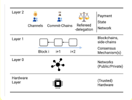
SoK- Layer-Two Blockchain Protocols

- Blockchains
  - revolutionize
  - high latencies
  - transaction loads
  - layers
    - hardware
      - Trusted Execution Environments (TEE)
        - No collateral lockup
        - Interoperability
        - Parallelized Disputes
        - Ensured fees
        - security concerns
          - rollback
          - side-channel attacks
    - layer-zero
      - Network Layer
        - peer-to-peer
        - scalability
        - security
        - privacy
    - layer-one
      - Blockchain Layer
        - consen- sus algorithm
        - integrity
        - eventual synchronicity
    - layer-two
      - **Definition 1.** *(Layer-two protocols). A layer-two protocol allows transactions between users through the exchange of authenticated messages via a medium which is outside of, but tethered to, a layer-one blockchain. Authenticated assertions are submitted to the parent-chain only in cases of a dispute, with the parent-chain deciding the outcome of the dispute. Security and non-custodial properties of a layer-two protocol rely on the consensus algorithm of the parent-chain.*
      - protocols
        - chan-nels
        - commit-chains
        - refereed delegation



- Layer-two
  - on top of (layer-one) blockchains
  - exchang- ing authenticated transactions off-chain
  - blockchain only as a recourse for disputes
  - off-chain transactions
    - sub-seconds
    - retaining asset security
    - reducing fees
    - allowing blockchains to scale
  - protocols
    - private and authenticated communication
    - channels
      - proposing pay- ment
      - state
        - state transitions
        - n parties to agree
          - unanimous consent
      - virtual
      - payment channel net- works
      - privacy-enhancing channels
    - routing protocols
      - Effectiveness
      - Efficiency
      - Scalability
      - Cost-Effectiveness
      - Privacy
    - channel hubs
      - lower average path length
        - reduction in collateral cost
        - route discovery complexity
      - significant locked capital requirements

        Issue
    - commit-chains
      - Free Establishment
      - Agreed Transition
      - Balance Security
      - State Progression
      - Commitment Integrity
    - channel factories
    - channel rebalanc- ing

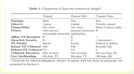


Table 1. Comparison of layer-two transaction designs[1].

	Channel	Channel Hub	Commit-Chain
Topology	Mesh	Star	Star
Lifecycle	3-phase	3-phase	Periodic commit
Compatibility	Any chain	Any chain	Smart Contract chain
Privacy	value privacy, relationship anonymity	payment anonymity, unlinkability	✕
Offline TX Reception	✕	✕	✓
Mass-Exit Security	✕	✕	✓(payments)
TX Finality	Instant	Instant	Delayed or Instant
Instant TX Collateral	Full	Full	Reusable [26]
Delayed TX Collateral	NA	NA	0
Collateral Allocation	$O(n)$ on-chain	$O(n)$ on-chain	$O(1)$ on-chain [26]
User On-Boarding	On-chain TX	On-chain TX	Off-chain [26]

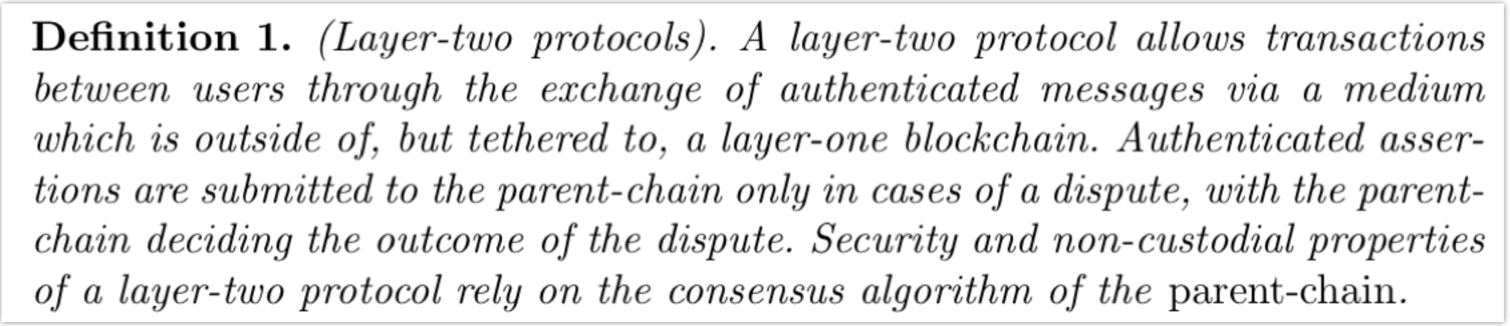
[1] Protocols for refereed delegation, distinct in nature with less focus on payments, are presented in Section 5.

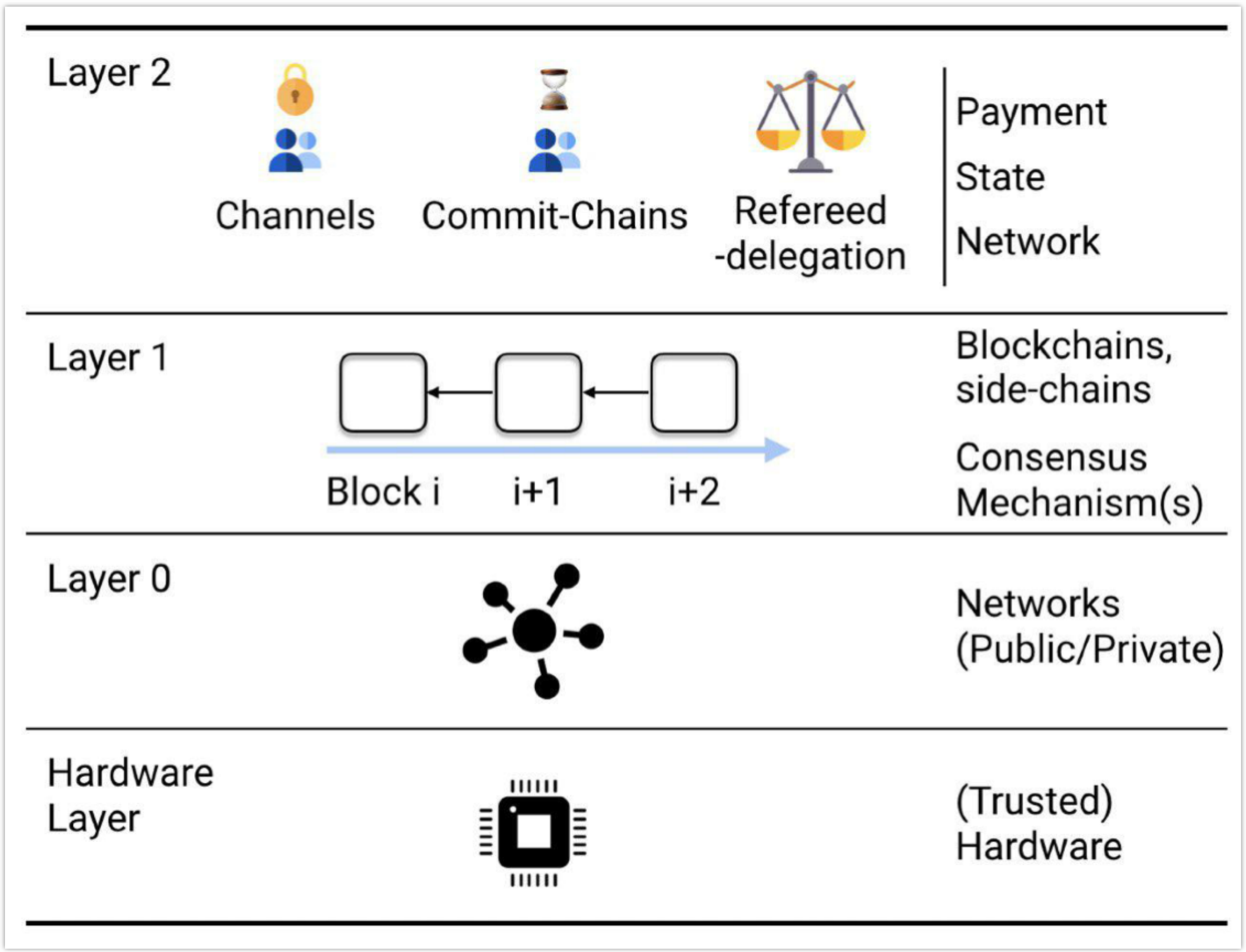
- Systematization of Knowledge
  - payment and state channels
  - commit-chains
  - pro- tocols
  - comparison
  - syn- chronization and routing
    - privacy
    - security

- mistrusting entities can cooperate in the absence of a trusted third party

- blockchain scaling solutions
  - consensus ar- chitectures
    - changing one of the key elements of a blockchain
    - lack of backward compati- bility
    - lead to different, forked systems
  - sharding
  - side-chains

- SoK- Layer-Two Blockchain Protocols
  - Blockchains ①
    - revolutionize ①
    - high latencies ①
    - transaction loads ①
    - layers ②
      - hardware ③
        - Trusted Execution Environments (TEE) ③
          - No collateral lockup ⑭
          - Interoperability ⑭
          - Parallelized Disputes ⑭
          - Ensured fees ⑭
          - security concerns ⑭
            - rollback ⑭
            - side-channel attacks ⑭
      - layer-zero ③
        - Network Layer ③
          - peer-to-peer ③
          - scalability ③
          - security ③
          - privacy ③
      - layer-one ③
        - Blockchain Layer ③
          - consen- sus algorithm ③

- integrity
- eventual synchronicity
- layer-two
  - 

    Definition 1. *(Layer-two protocols). A layer-two protocol allows transactions between users through the exchange of authenticated messages via a medium which is outside of, but tethered to, a layer-one blockchain. Authenticated assertions are submitted to the parent-chain only in cases of a dispute, with the parent-chain deciding the outcome of the dispute. Security and non-custodial properties of a layer-two protocol rely on the consensus algorithm of the* parent-chain.
  - protocols
    - chan-nels
    - commit-chains
    - refereed delegation
- 

- Layer-two
  - on top of (layer-one) blockchains
  - exchang- ing authenticated transactions off-chain
  - blockchain only as a recourse for disputes
  - off-chain transactions
    - sub-seconds

  - retaining asset security ①
  - reducing fees ①
  - allowing blockchains to scale ①
- protocols ②
  - private and authenticated communication ②
  - channels ②
    - proposing pay- ment ②
    - state ②
      - state transitions ④
      - n parties to agree ④
        - unanimous consent ④
    - virtual ②
    - payment channel net- works ②
    - privacy-enhancing channels ②
  - routing protocols ②
    - Effectiveness ⑨
    - Efficiency ⑨
    - Scalability ⑨
    - Cost-Effectiveness ⑨
    - Privacy ⑨
  - channel hubs ②
    - lower average path length ⑩
      - reduction in collateral cost ⑩
      - route discovery complexity ⑩

            - significant locked capital requirements ⑩

              Issue
        - commit-chains ②
            - Free Establishment ⑫
            - Agreed Transition ⑫
            - Balance Security ⑫
            - State Progression ⑫
            - Commitment Integrity ⑫
        - channel factories ②
        - channel rebalanc- ing ②
    - ⑬

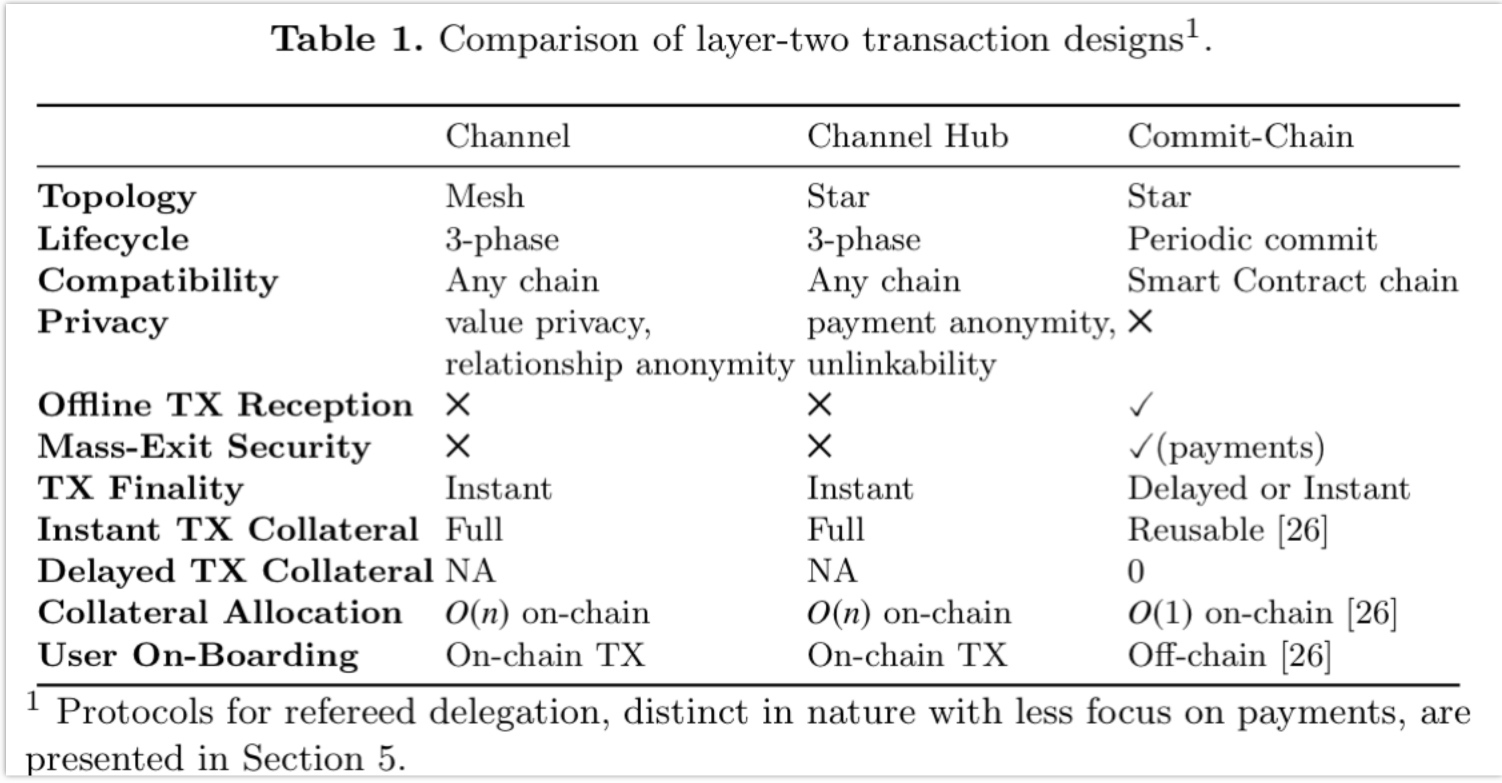


Table 1. Comparison of layer-two transaction designs[1].

	Channel	Channel Hub	Commit-Chain
Topology	Mesh	Star	Star
Lifecycle	3-phase	3-phase	Periodic commit
Compatibility	Any chain	Any chain	Smart Contract chain
Privacy	value privacy, relationship anonymity	payment anonymity, unlinkability	✗
Offline TX Reception	✗	✗	✓
Mass-Exit Security	✗	✗	✓(payments)
TX Finality	Instant	Instant	Delayed or Instant
Instant TX Collateral	Full	Full	Reusable [26]
Delayed TX Collateral	NA	NA	0
Collateral Allocation	$O(n)$ on-chain	$O(n)$ on-chain	$O(1)$ on-chain [26]
User On-Boarding	On-chain TX	On-chain TX	Off-chain [26]

[1] Protocols for refereed delegation, distinct in nature with less focus on payments, are presented in Section 5.

- Systematization of Knowledge ①
    - payment and state channels ①
    - commit-chains ①
    - pro- tocols ①
    - comparison ①
    - syn- chronization and routing ①
        - privacy ①
        - security ①
- mistrusting entities can cooperate in the absence of a trusted third party ①

- blockchain scaling solutions ①
  - consensus architectures ①
    - changing one of the key elements of a blockchain ②
    - lack of backward compatibility ②
    - lead to different, forked systems ②
  - sharding ①
  - side-chains ①