Rethinking General-Purpose Decentralized Computing

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

HotOS XVII
May 13, 2019
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
- Access to reliable real-world data
- Store data off-chain
- 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
- Global hard forks
Monolithic architecture

Consensus and code execution are tightly coupled
Modular architecture

1. Parts required:
   - 6x
   - 28x
   - 12x
   - 16x
   - 10x
   - 20x

2. 16x
   - 4x
   - 2x
   - 1x
• Distributed systems that provide distinct specialized computations

• Similar to **microservices** architecture in cloud computing
Functional units

Ethereum

State & Execution unit
Functional units

State unit

Execution unit

PROTEAN
Functional units

- Private-storage unit
- State unit
- Execution unit

PROTEAN
Functional units

Private-storage unit

Oracle unit

PROTEAN

State unit

Execution unit
Functional units

- Private-storage unit
- Oracle unit
- PROTEAN
- Execution unit
- State unit
- Randomness unit
Functional units

- Private-storage unit
- Oracle unit
- Encryption unit
- Shuffler unit
- State unit
- Execution unit
- Randomness unit

PROTEAN
Functional units

- Private-storage unit
- Oracle unit
- Encryption unit
- State unit
- Execution unit
- Shuffler unit
- Randomness unit
- PROTEAN

OU1-v1
OU1-v2
Functional units

- Private-storage unit
- Oracle unit
- Encryption unit
- Shuffler unit
- State unit
- Execution unit
- Randomness unit

PROTEAN

OU1-v1
OU2-v1
OU1-v2
Functional units

- Oracle unit
- Private-storage unit
- Private-storage unit
- Randomness unit
- Encryption unit
- Execution unit
- Shuffler unit

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
Executing applications

- Oracle unit
- State unit
- Private-storage unit
- Execution unit

Reveal
Executing applications
Executing applications
Executing applications

Execution plan

Compiler unit

Oracle unit

State unit

Execution unit

Private-storage unit
Executing applications

- Compiler unit
- Private-storage unit
- Oracle unit
- Execution unit
- State unit
Executing applications
Executing applications
Executing applications

- Compiler unit
- Oracle unit
- Execution unit
- State unit
- Private-storage unit
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