SnT

Summary of Session 3:

Dependability and Security Aspects of Blockchain

83rd Meeting of the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance

Marcus Völp (marcus.voelp@uni.lu)

UNIVERSITY OF LUXEMBOURG

Two Talks

- **Securing Blockchain Systems: Codes and Human**
  Prof. Yang Xiang, Swinburne University, Australia

- **Blockchain Replication – Replicating Smart Contracts over multiple Blockchains for for Dependability**
  Prof. Miguel Correia, INESC-ID/IST, Portugal

Securing Blockchain Systems: Codes and Human

Presentation by Prof. Yang Xiang, Swinburne University of Technology

- **Provenance-Provided Data Sharing Model**
  => move access control to blockchain
- **Image-based Priv.-preserving Blockchain for Financial Services**
  => embedding encrypted images on blockchain
- **Automated Consent Management**
  => smart contracts to grant control over what stakeholders have and want
- **Hierarchical Data Model**
  => automated tests for sharability
- **DeFI enabled Data Sharing and Trading Systems**
  => smart contracts to discover and price information

Securing Blockchain Systems: Codes and Human

Presentation by Prof. Yang Xiang, Swinburne University of Technology

- **Privacy Protection**
  => tension between share and use
- **Incentives for Fed. Learning**
  => automated data sharing while minimizing incentives by measuring reputation
- **Security of cross chain smart contracts**
  => need basic mechanisms to obtain unified security across chains
- **Lots of interesting future work**
  - Smart contract audit framework
  - Anti-money laundry platform
  - Cross chain vulnerability detection
  - Real-time transaction path tracing
  - Fuzzing based dynamic smart contract vulnerability detection tool
  - Crypto exchange security audit
  - Smart contract lifelong monitoring

Securing Blockchain Systems: Codes and Human

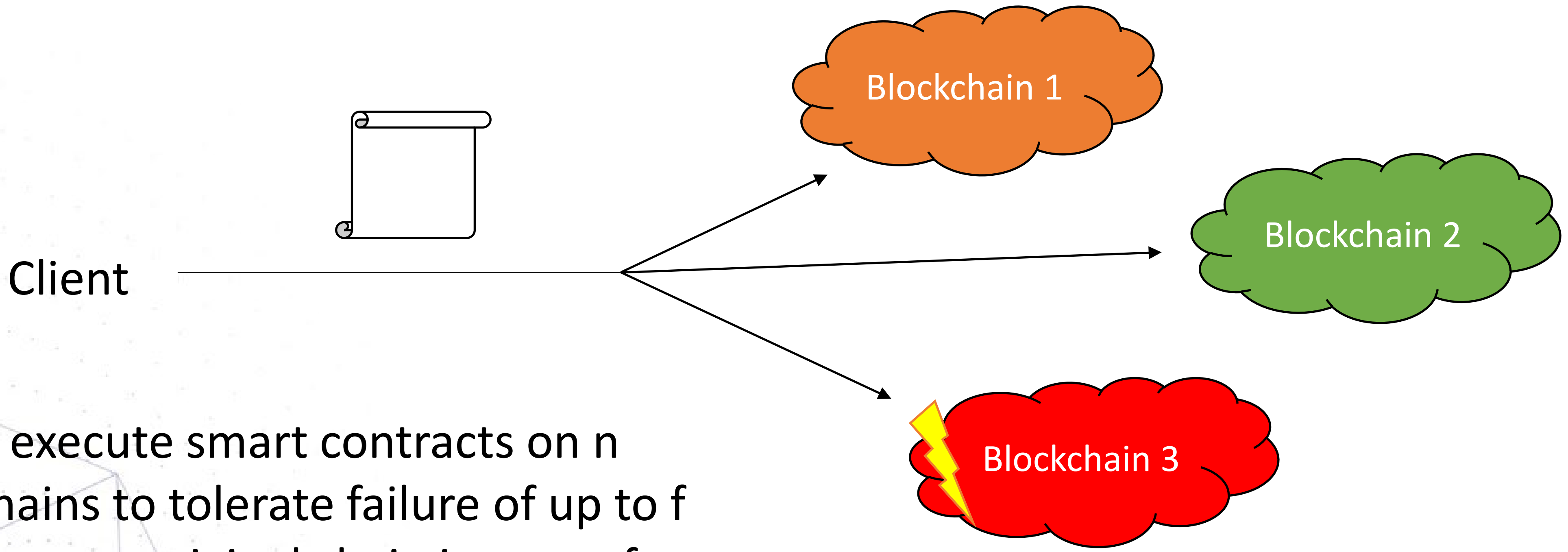
Presentation by Prof. Yang Xiang, Swinburne University of Technology

Discussion

- How much centralization (e.g., also in terms of governance) do we need to establish trustworthiness of the blockchain?
- Scalability
  => batching transactions helps increase throughput despite limited latency
  => also in Session 4 in terms of applying real application workloads
  => shift from consensus to transaction validation
- How to prevent / give users something back if they loose ownership over their data
  - Not possible as it requires changing the game of rule
  - Embed usage rules into blockchain stops when data leaves the chain
  - Processing on the chain remains prone to errors

Blockchain Replication: The Whys and The Hows
Replicating Smart Contracts for Dependability

Presentation by Prof. Miguel Correia, INESC-ID/IST



Clients execute smart contracts on n blockchains to tolerate failure of up to f

- E.g., prune original chain in case of fork

Blockchain Replication: The Whys and The Hows
Replicating Smart Contracts for Dependability

Presentation by Prof. Miguel Correia, INESC-ID/IST

- A lot of challenges
  - BCs are distributed systems themselves
  - Can’t change how blockchains execute (we can only use the smart contracts they support)
  - Contracts can’t communicate across chains
  - Contracts can’t sign
  - Weak finality (only after length d)
  - Correct only after reaching a nodes
  - Currencies have different prices
  - Interoperability issues

- Register Contracts
  - read / write w. regular consistency
  - quorum protocol
- Token Contracts (e.g., NFTs)
  - Data is no longer self-verifying
  - Solution:
    - Computation Conflict-free Replicated Data Types (CCRDTs)
- Faulty Clients

Blockchain Replication: The Whys and The Hows
Replicating Smart Contracts for Dependability

Presentation by Prof. Miguel Correia, INESC-ID/IST

Takeaways and Discussion

- First shot on replicated contracts
- many challenges, but also first solution (CCRDTs + quorum protocols)

- Benefits of combining CCRDTs + quorum protocols => stay out of sync, but synchronize eventually
- Blockchain immutability => confusing; datastructure is not; state of contracts are
- Clients could coordinate/execute the entire contract

Questions from Marcus

Securing Blockchain Systems

- Do we already know what set of mechanisms we need on the blockchain?
- How much of this functionality can already be provided as libraries, … for simple composition?

Blockchain Replication

- Application beyond blockchains?
- Pathway towards automatic translation of blockchain contracts to multi-blockchain contracts?