresses [Androulaki2013].
- The fact that everyone can contribute to consensus means that settlement is probabilistic, not definitive.
- Smart contracts are difficult to reason about. Defects in smart contracts on public/permissionless chains cannot be remedied by conventional means based on the rule of law.

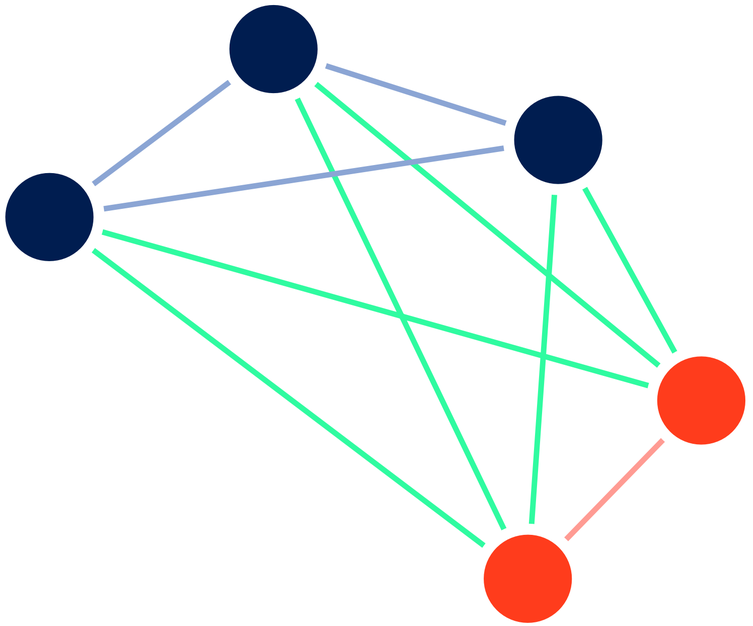
Siloed Permissioned Blockchains

- Hyperledger Fabric, Quorum
- **Hyperledger Fabric** uses pairwise ‘channels’ to enable privacy for multilateral transactions [Androulaki2018]
- **Quorum** is **Ethereum** based and implements privacy in a similar fashion, i.e. by splitting the larger public ledger into a public and a private ledger. The public ledger is visible to all nodes in the network, the private ledger is visible only to the transacting parties [Baliga2018]
- Difficult to reason about privacy implications and transferability of assets and states



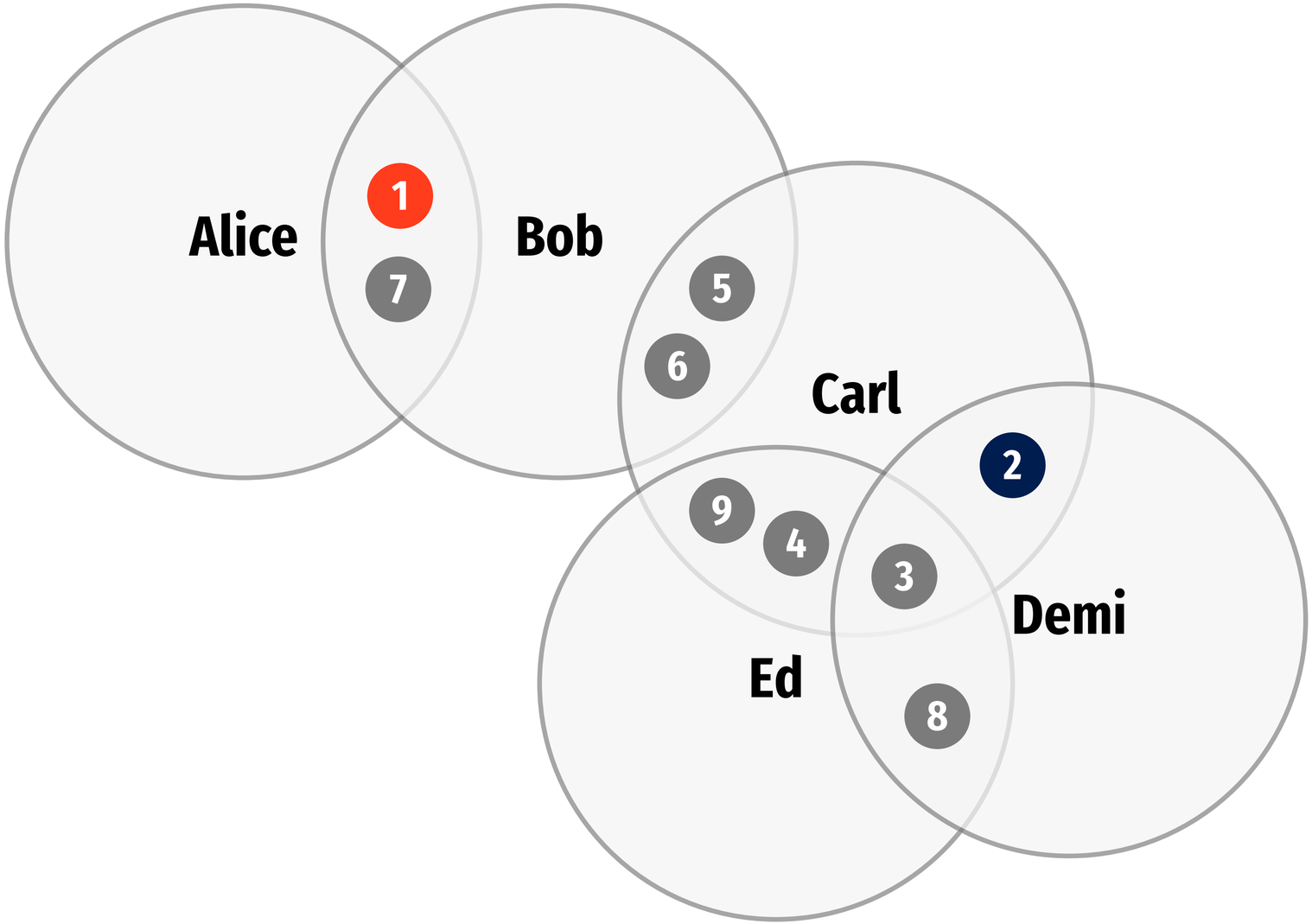
Corda: Public/Private Permissioned DLT

- DLT that allows building *private networks* as well as joining a *publicly available* internet of Corda nodes.
- Participant Identity based on Public Key Infrastructure (PKI) standards
- Subnetworks ('Business Networks') rearrange freely
- Assets remain transferable
- Only parties who should have access to the details of a transaction are those parties themselves and others with a legitimate need to know [Brown2016]
- Pluggable consensus protocols using dedicated 'notary nodes'



The Corda Privacy Model [R32018]

- Transaction details are only ever revealed to direct participants and notaries
- Corda uses notaries that validate transactions according to different consensus algorithms
- These can operate in ‘non-validating’ mode that does not reveal transaction details



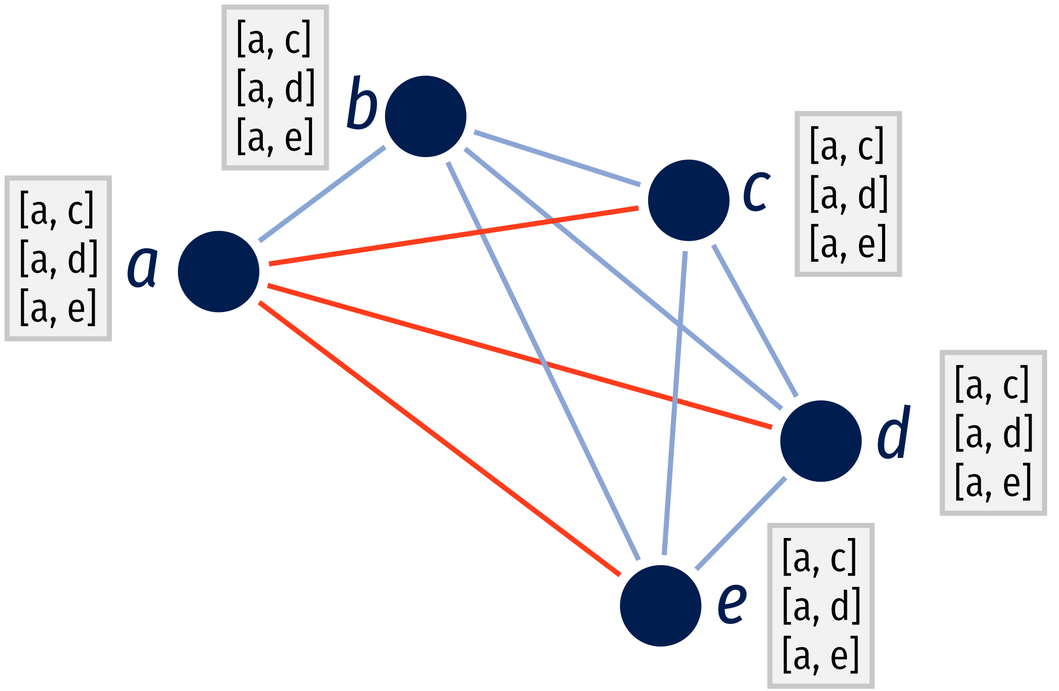
Corda Node Performance [R32018]

- Limiting distributing updates to the participants involved only allows high throughput
- Looking beyond individual participants, common usage patterns scale well network-wide

Node Cores	Enterprise (Issuance)	Enterprise (Payment)
1	90 tps	14 tps
2	103 tps	22 tps
4	225 tps	46 tps
8	350 tps	70 tps
16	730 tps	130 tps
32	1,001 tps	205 tps

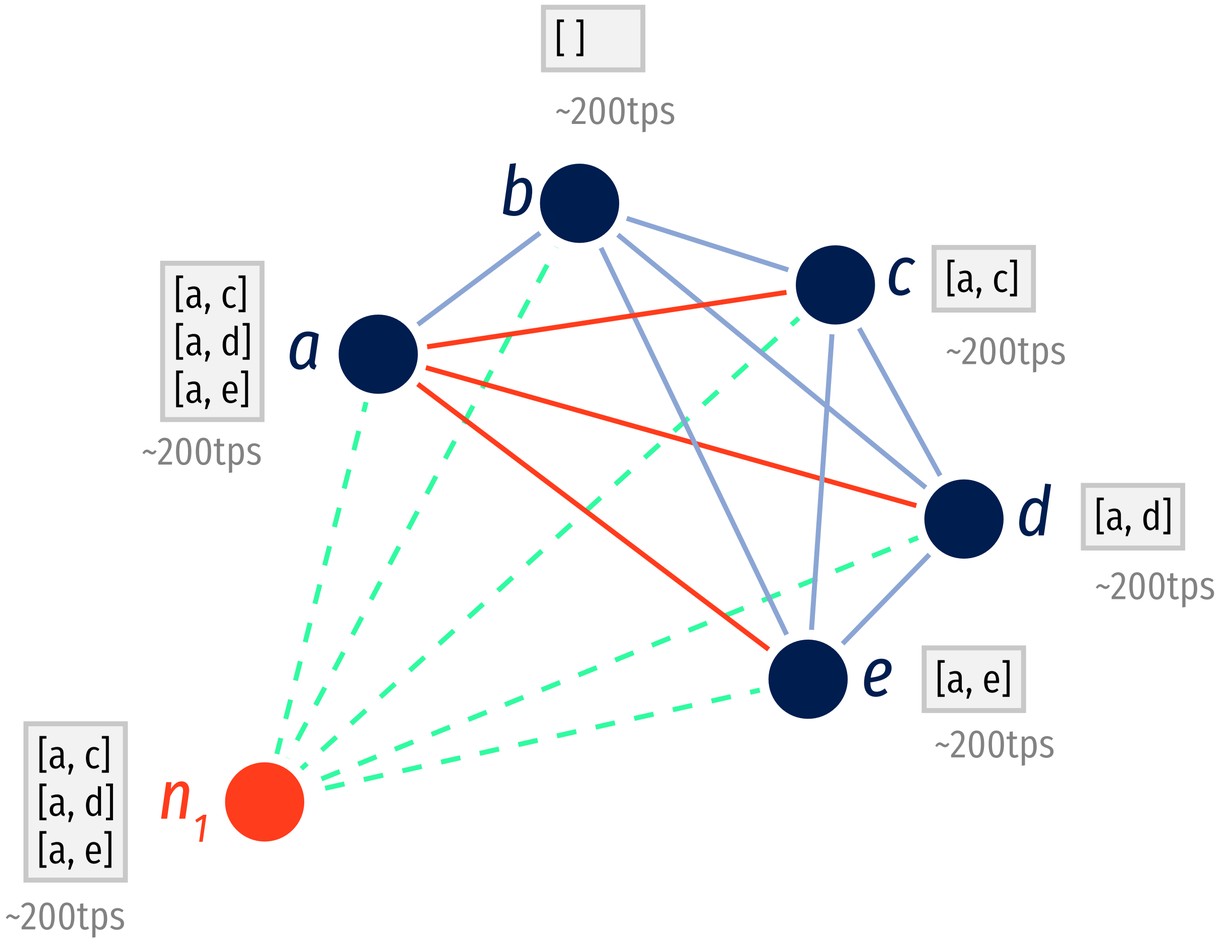
The Link Between Privacy and Performance

- In public permissionless systems, having to achieve global network consensus and distributing updates in blocks globally leads to severe performance ceilings
- Corda's privacy preserving paradigm means that dedicated notaries can validate transactions and only direct participants need updates



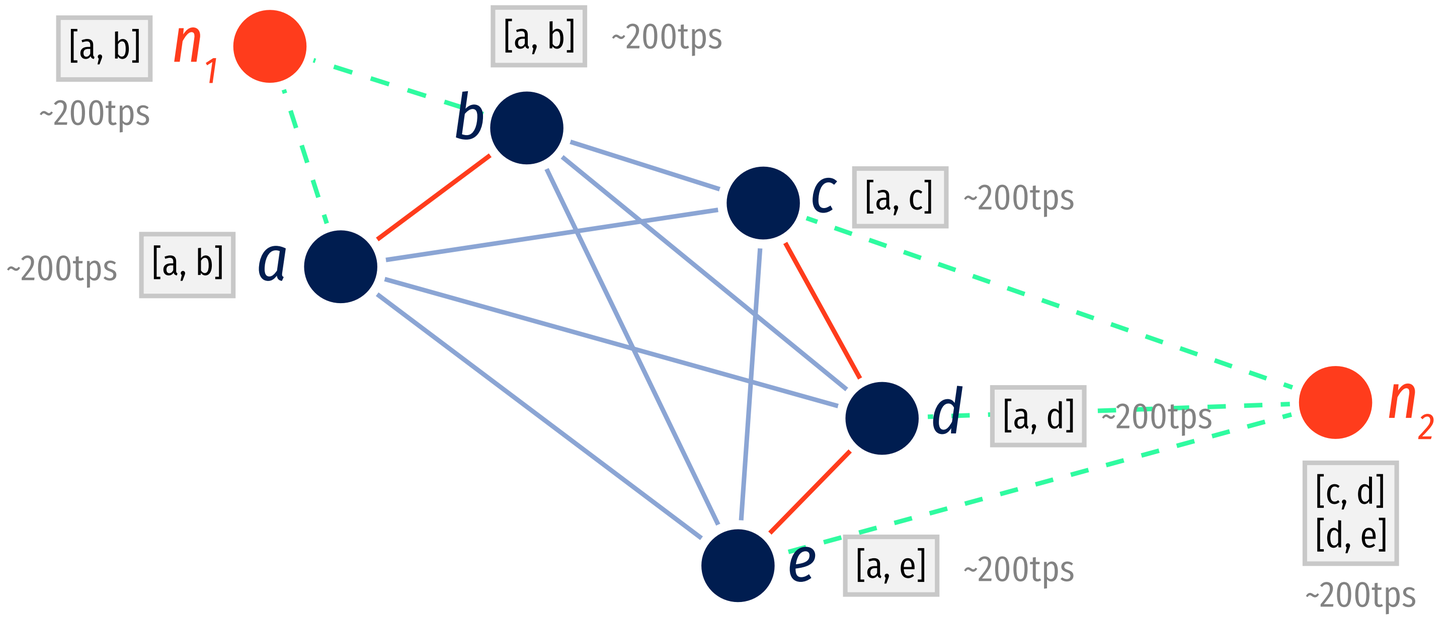
The Link Between Privacy and Performance

- Not having to relay all transactions to all participants has positive performance implications
- Node-level throughput is limited by the node performance (*a*, *e*) and notary performance (n_1)
- In a network *a*, *b*, *c*, *d*, *e* with notary n_1 all with individual performance of *200tps* the network throughput ceiling is equally *200tps*



The Link Between Privacy and Performance

- Node-level throughput is still limited
- Understanding traffic patterns allows for shaping network throughput
- A network where the majority of transactions is between subsets of nodes can benefit from partitioning
- For fully utilised *n1*, *n2* the network performance is ~400tps



Corda's Strengths

- Corda is an implementation of the DLT paradigm that satisfies enterprise requirements:
  - True finality of transactions (as opposed to probabilistic finality in 'Proof-of-Work' systems)
  - A private/permissioned model that represents industry reality well (i.e. consortia)
  - Strong privacy guarantees by revealing transaction details on a 'need-to-know' basis
  - High performance on participant level
  - Positive scaling characteristics on network level through partitioning

Research Agenda

- Maturity
  - Performance, Throughput, Scalability
  - Stability, Verifiability
  - Cross-chain compatibility
- Computing
  - Confidential Computing
  - Zero-Knowledge-Proofs
- Economy
  - Token economies
- Legislative Environment
  - Tokenisation
  - Digital Currency
  - Governance and Incentives of Block-chain Networks

Bibliography

InBook (Weik2001)
Weik, M. H.
finite state machine
Computer Science and Communications Dictionary, Springer US, **2001**, 609-609

InProceedings (Wuest2018)
Wüst, K. & Gervais, A.
Do you Need a Blockchain?
2018 Crypto Valley Conference on Blockchain Technology (CVCBT), **2018**, 45-54

Misc (Nakamoto2008)
Nakamoto, S.
Bitcoin: A peer-to-peer electronic cash system
2008

WWW (Jenkinson2017)
Jenkinson, G.
Bitcoin Mining Uses More Power Than Most African Countries
https://cointelegraph.com/news/bitcoin-mining-uses-more-power-than-most-african-countries
2017

InProceedings (Gervais2016)
Gervais, A.; Karame, G. O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H. & Capkun, S.
On the Security and Performance of Proof of Work Blockchains
Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, **2016**, 3-16

InProceedings (Androulaki2013)
Androulaki, E.; Karame, G. O.; Roeschlin, M.; Scherer, T. & Capkun, S.
Sadeghi, A.-R. (Ed.)
Evaluating User Privacy in Bitcoin
Financial Cryptography and Data Security, Springer Berlin Heidelberg, **2013**, 34-51

InProceedings (Androulaki2018)
Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; Muralidharan, S.; Murthy, C.; Nguyen, B.; Sethi, M.; Singh, G.; Smith, K.; Sorniotti, A.; Stathakopoulou, C.; Vukolić, M.; Cocco, S. W. & Yellick, J.
Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains
Proceedings of the Thirteenth EuroSys Conference, ACM, **2018**, 30:1-30:15

Misc (Baliga2018)
Baliga, A.; Subhod, I.; Kamat, P. & Chatterjee, S.
Performance Evaluation of the Quorum Blockchain Platform
2018

TechReport (Brown2016)
Brown, R. G.; Carlyle, J.; Grigg, I. & Hearn, M.
Corda: An Introduction
R3CEV LLC, R3CEV LLC, **2016**

WWW (R32018)
R3
Corda Enterprise Documentation
https://docs.corda.r3.com/_static/corda-developer-site.pdf
2018

Picture Credit

Two black cable cars under grey sky
Photo by Tomas Robertson on Unsplash
https://unsplash.com/@tomasrobertson