Blockchain Scaling

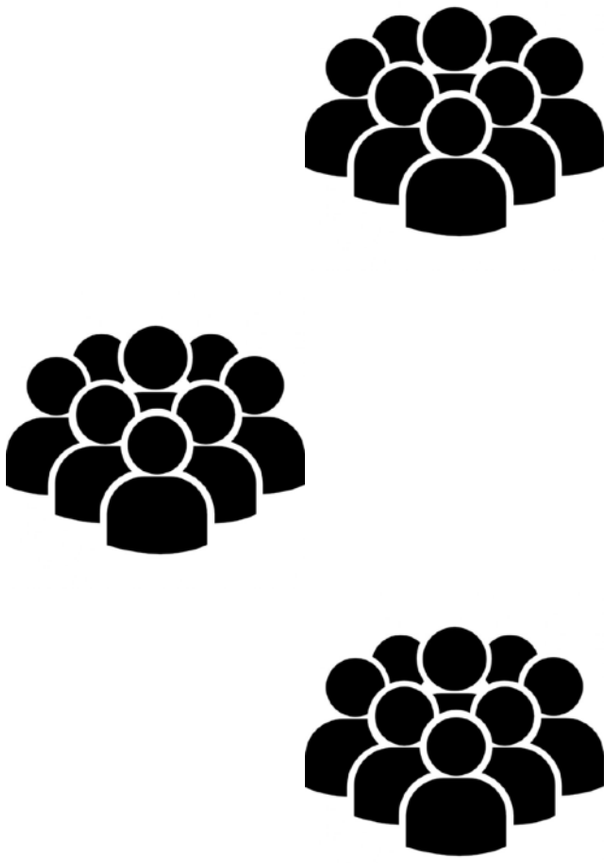
Existing cryptocurrencies do not scale (in terms of TPS)

~ 10 tps

Size of transaction in KB

Complexity of transaction in “Gas”

Why doesn’t it scale?



Many users

Many validators

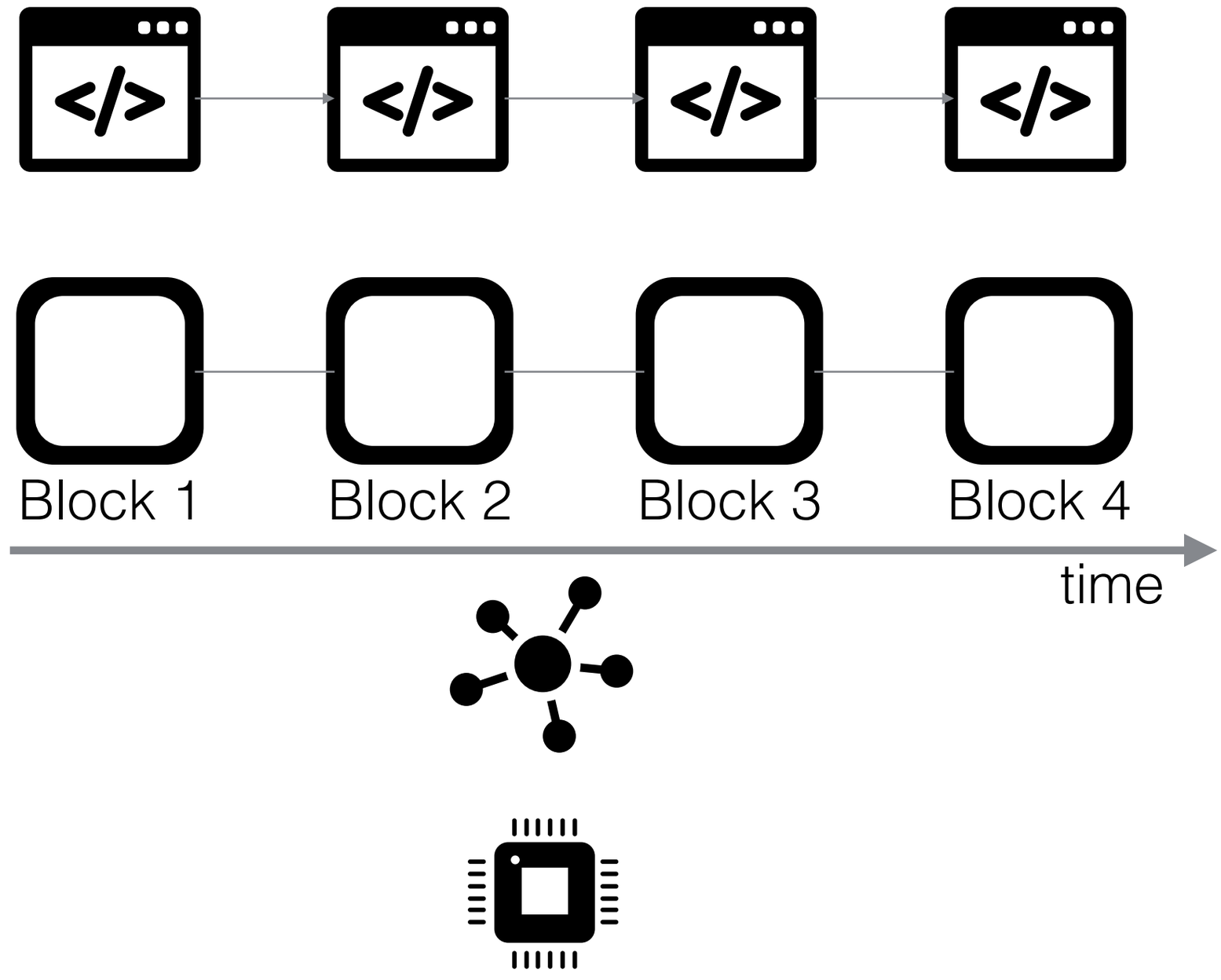
Blockchain Layers

Application
Layer 2

Blockchain
Layer 1

Network
Layer 0

Hardware
Layer -1



How can we scale?

Scaling

- **Network** →  **Comm. latency/bandwidth**
- **Consensus** →  **Tweak Consensus**
- **Sharding** →  **Partitioning the network**
- **Off-Chain** →  **Delayed on-chain settlement**

How can we scale?

Scaling

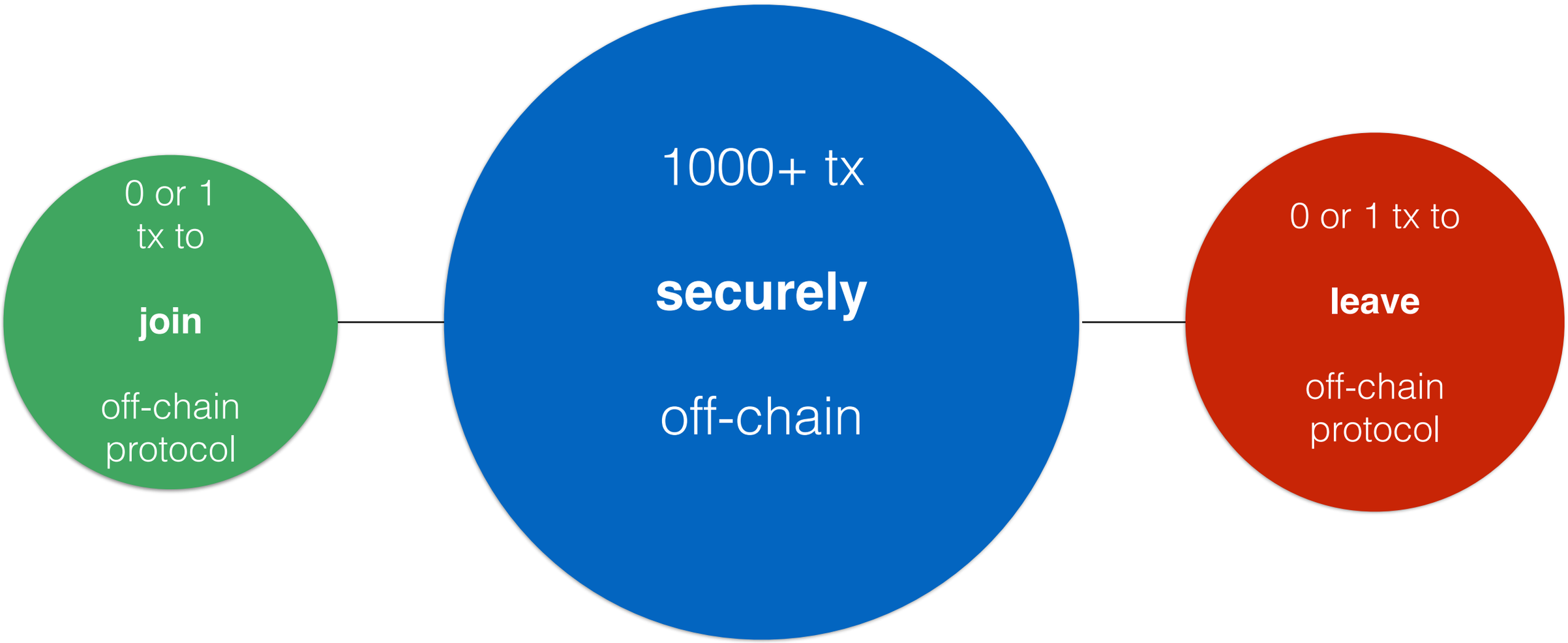
- **Network** → Comm. latency/bandwidth
- **Consensus** → Tweak Consensus
- **Sharding** → Partitioning the network
- **Off-Chain** → **Delayed on-chain settlement**

Complementary!

Off Chain Transaction ==

Transaction outside the blockchain, secured *by* the blockchain

Why is Off-Chain Exciting?



No consensus latency or mining fees,
while still achieving non-custodial security

Backward compatibility!

SoK: Off The Chain Transactions

Lewis Gudgeon
Imperial College London
l.gudgeon18@imperial.ac.uk

Pedro Moreno-Sanchez
TU Wien
pedro.sanchez@tuwien.ac.at

Stefanie Roos
TU Delft
s.roos@tudelft.nl

Patrick McCorry
King's College London
patrick.mccorry@kcl.ac.uk

Arthur Gervais
Imperial College London, Liquidity Network,
Lucerne University of Applied Sciences and Arts
a.gervais@imperial.ac.uk

***Abstract*—Blockchains have the potential to revolutionize markets and services, yet, currently exhibit high latencies and fail to handle loads comparable to those managed by traditional custodian financial systems. *Layer-two* protocols, built on top of (*layer-one*) blockchains, avoid disseminating every transaction to the whole network by sending transactions *off-chain* and instead utilize the blockchain only as a recourse for disputes. The promise of layer-two protocols is to complete transactions in sub-seconds, reduce fees, and allow blockchains to scale.**

With this Systematization of Knowledge, we are the first to structure the complete rich and multifaceted body of research on layer-two transactions. Categorizing the research into payment and state channels as well as commit-chains, we provide a comparison of the protocols and their properties. We contribute a systematization of the associated synchronization and routing protocols along with their privacy and security aspects. Contrary to common belief in the blockchain community, we show that layer-two can scale blockchains; that layer-two protocols are secure without full collateralization; that privacy of layer-two transaction is not granted by default; and that fees depend on the transmitted transaction value. The SoK clears the layer-two fog, highlights the potential of layer-two solutions and identifies their unsolved challenges and promising avenues of future work.

I. Introduction

The advent of blockchains over a decade ago [1]–[4] spurred rapid and extensive innovation across different scientific disciplines. Blockchains offer a mechanism through which mutually mistrusting entities can cooperate in the absence of a trusted third party. However, the use of broadcast in those non-custodial protocols limits their scalability to about ten transactions-per-second (tps) [5], [6], compared to custodian payment systems with thousands of tps [7]. Scaling limitadecentralized structure. Consensus changes might even lead to different, forked systems [23]. Layer-two protocols enable users to perform so-called *off-chain* transactions through private communication, rather than broadcasting the transaction on the (parent) blockchain. This optimization reduces the transaction load on the underlying blockchain and is fully backward compatible. The theoretical transaction throughput is only bounded by the communication bandwidth and latency of the involved parties. Off-chain transaction security can be guaranteed via allocated collateral, e.g. in payment channel designs [24]–[27] or by offering delayed transaction finality in commit-chain proposals [28].

A. This Systematization of Knowledge

A rich body of literature has emerged on off-chain protocols, proposing payment [24]–[27], [29], state [30] and virtual [31] channels, payment channel networks (PCNs) [27], [29] and related routing protocols [32]–[37], channel rebalancing [38] and channel factories [39] constructions, commit-chains [28], [40], channel hubs [41], [42], privacy-enhancing channels [41], [43]–[45]. However, the sources of information about layer-two protocols are highly disparate. Moreover, in part due to the rapid pace of advancement in the blockchain field, we observe, mostly outside academia, a frequent under-specification of constructions and their adversarial assumptions. This makes it exceedingly difficult to discern thought-through concepts from marketing activities. We aim to clear the fog surrounding layer-two protocols, equipping newcomers to this inaccessible field with a concise reference, and inform the directions of future

Which Off-Chain Solution?