Rethinking General-Purpose Decentralized Computing

Enis Ceyhun Alp
Eleftherios Kokoris-Kogias, Georgia Fragkouli, Bryan Ford
Decentralized and Distributed Systems Lab (DEDIS)

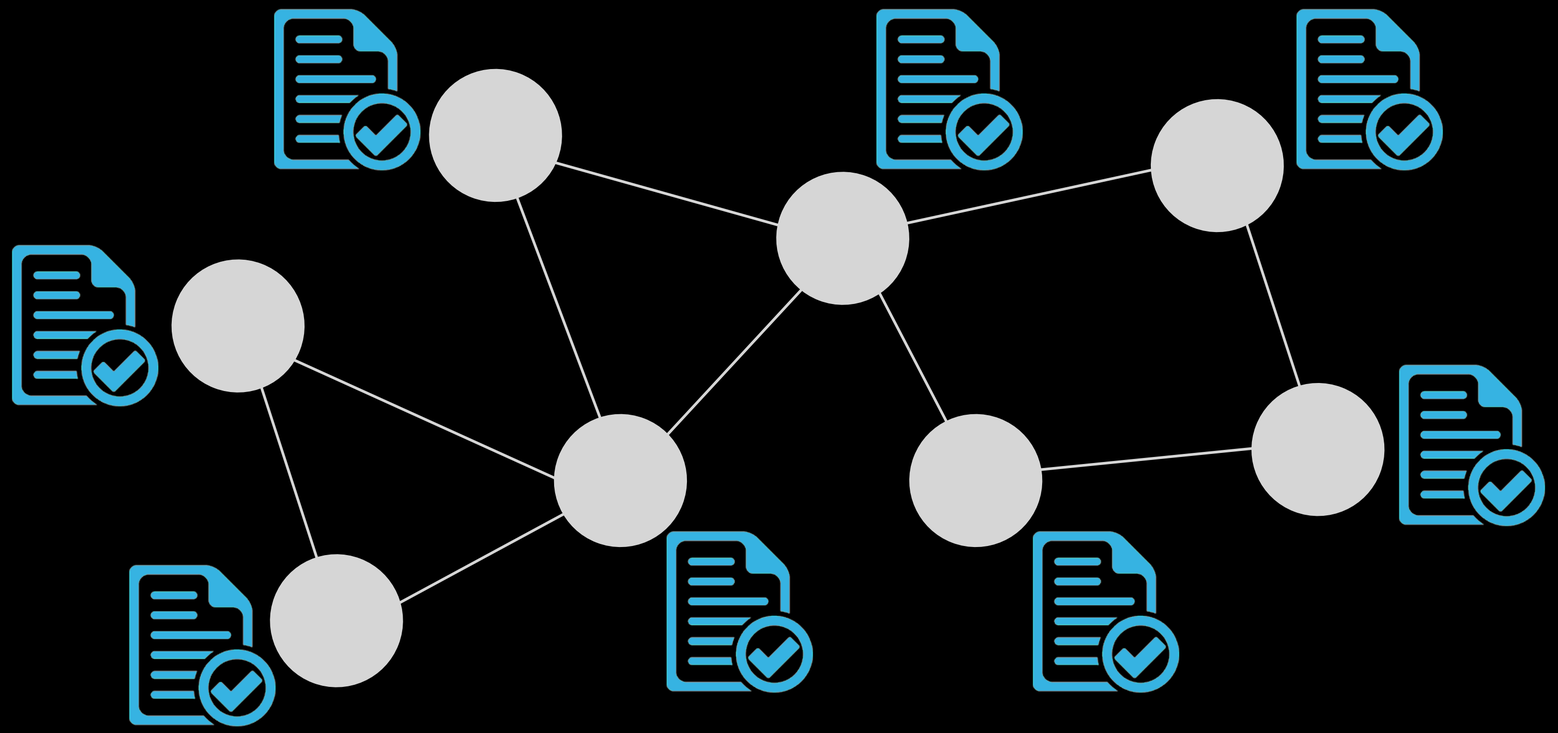
EPFL

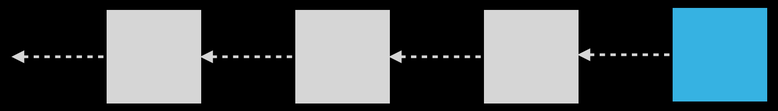
HotOS XVII
May 13, 2019


MORE BLOCKCHAIN

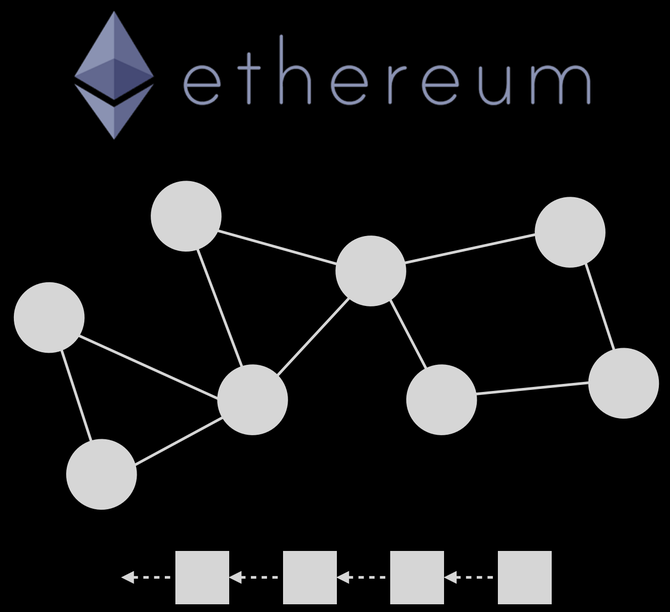
MORE BLOCKCHAIN

Smart contracts





Ethereum



- 2nd largest cryptocurrency
- ~445M transactions processed
- ~1.5M contracts deployed
- “The world computer”

BUT…

What’s wrong?

😔 Limited functionality

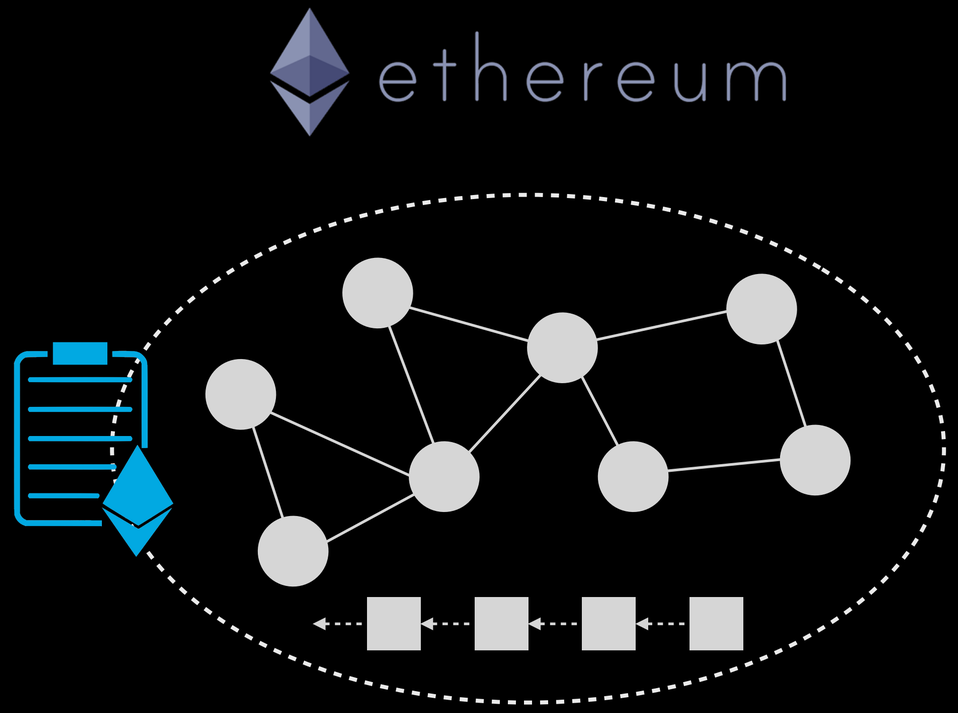
- ❖ No support for non-determinism
- ❖ Cannot securely operate on private data

😔 Difficulty of system upgrades

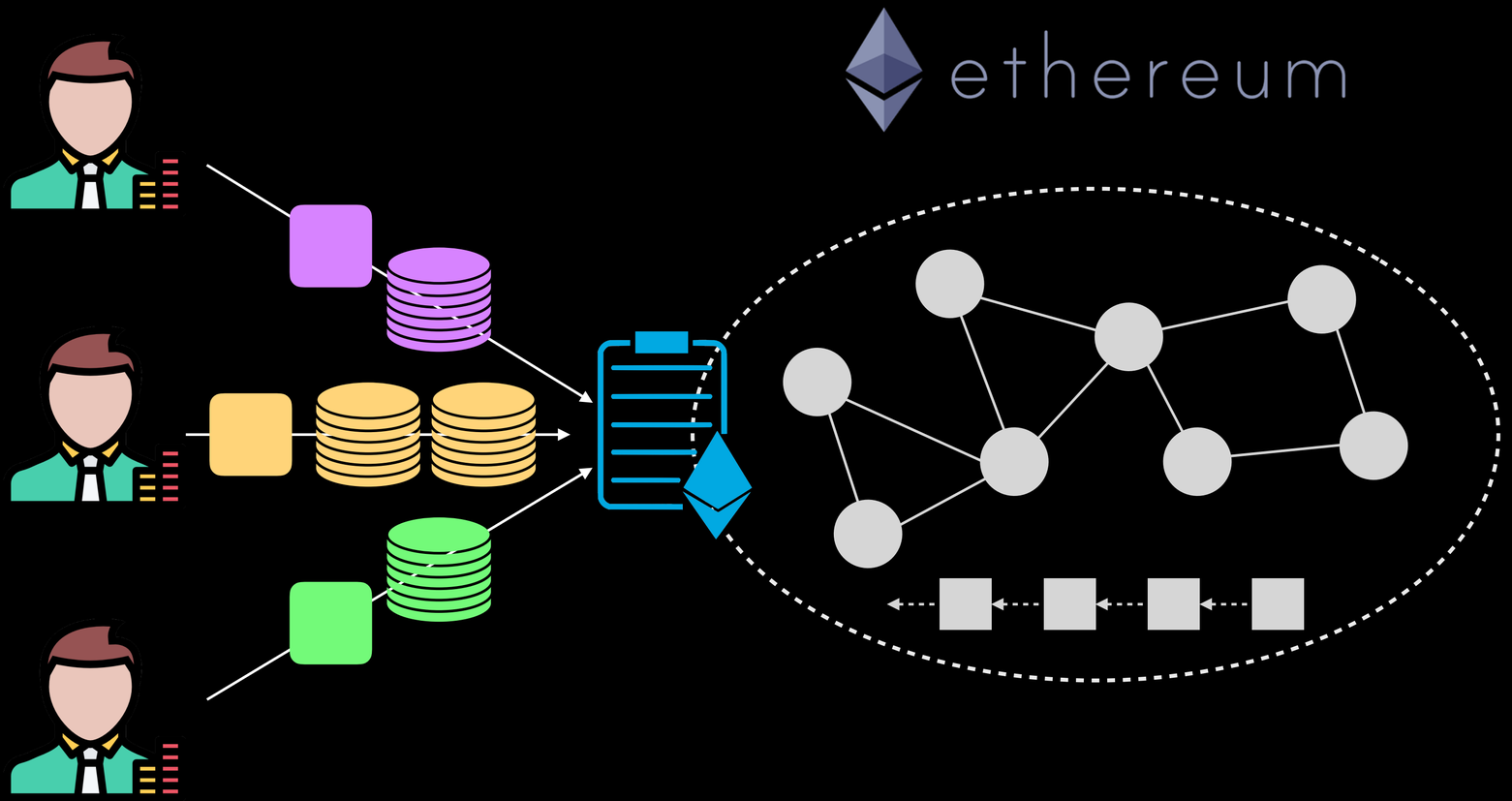
😔 Poor performance

- ❖ Every node runs every contract

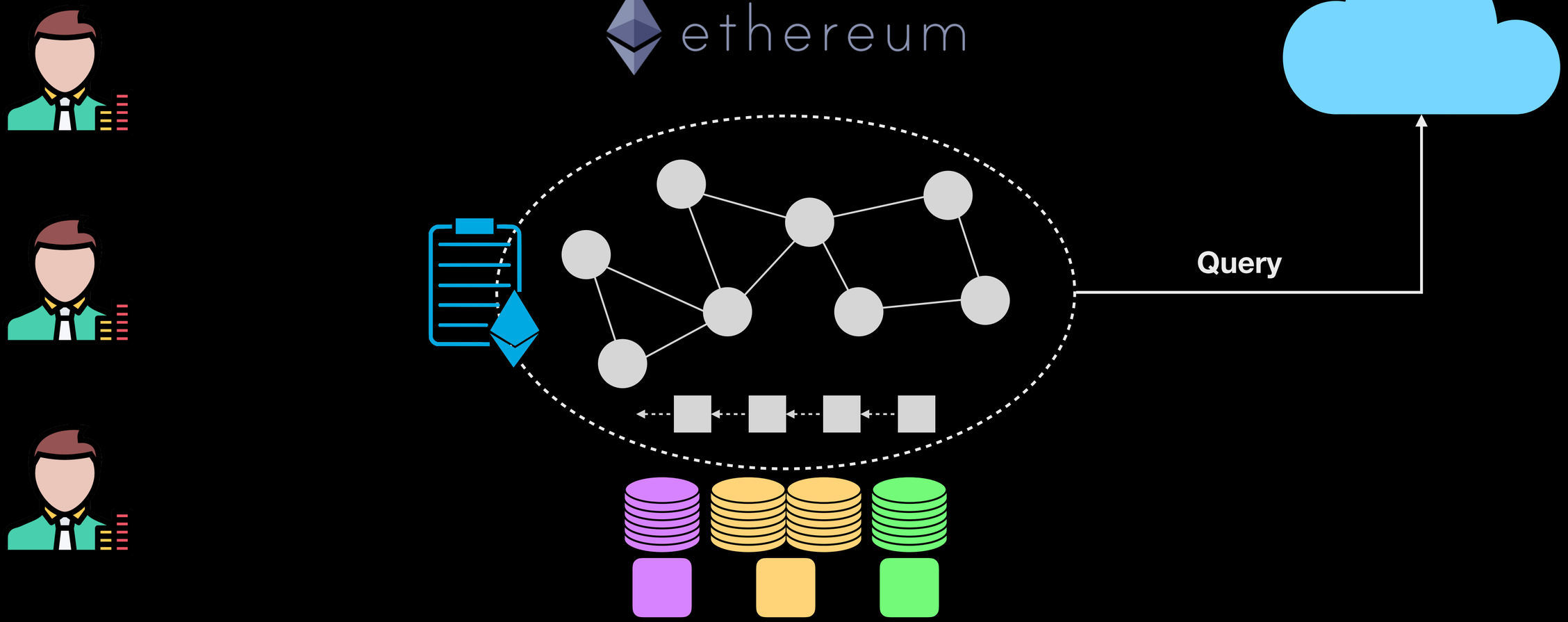
Running example: Betting application



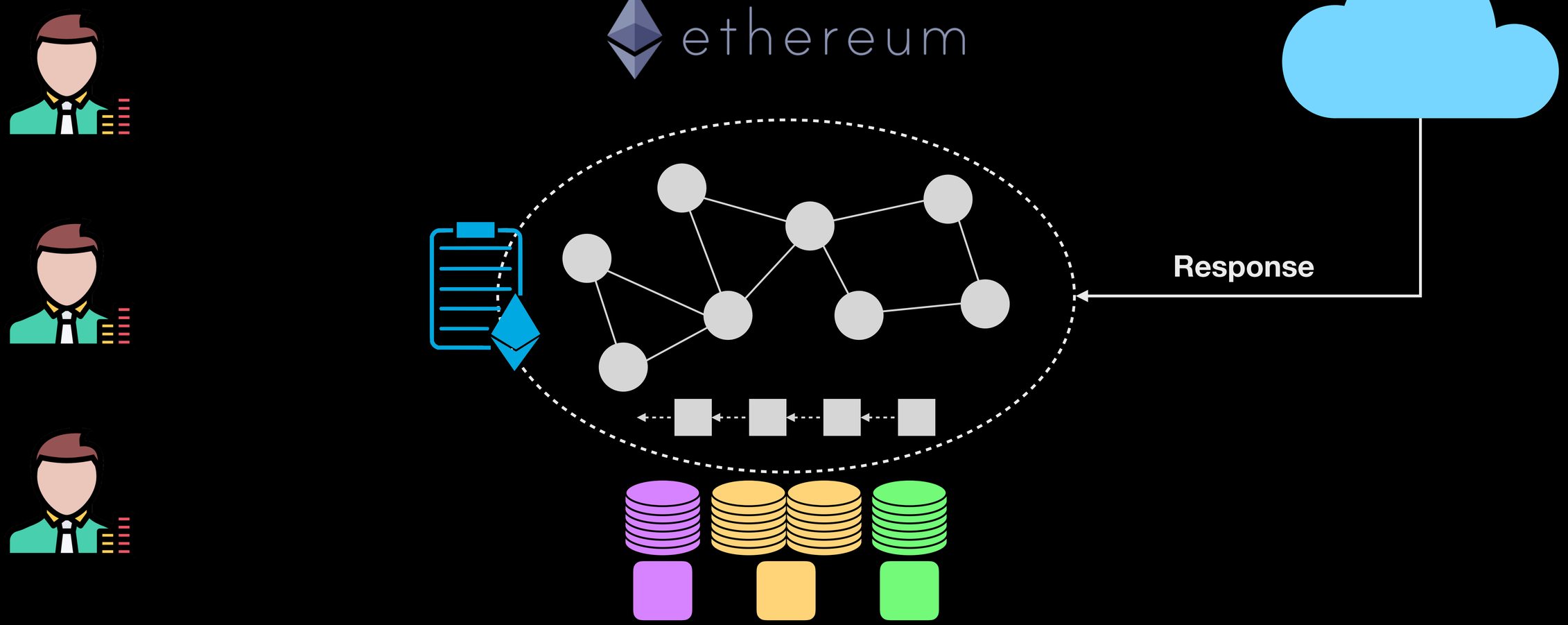
Running example: Betting application



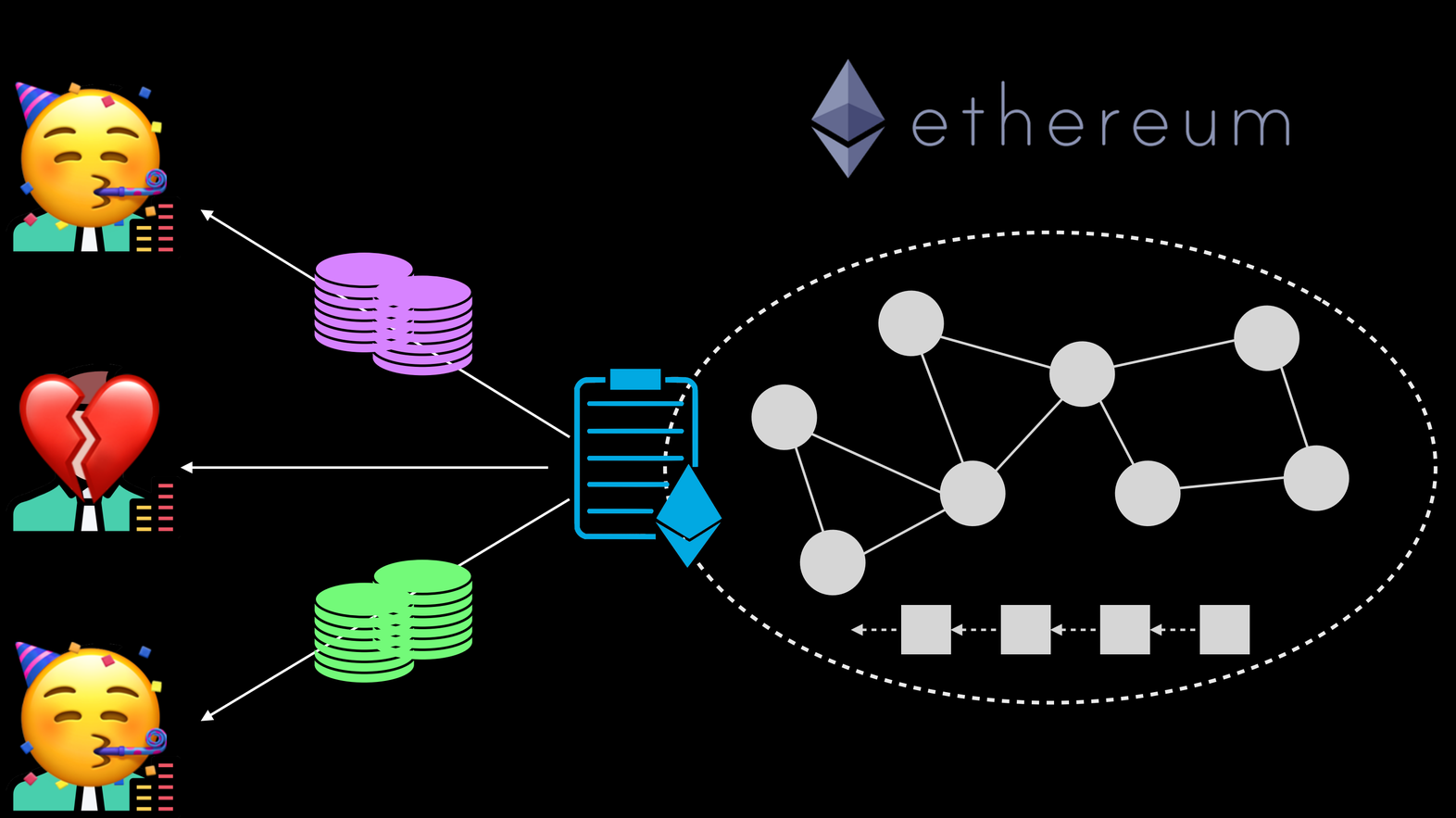
Running example: Betting application



Running example: Betting application



Running example: Betting application



Challenges

Hide predictions until release time

Store data off-chain

Access to reliable real-world data

Third-party oracle services

Challenges

Hide predictions until release time

Access to reliable real-world data

Upgrade for new functionalities

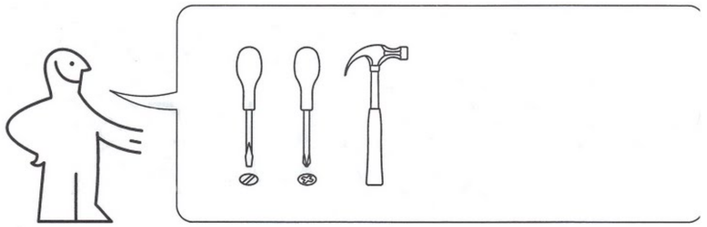
Challenges

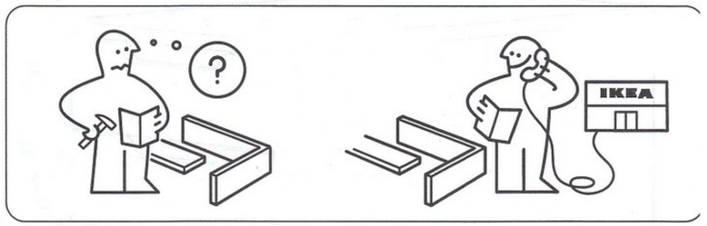
Hide predictions until release time

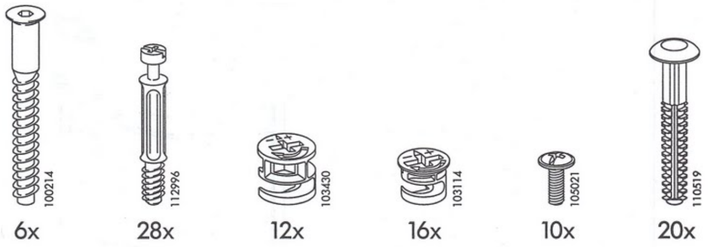
Access to reliable real-world data

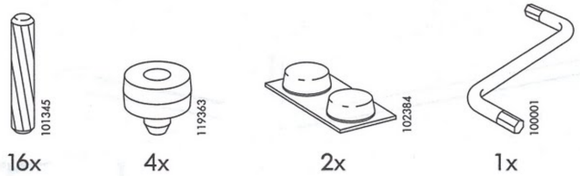
Monolithic architecture

Consensus and **code execution**
are **tightly coupled**



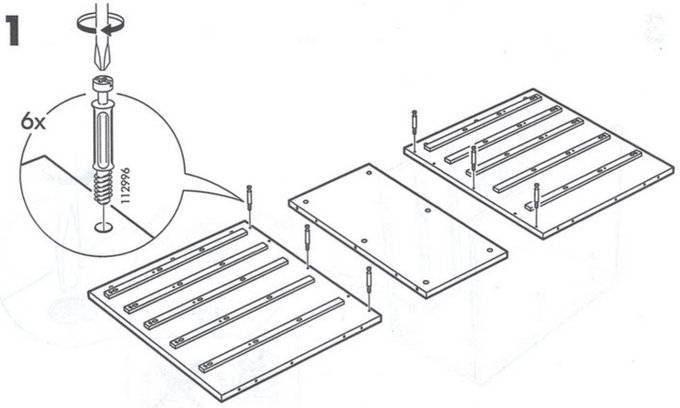

?
IKEA


100214
6x
112996
28x
103430
12x
103114
16x
105021
10x
110519
20x

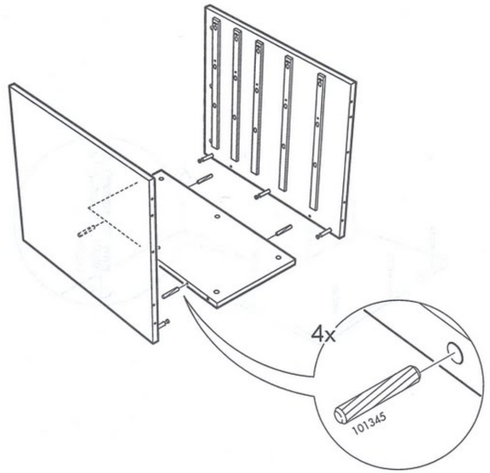

101345
16x
119363
4x
102384
2x
100001
1x

AA-343514-

1


6x
112996

2


4x
101345

PROTEAN

A modular architecture for general-purpose decentralized computing

Functional separation of nodes into special-purpose modules

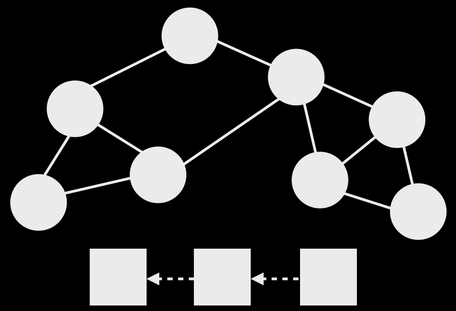
Functional units

- Distributed systems that provide distinct specialized computations
- Similar to **microservices** architecture in cloud computing

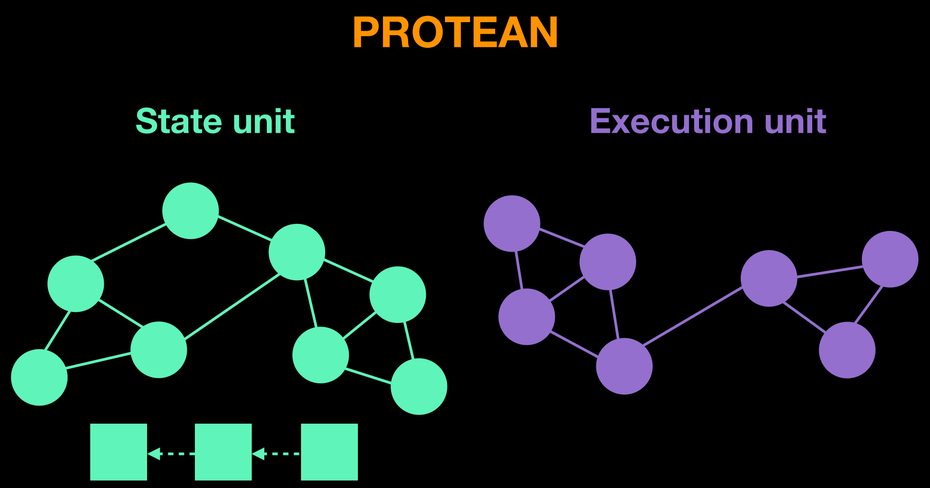
Functional units

Ethereum

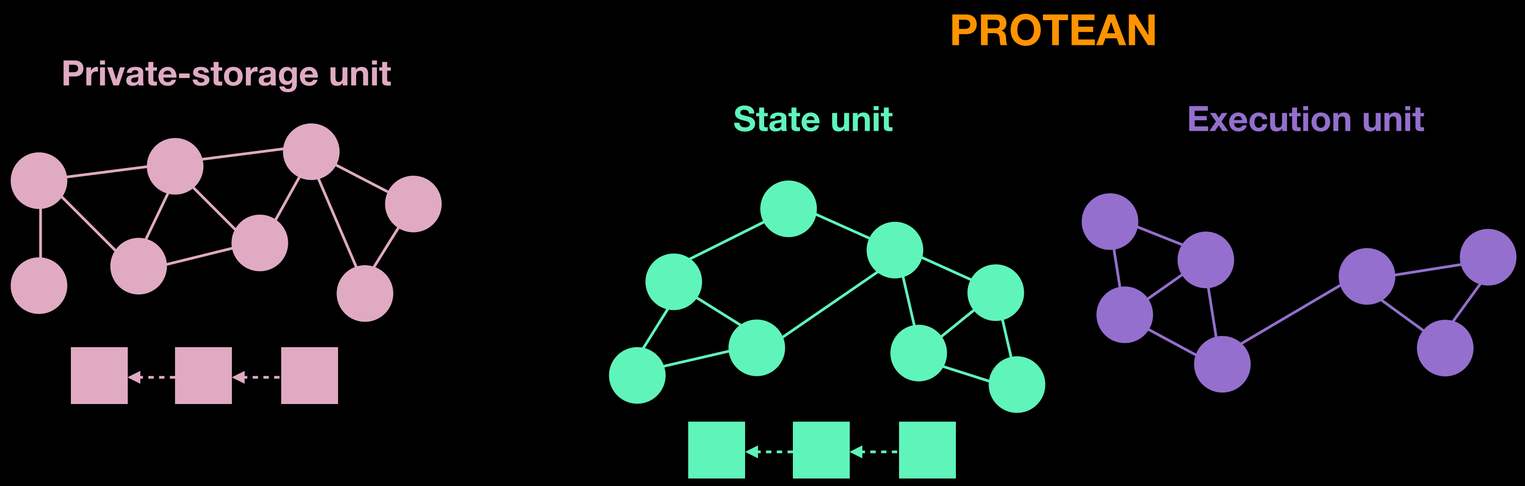
State & Execution unit



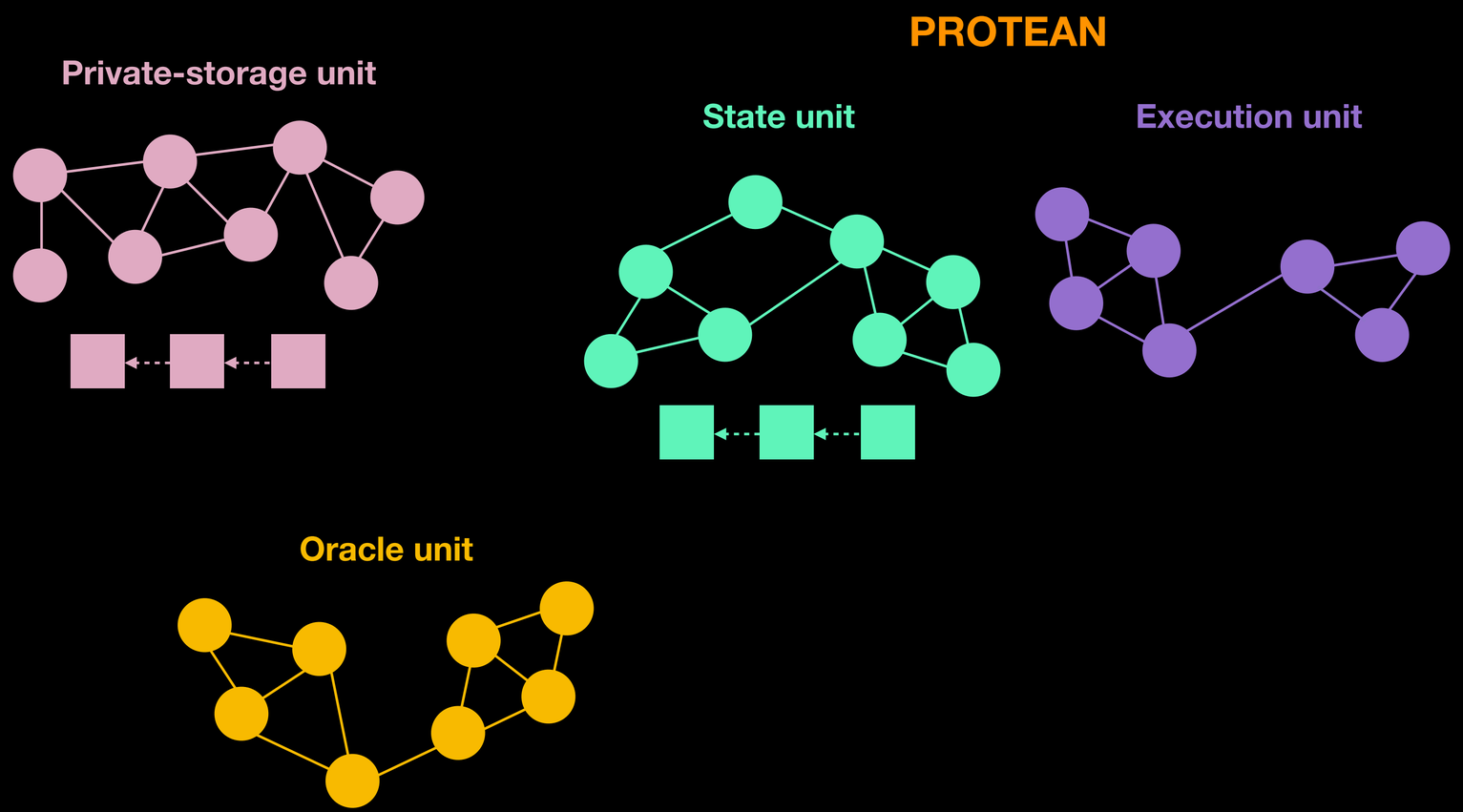
Functional units



Functional units



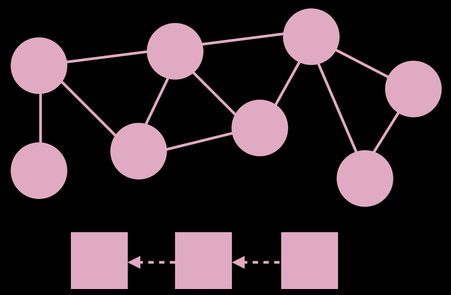
Functional units



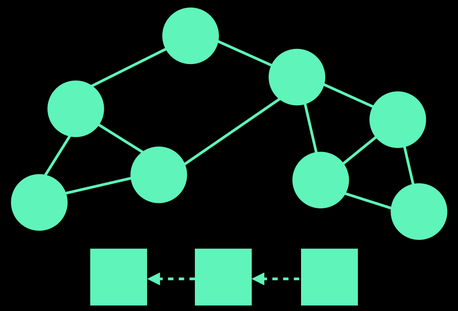
Functional units

PROTEAN

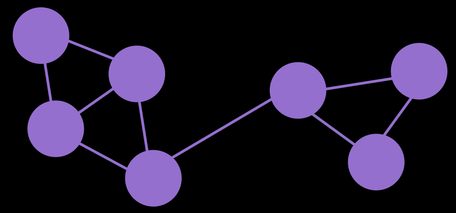
Private-storage unit



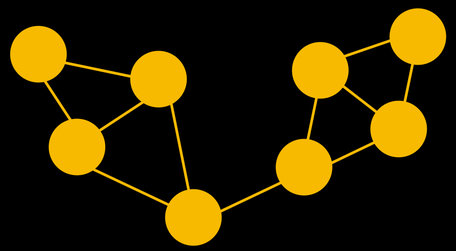
State unit



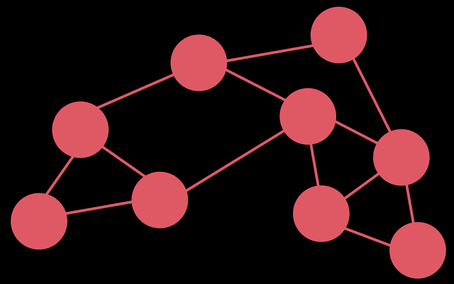
Execution unit



Oracle unit



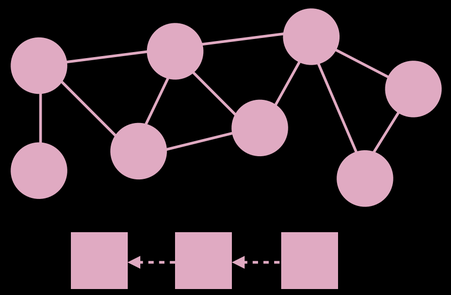
Randomness unit



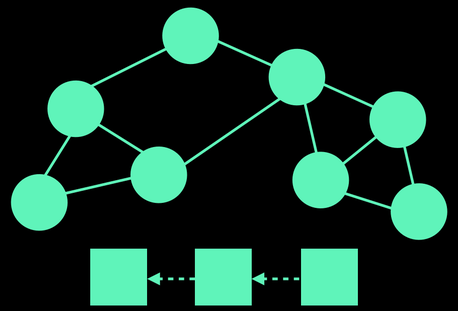
Functional units

PROTEAN

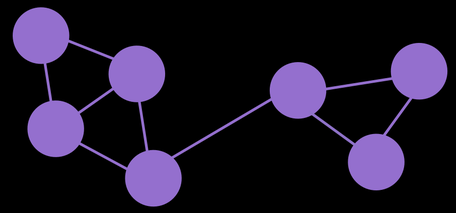
Private-storage unit



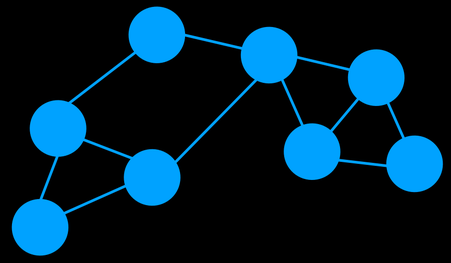
State unit



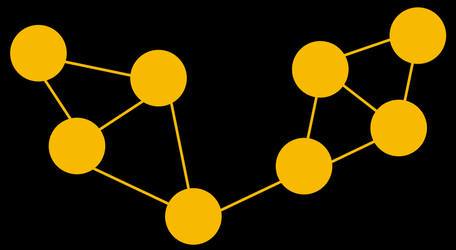
Execution unit



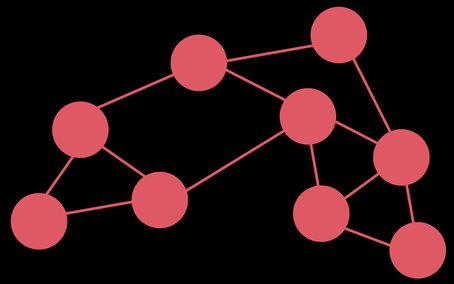
Shuffler unit



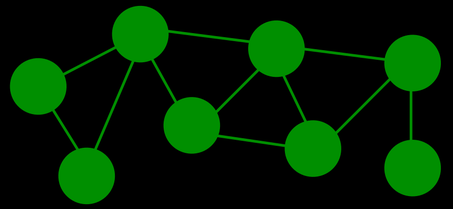
Oracle unit



Randomness unit



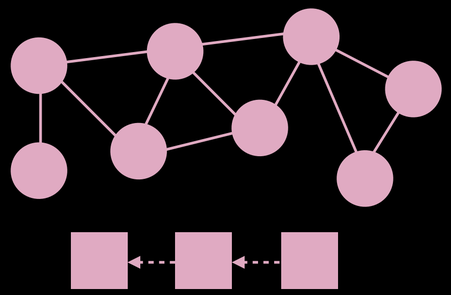
Encryption unit



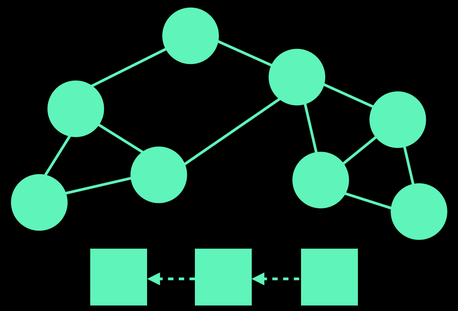
Functional units

PROTEAN

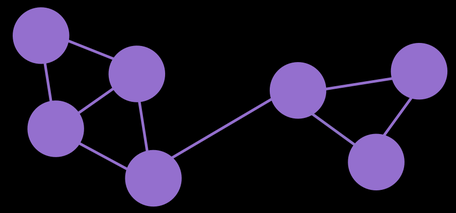
Private-storage unit



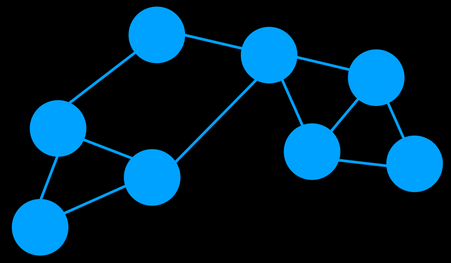
State unit



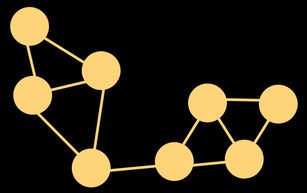
Execution unit



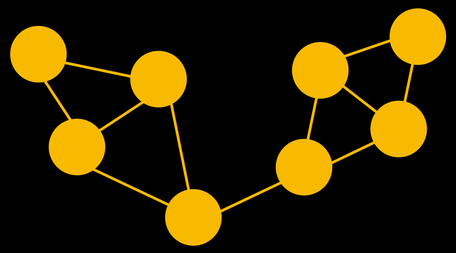
Shuffler unit



OU1-v2

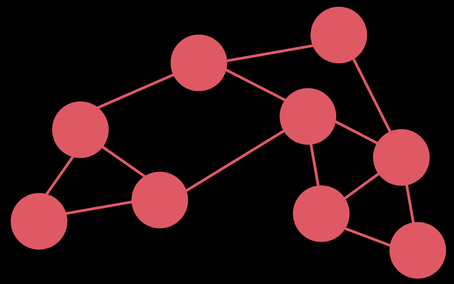


Oracle unit

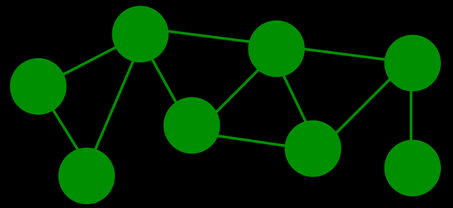


OU1-v1

Randomness unit



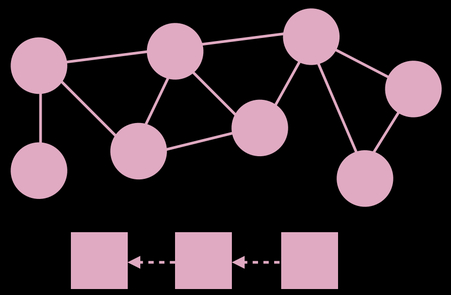
Encryption unit



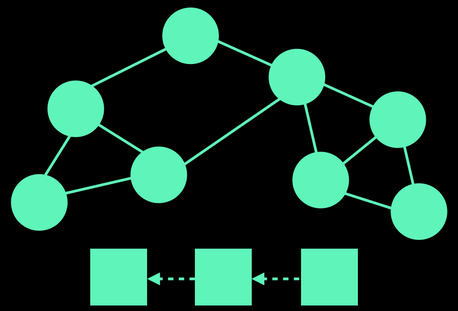
Functional units

PROTEAN

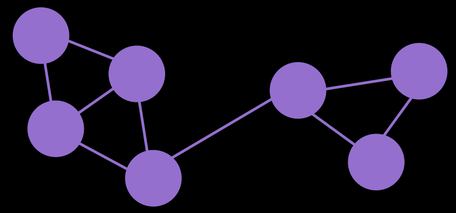
Private-storage unit



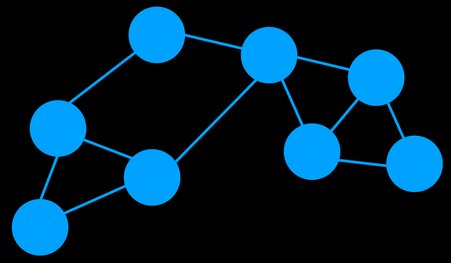
State unit



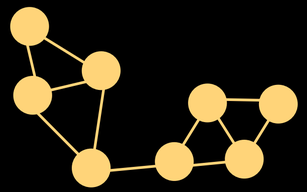
Execution unit



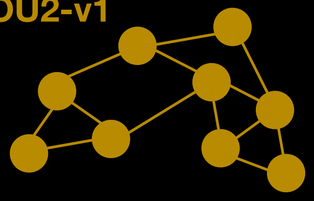
Shuffler unit



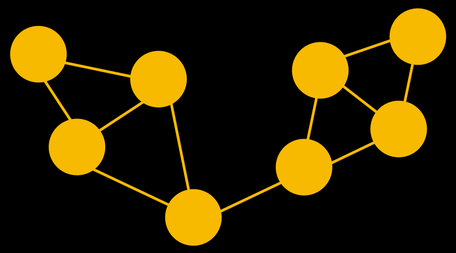
OU1-v2



OU2-v1

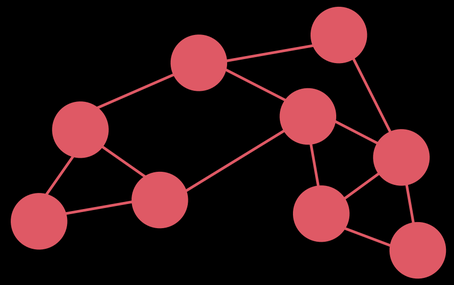


Oracle unit

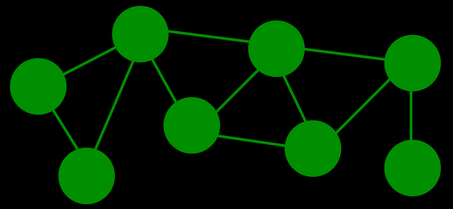


OU1-v1

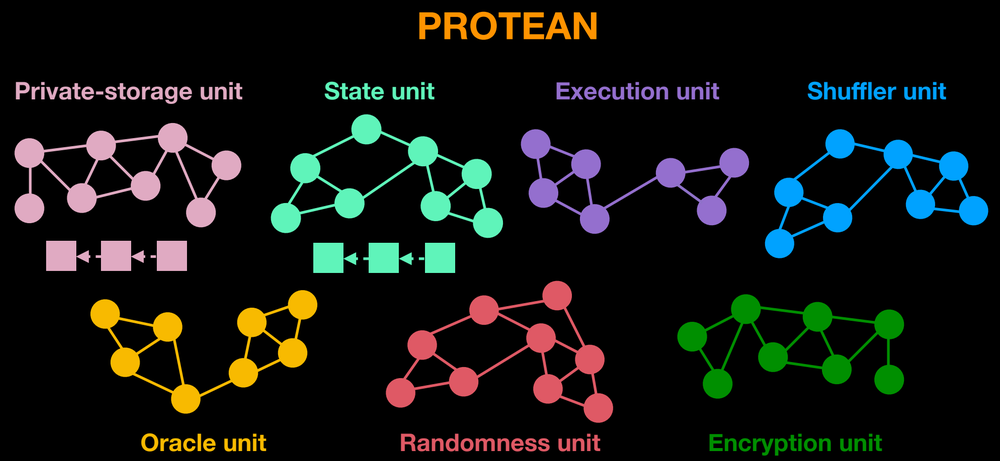
Randomness unit



Encryption unit



Functional units



Richer set of functionalities

Permissionless evolution

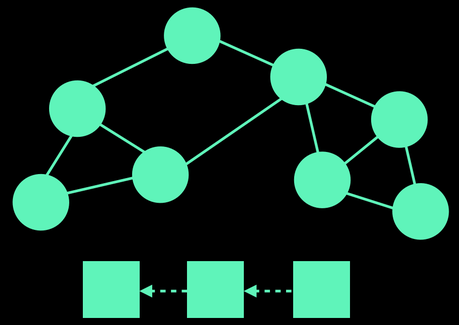
Functional units

- Expose a set of **transactions**
  - ❖ Building blocks for decentralized applications
  - ❖ Well-defined semantics and API
  - ❖ Executed atomically by the unit
- Provide cryptographic proof of successful execution

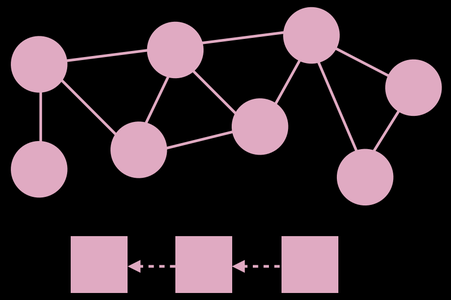
Building applications

Bet

State unit

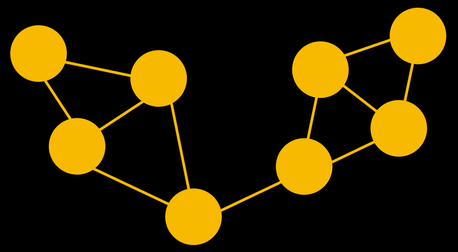


Private-storage unit

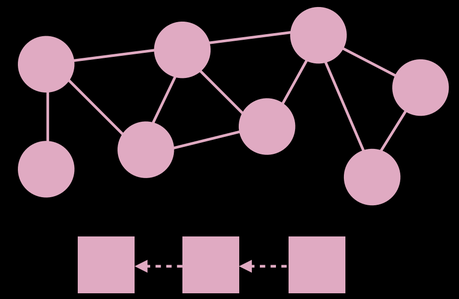


Reveal

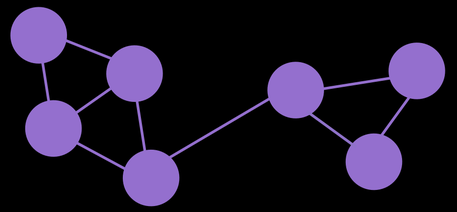
Oracle unit



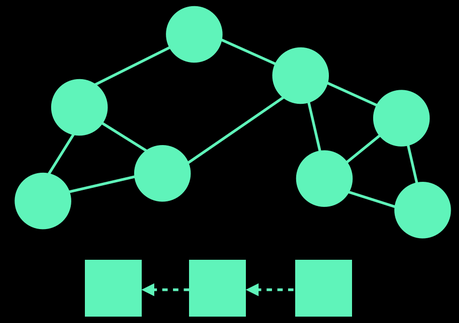
Private-storage unit



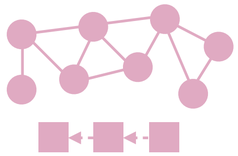
Execution unit



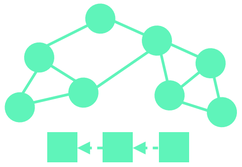
State unit



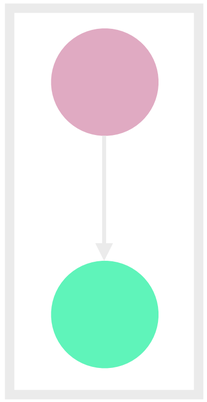
Private-storage unit



State unit



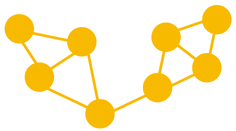
Workflow



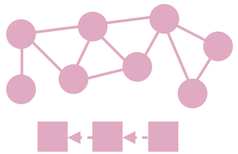
store_secret

update_state

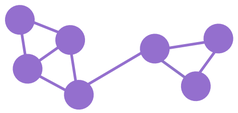
Oracle unit



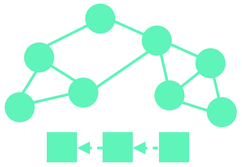
Private-storage unit



Execution unit



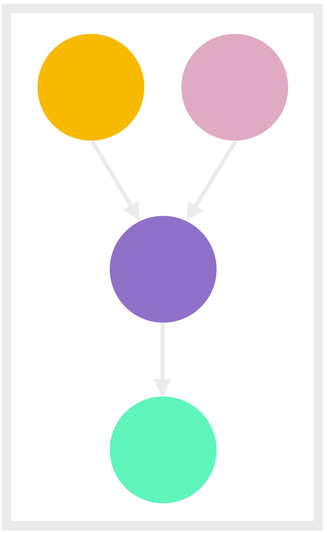
State unit



oracle_query

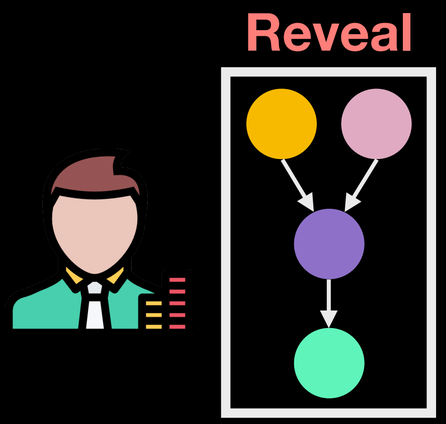
execute

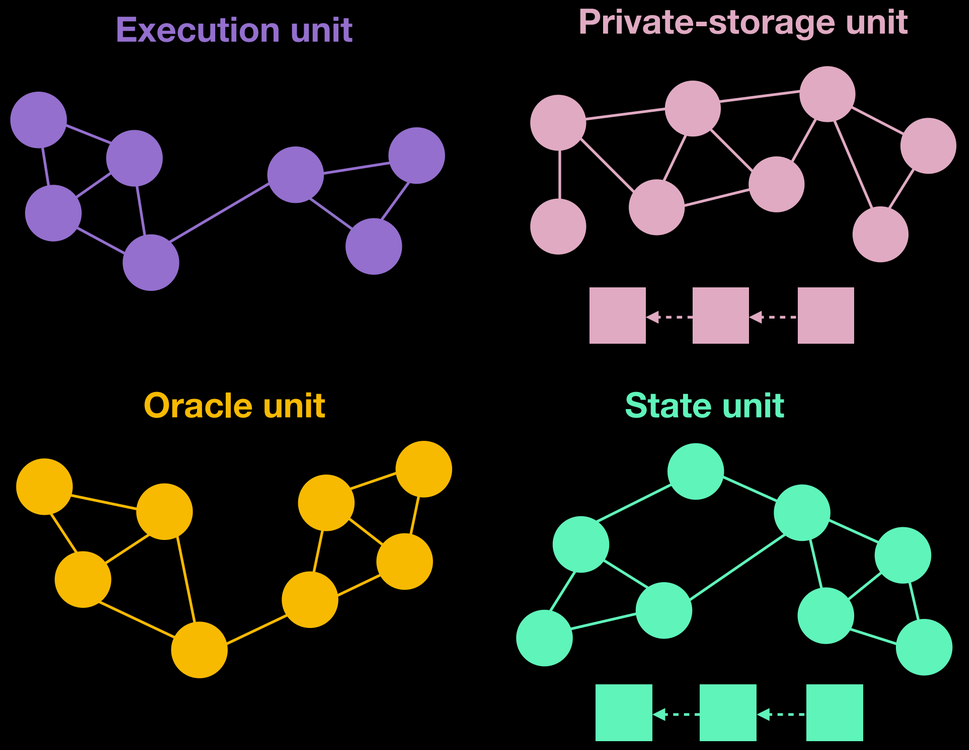
update_state



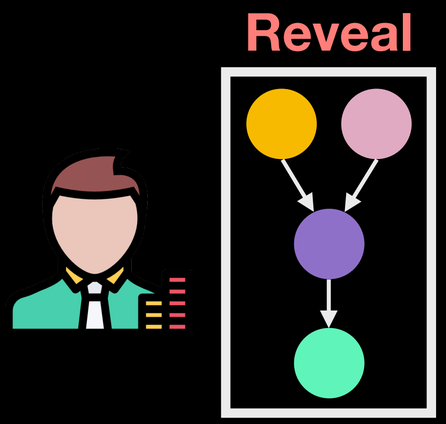
get_secret

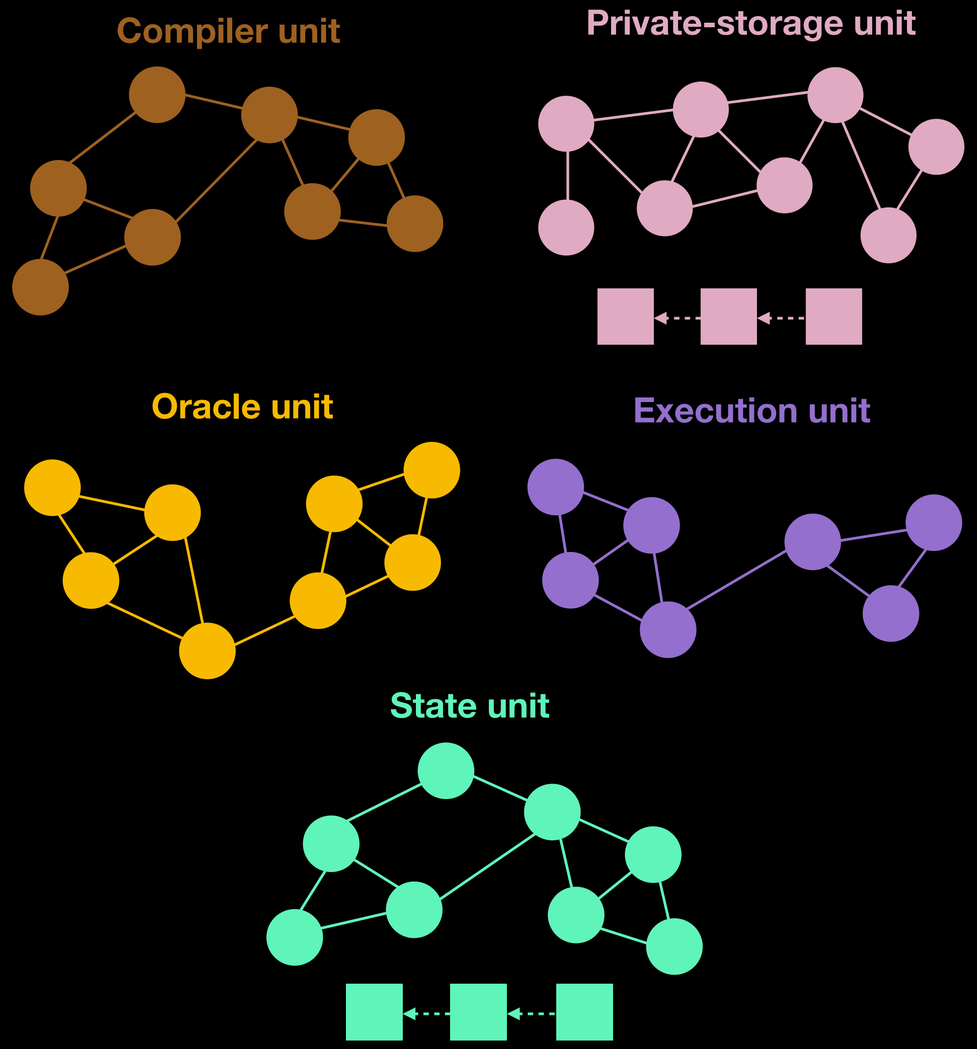
Executing applications



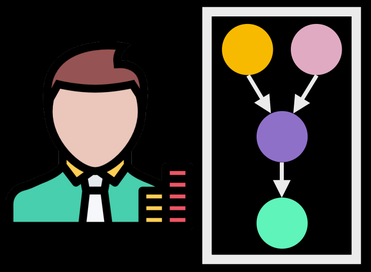


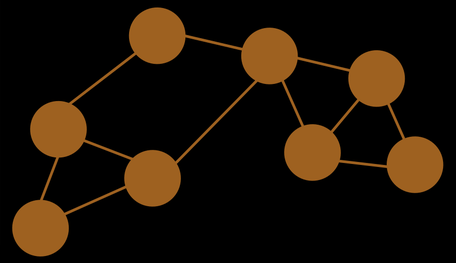
Executing applications

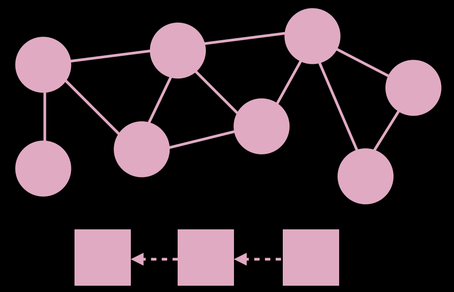


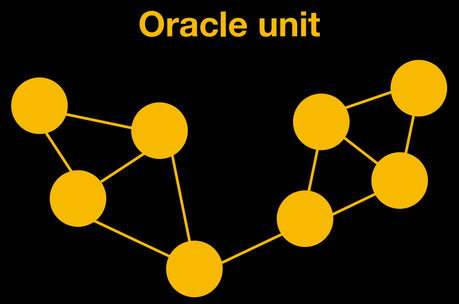


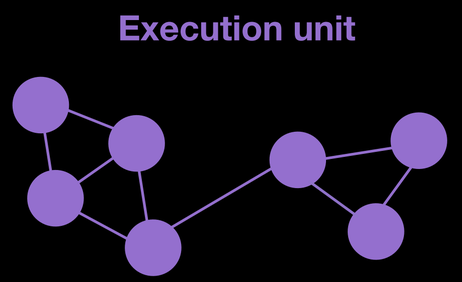
Executing applications

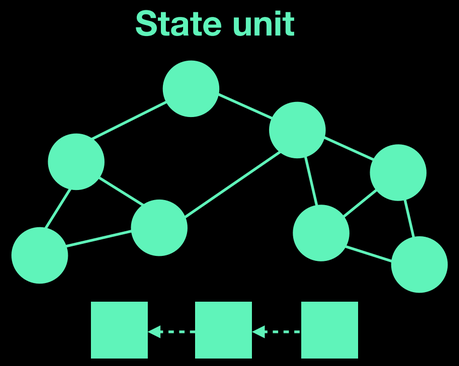




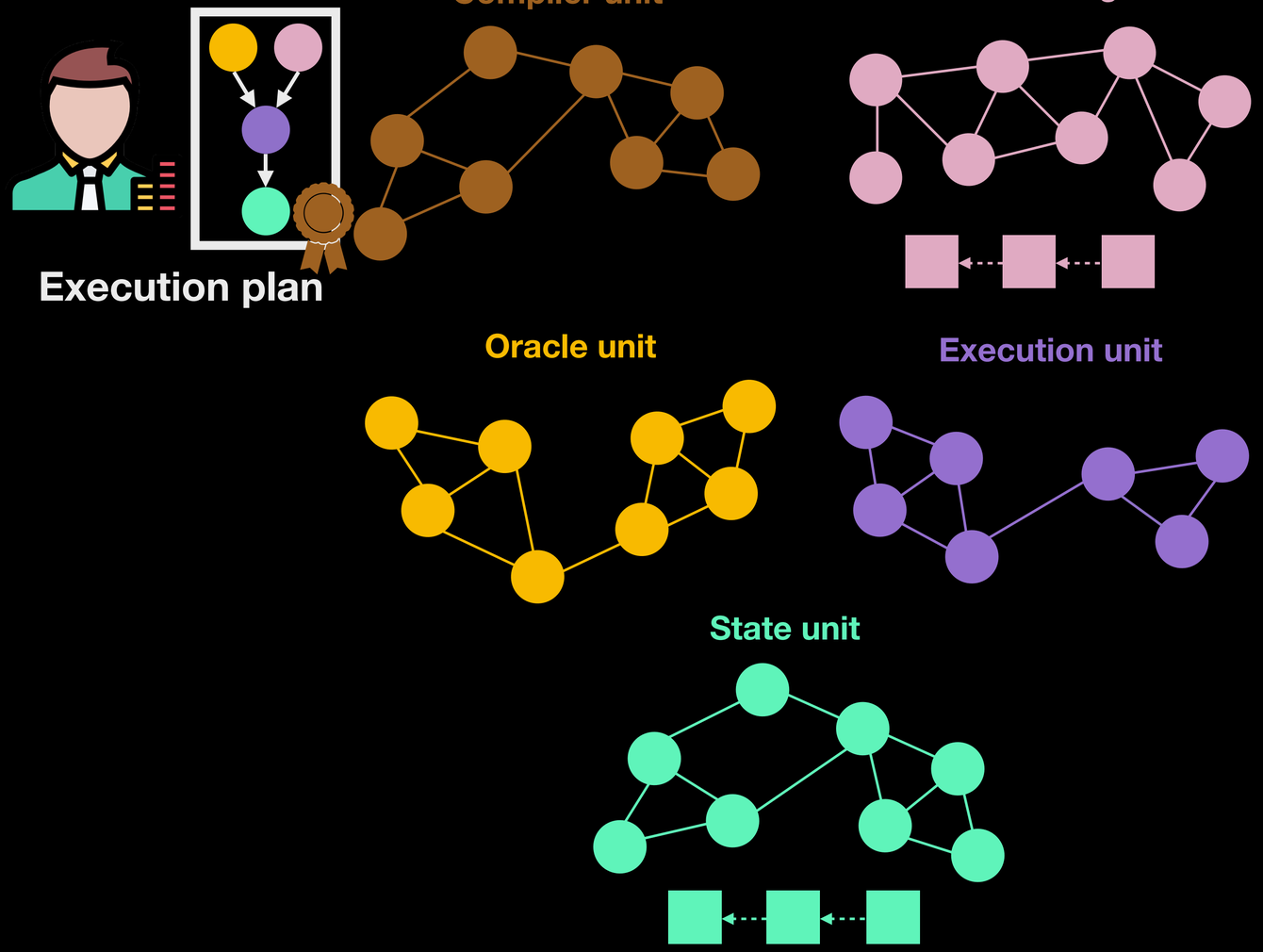




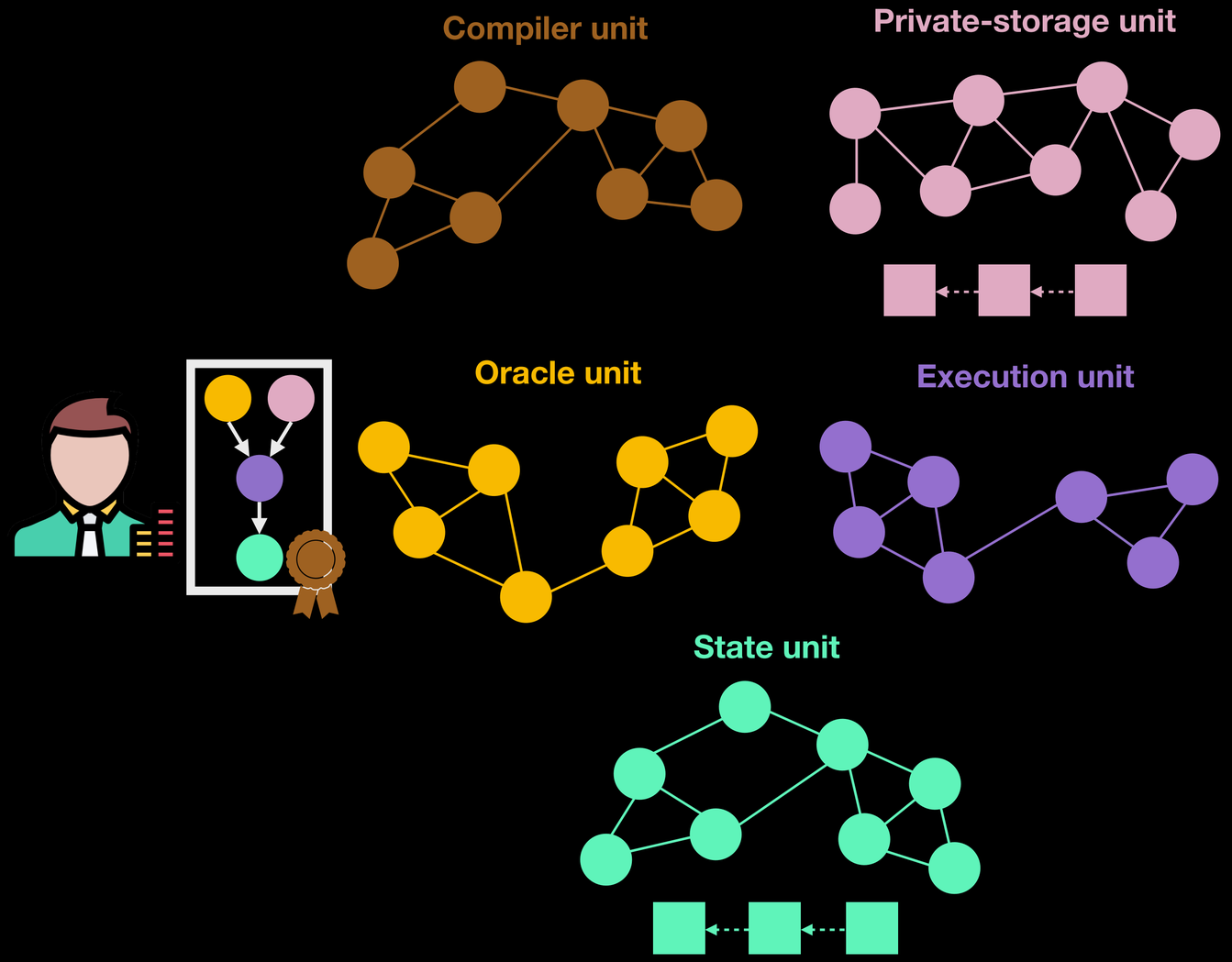




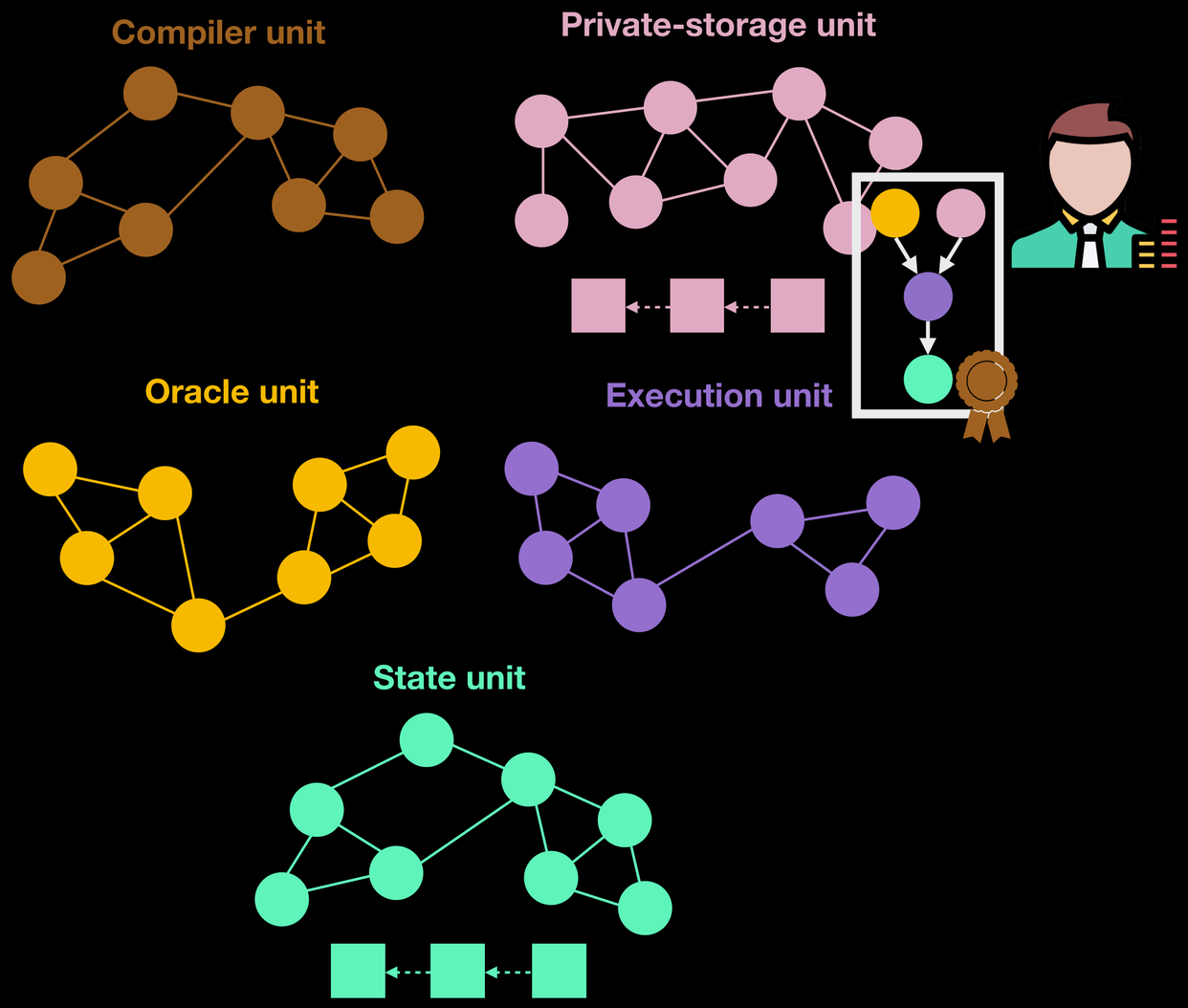
Executing applications



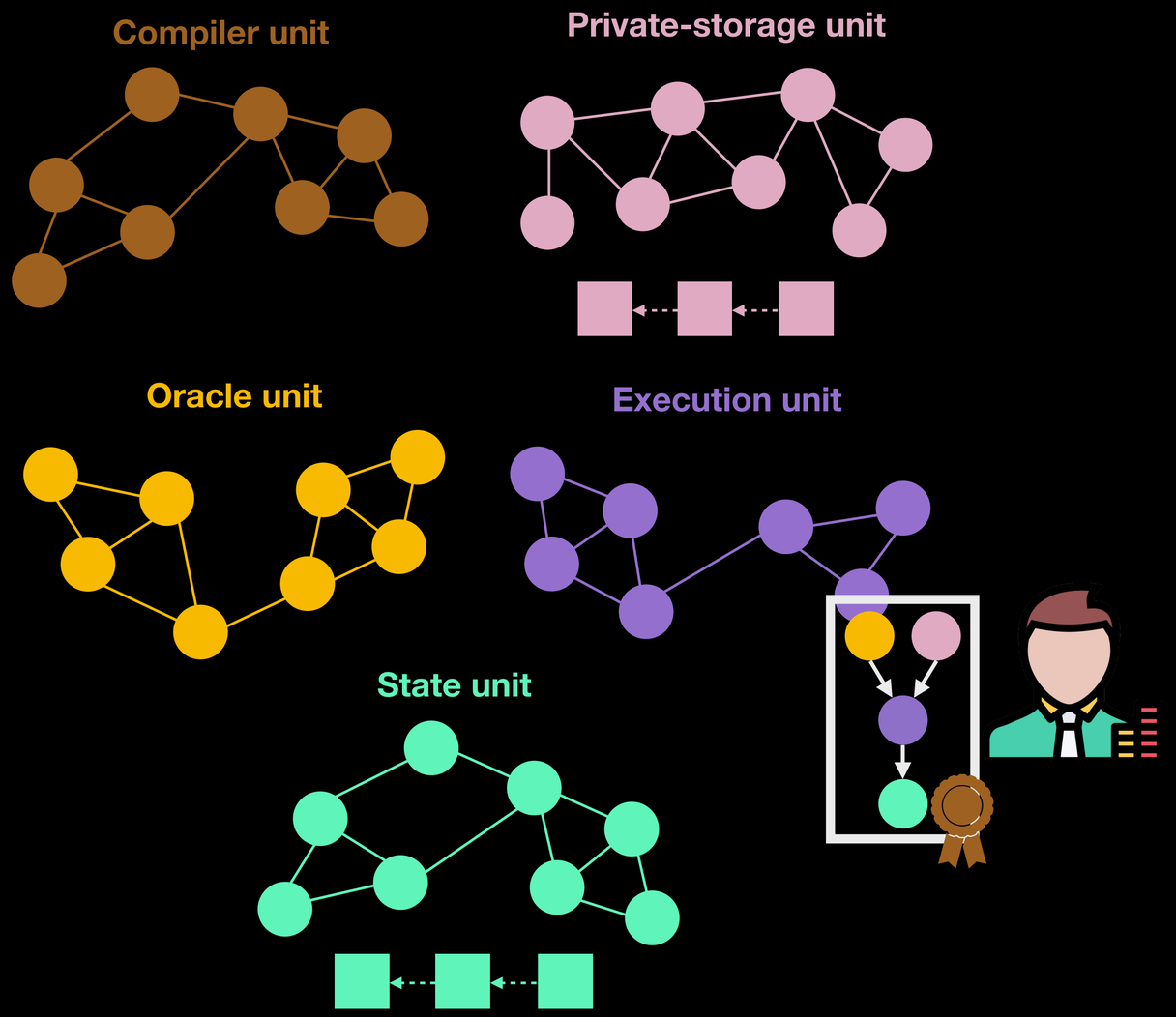
Executing applications



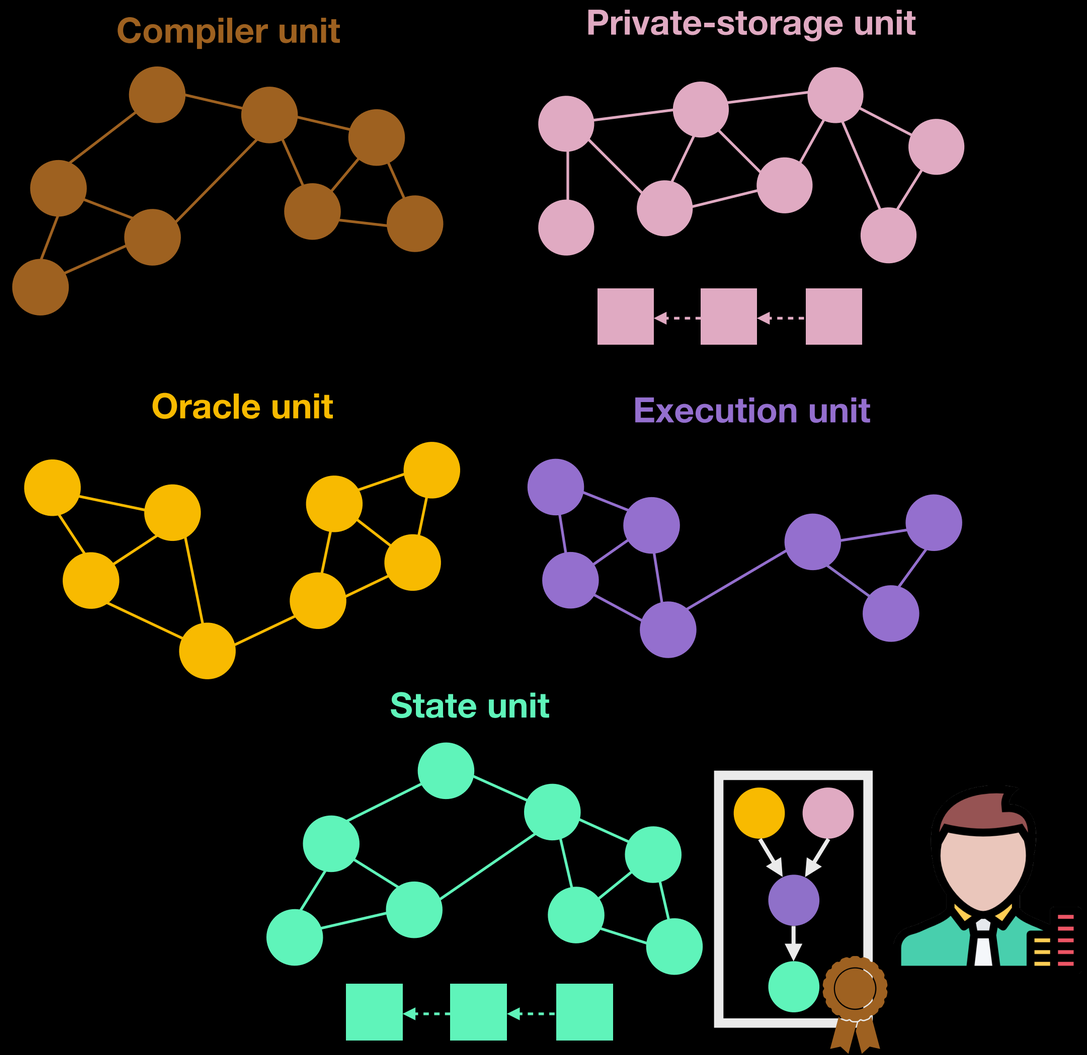
Executing applications



Executing applications

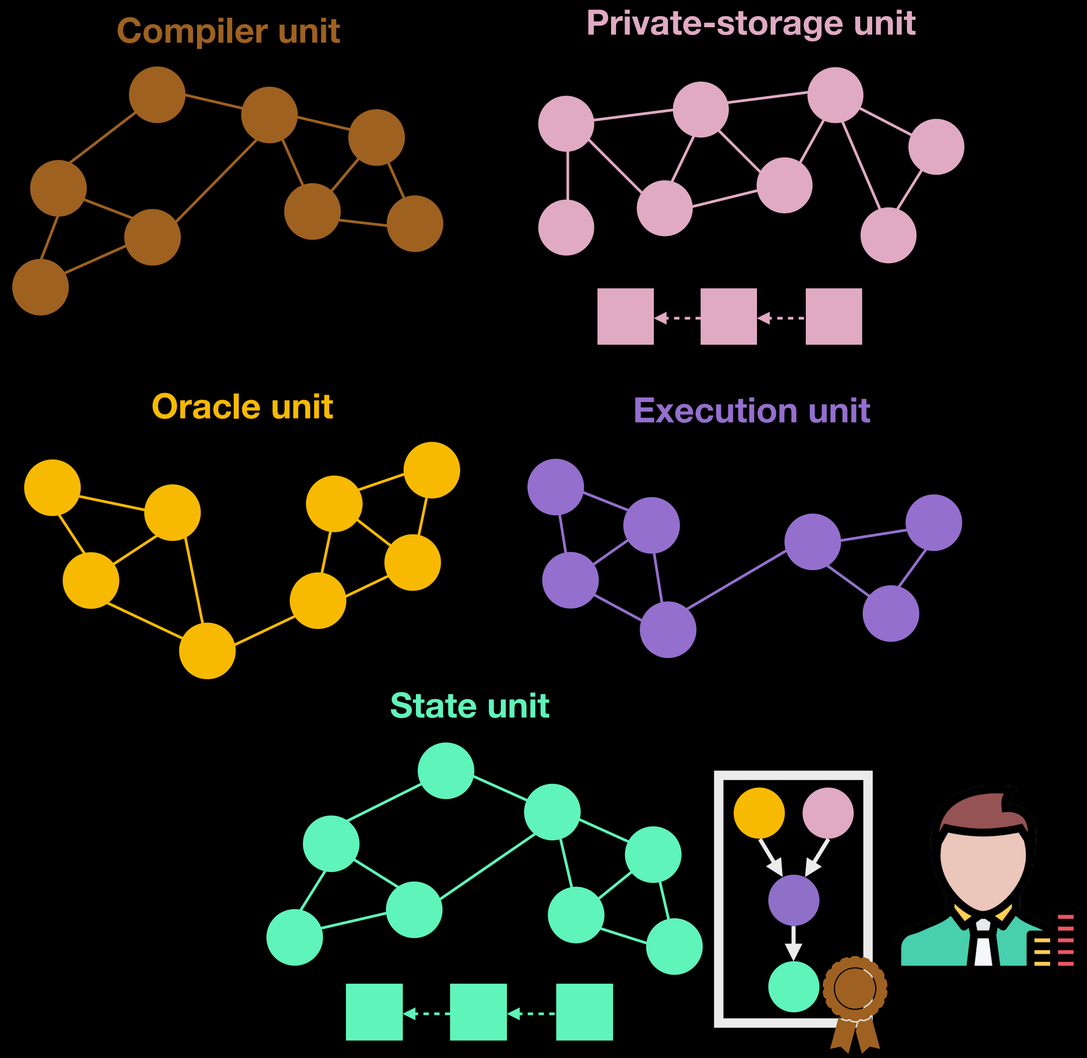


Executing applications



Executing applications

Inadvertently or maliciously deviate from the execution plan

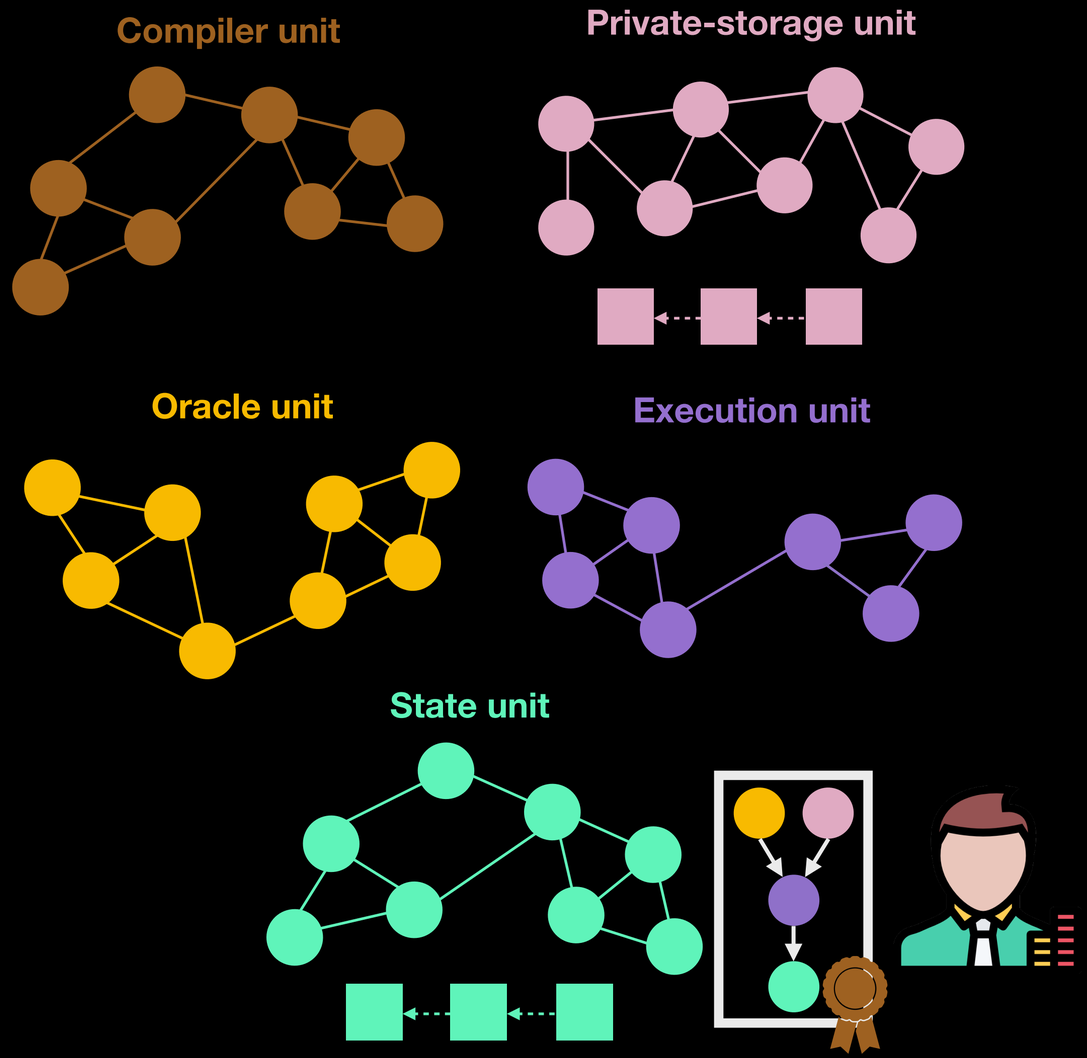


Executing applications

Inadvertently or maliciously deviate from the execution plan

Collective witnessing

- Collectively sign the execution plan
- Check signatures from parents are present



Summary

- PROTEAN: A modular architecture for building general-purpose decentralized applications
- Functional separation of nodes into special-purpose modules
- Enables applications currently insecure/impossible in smart contracts
- Permissionless evolution: easy/modular addition of new functionality
- Opportunity for node specialization for efficient execution

enis.alp@epfl.ch