Smart Contract Security

Kepeng Li

Senior Standard Expert, Tencent
Mobile: +86-18682391020
Email: kernli@tencent.com

腾讯标准 Tencent Standard

ITU

Content

- Definitions of smart contracts
- Characteristics
- Security attacks
- Security challenges
- Security considerations in lifecycle management
- Related standards
- Industry practices

Definition of Smart Contract

- **Definition of smart contract [ITU-T X.1400]**: A program written on a distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated and triggered by specific conditions.
- **Definition of smart contract [ISO/TR 23455:2019]**：computer program recorded on a distributed ledger system wherein consensus about the effects of any execution of the program is recorded on the distributed ledger system.

Security Events Caused by Smart Contracts

- **In June 2016,** the DAO security breach resulted in $50 million in economic losses;
- **In July 2017,** the security breach of the multi-signature wallet caused by smart contracts resulted in economic losses of more than 182 million U.S. dollars;
- **In April 2018,** due to a security breach of one line of code, the market value of US$ 900 million was almost reduced to zero;
- **In May 2019,** a platform was hacked and more than 7,000 bitcoins were stolen.

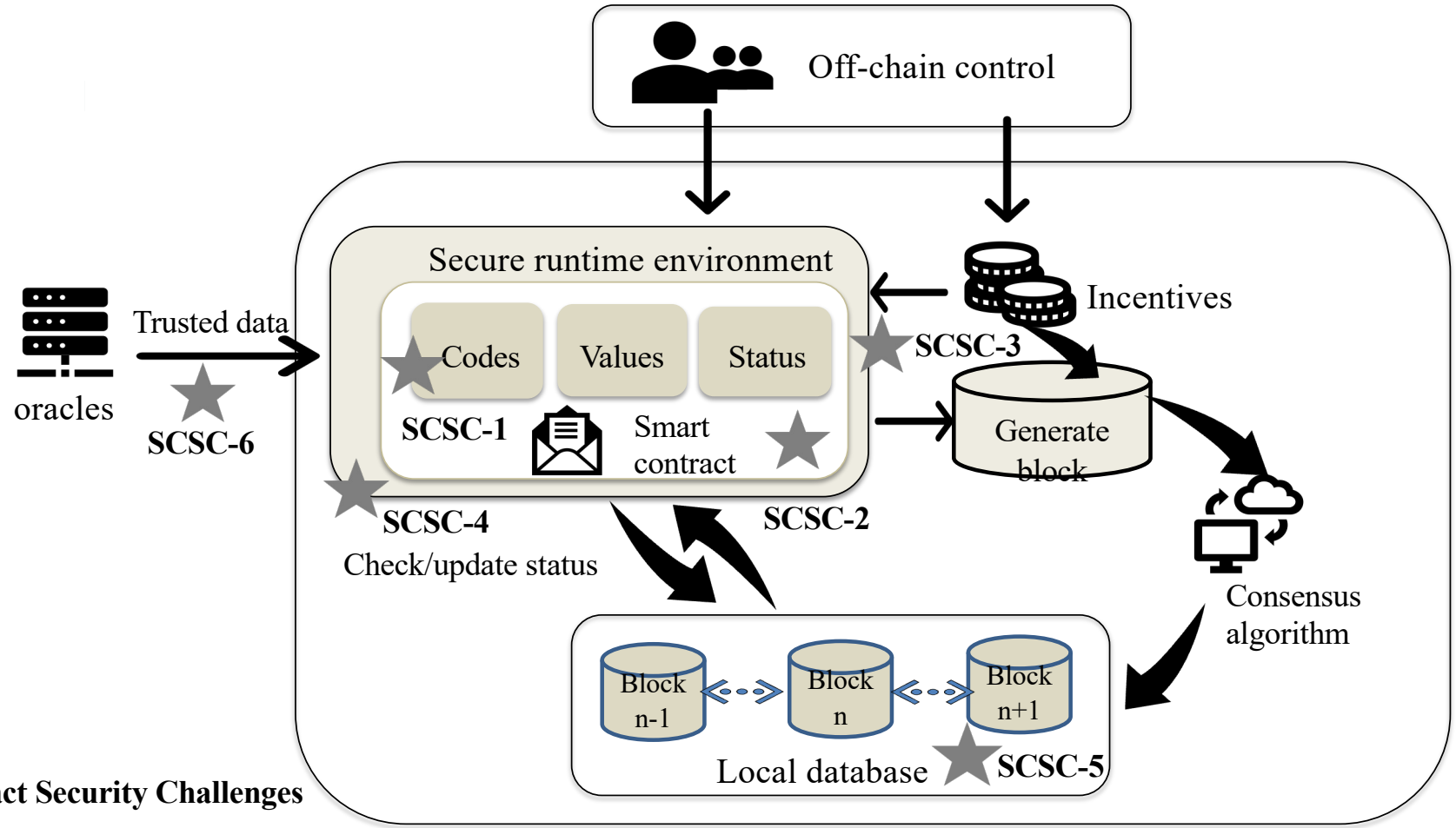
Characteristics of Smart Contracts

- Automation
- Tamper-proof
- Efficiency
- Low cost
- Transparent
- Traceable

Security Attacks to Smart Contracts

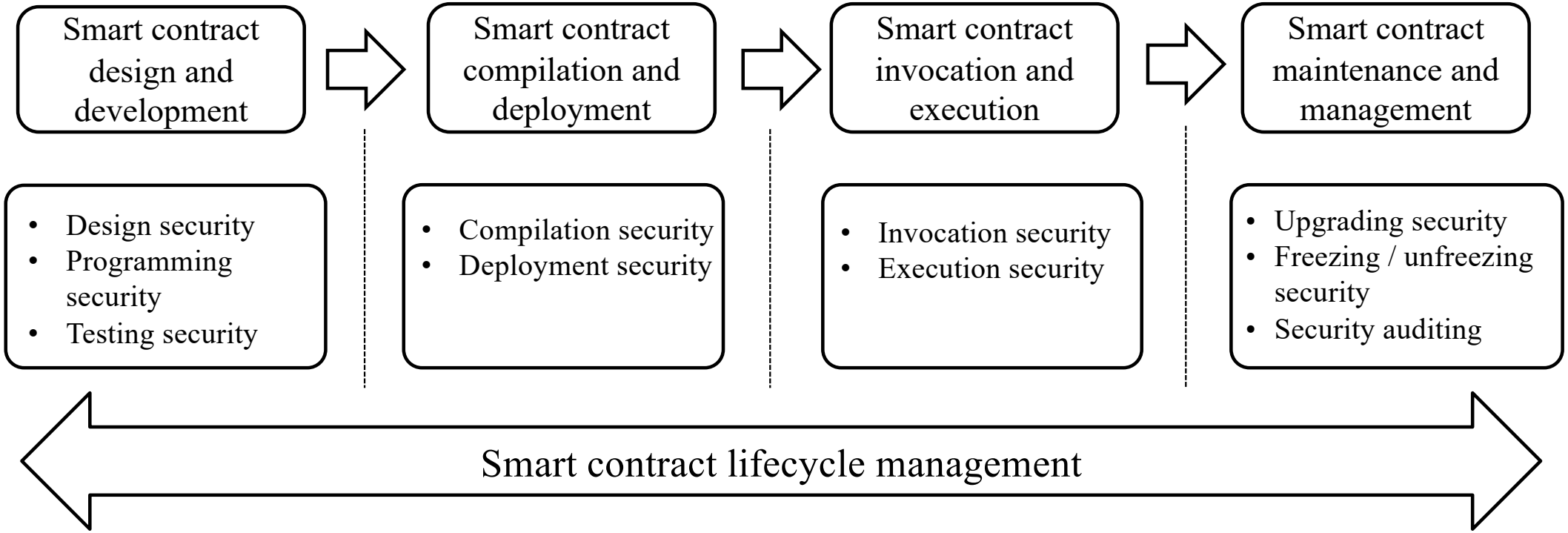
- Reentrant attack
- Call depth attack
- Transaction Order Dependency Attack
- Timestamp dependent attack
- Integer overflow attack
- Maloperation exception attack

Smart Contract Security Challenges



SCSC:
Smart Contract Security Challenges

Smart contract lifecycle management



Design and Development Security

Design Security

- Defect mitigation capability
- Sensitive information encryption
- Avoid predictable random numbers attack
- Avoid timestamp dependency attack
- … …

Development Security

- Development environment security
- Coding security: boundary conditions, avoid unreliable input, error handling, etc.
- Logical security: avoid sequence dependence risk, platform compliance, etc.

Testing Security

- Static security scanning
- Dynamic security scanning
- Formal verification

Compilation and Deployment Security

Compilation Security

- Mature and secure compilation tools
- Update compilation tools in time
- Guarantee code consistency
- … …

Deployment Security

- Get consensus before deployment
- Integrity verification before deployment
- Signature verification before deployment
- … …

Invocation and Execution Security

Invocation Security

- Have clear declarations for the interfaces
- Prevent untrusted external smart contracts
- Invocation scope verification
- Check and verify invocation parameters
- … …

Execution Security

- Execution environment security
- Data security
- Resource security

Maintenance and Management Security

Upgrading Security

- Online upgrading
- Retain historical versions
- Roll back
- … …

Freezing / unfreezing Security

- Freeze / unfreeze the smart contract
- User authentication and authorization

Security Auditing

- Audit the source code
- Audit the compilation environment security
- Audit execution environment security
- Keep auditing records

Related Standards

- **ITU-T SG17 Q14:**
  - **ITU-T X.srscm-dlt:** Security requirements for smart contract management based on the distributed ledger technology
- **ITU-T SG16 Q22:**
  - **ITU-T H.dlt-sclmr:** Smart contract lifecycle management requirements for distributed ledger technology systems
- **ISO TC 307:**
  - **ISO/TR 23455:2019:** Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
  - **ISO/WD TR 23642:** Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues

Tencent's practices

Account Authority Module

Support multiple account modules, including Cert、PWK、Public etc.

P2P Network Module

Self-developed LibP2P, Liquid two linking methods

Trading Engine Module

Batch transaction pool to process transactions in batches

Storage Module

Adapt LevelDB、BadgerDB、TikvDB、MySQL etc.

Consensus Module

Support multiple consensus algorithms, including RAFT，TBFT、ABFT etc.

Smart Contract Module

Security supports during the whole lifecycle management

Virtual Machine Module

Be compatible with Wasmer、Docker、EVM、WXVM etc.

Ecological Tool Module

Support cross-chain, Oracle, CMC, SDK etc.

Blockchain Assembly Line

Thank you!