ENTERPRISE
ETHEREUM
ALLIANCE

Tokenization Interest Group Webinar Series—Token Economics and Blockchain Security: Cyber, Information, Crosschain Mechanics

Benjamin Bukari, Co-Chair, EEA Tokenization Interest Group

Weijia Zhang, Co-Chair, EEA Crosschain Interoperability Group

Contents

1

Token Taxonomy

2

Crosschain Security

3

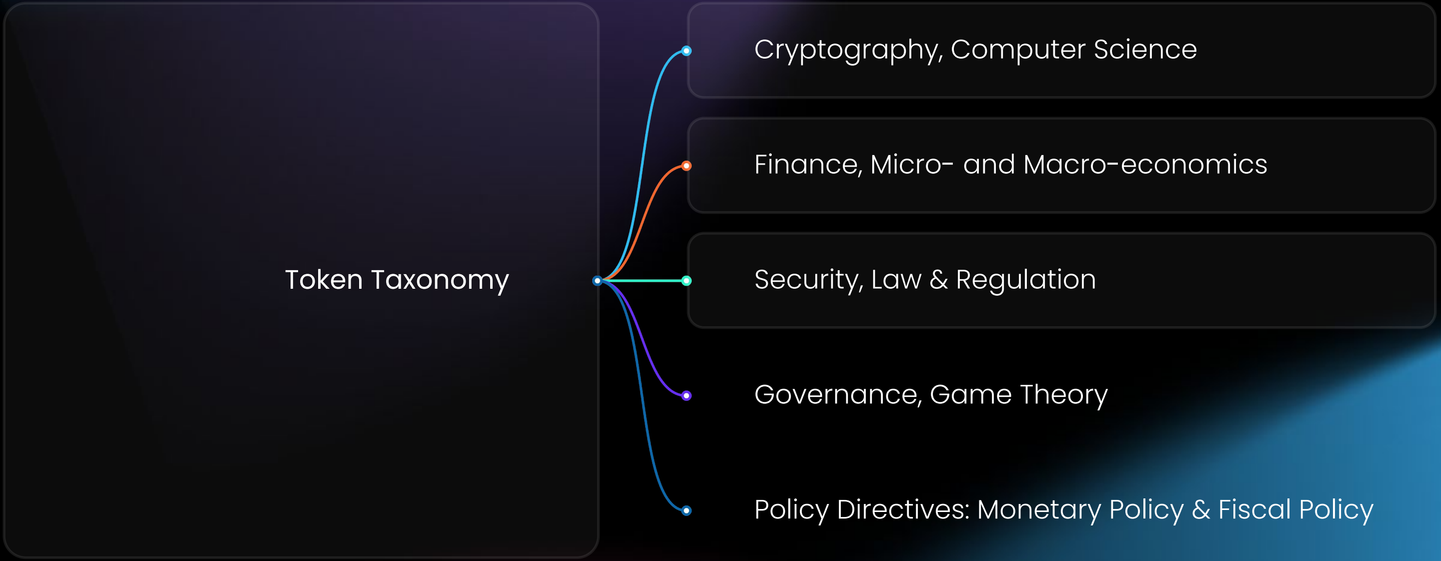
Smart Contract Development

4

Information Security Cybersecurity Data Privacy

Token Taxonomy

Token Taxonomy: Economic Designs for Distributed Systems



Token Taxonomy

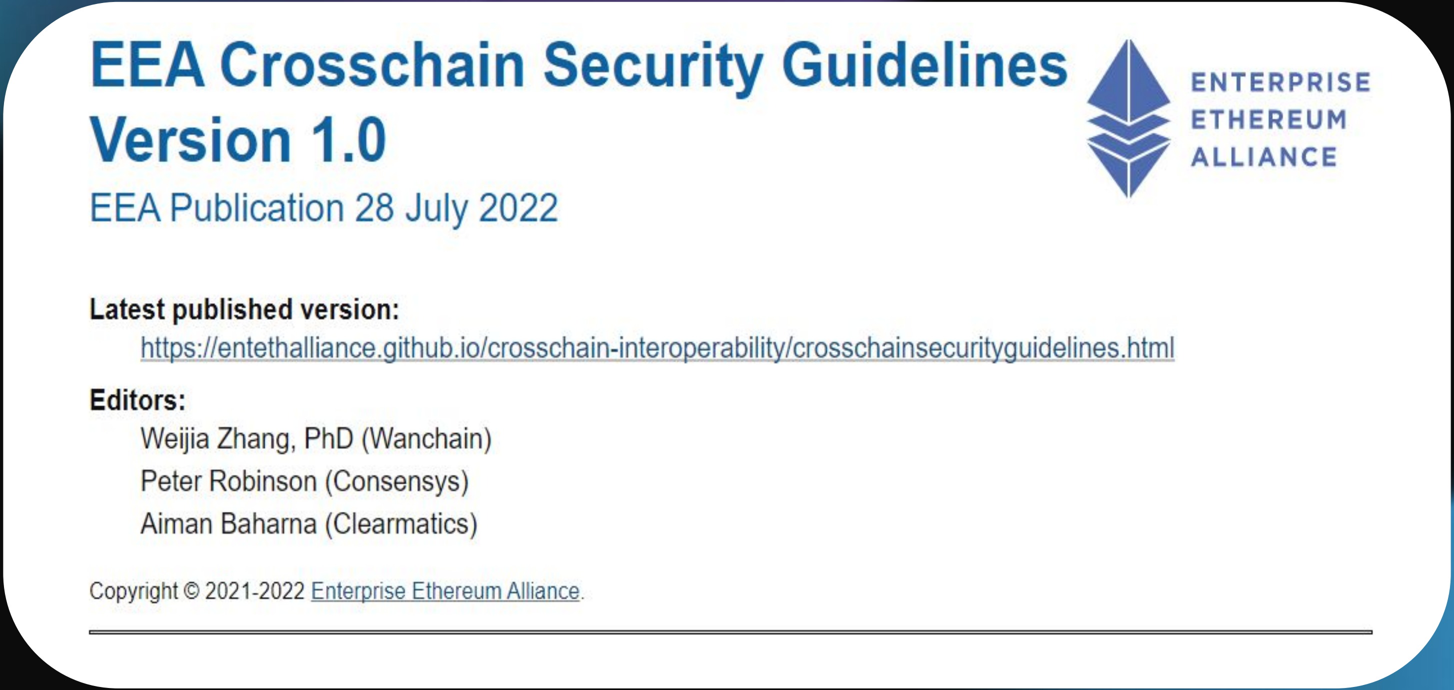
- Cryptography, Computer Science
- Finance, Micro- and Macro-economics
- Security, Law & Regulation
- Governance, Game Theory
- Policy Directives: Monetary Policy & Fiscal Policy

Crosschain Security

TOP 10 CROSSCHAIN BRIDGE HACKS

1.874 billion / year

2022-08-02	Nomad	Asset verification vulnerability	150
2022-06-24	Horizon	Validator private keys stolen	100
2022-03-29	Ronin Network	Attack on validator nodes	600
2022-03-20	Li.Finance	Vulnerability in getting external data	0.6
2022-02-06	Meter.io	Deposit verification vulnerability	4.2
2022-02-03	Womhole	Vulnerability of signature verification forgery	320
2022-01-28	Qbridge bridge	Deposit function vulnerability	80
2021-01-18	Multichain	Parameter management vulnerability	1.43
2021-08-10	Poly Network	Validator's Relayer public key replaced	610
2021-07-11	Chainswap	Consensus signature vulnerability	8



EEA Crosschain Security Guidelines Version 1.0

EEA Publication 28 July 2022

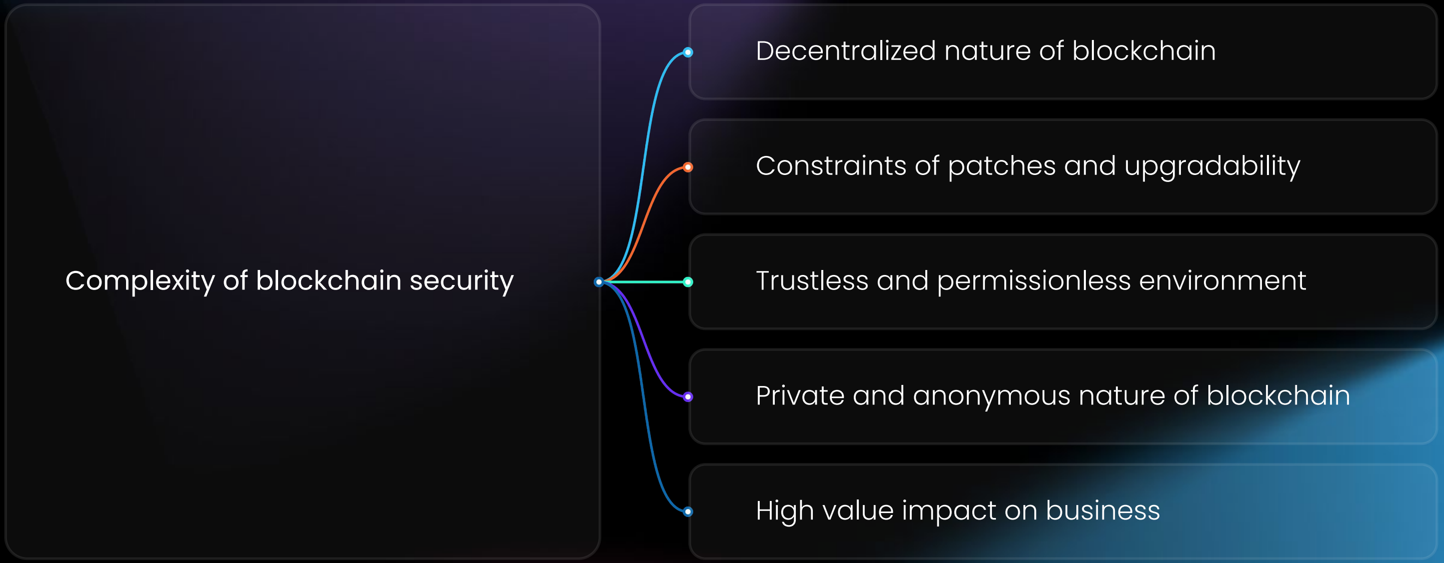
Latest published version:

https://entethalliance.github.io/crosschain-interoperability/crosschainsecurityguidelines.html

Editors:

Weijia Zhang, PhD (Wanchain)
Peter Robinson (Consensys)
Aiman Baharna (Clearmatics)

Complexity of Blockchain Security



Complexity of blockchain security

- Decentralized nature of blockchain
- Constraints of patches and upgradability
- Trustless and permissionless environment
- Private and anonymous nature of blockchain
- High value impact on business

COMPLEXITY OF BLOCKCHAIN SECURITY

Decentralization nature of blockchain

Any code written and deployed to the blockchain is going to run in thousands of machines

Anybody can access and run blockchain code

COMPLEXITY OF BLOCKCHAIN SECURITY

Constraints of patches and upgradability

Smart contracts deployed to blockchains cannot be modified

When security flaws are detected in blockchain applications, the cost of patching the applications is high and sometimes a fork of the blockchain is needed

COMPLEXITY OF BLOCKCHAIN SECURITY

Trustless and permissionless environment

For public blockchains, both the client nodes and decentralized applications are open to global participants

There is no security perimeter to block bad players from participating

COMPLEXITY OF BLOCKCHAIN SECURITY

Privacy and anonymous nature of blockchain

Blockchain users can remain anonymous

Smart contract functions do not have a way to check the profile of the users

Hackers can carry out blockchain attacks, get the assets, and remain unidentified

COMPLEXITY OF BLOCKCHAIN SECURITY

High value impact on business

Smart contracts manage high value crypto assets and each attack might bring catastrophic results to the decentralized application

Some decentralized applications have suffered huge losses due to simple errors in smart contracts

HACKING TECHNIQUES

Cybersecurity

Phishing
Malware
Ransomware
Spoofing
Adware
Zero Day threat
Brute Force Attack
Bot
Botnet
DDOS
Rootkit
RAT
Rug Pull

Smart Contracts

Function Vulnerabilities

Data Type and Data Vulnerabilities

Compiler Vulnerabilities

Randomness Vulnerability

Signature Vulnerability

Web3

Verification and Proof

Construction of TXs

User Interactions

Tx signing

CROSSCHAIN SECURITY:
BLOCKCHAIN LAYER

Discovery and identification of blockchains.

ChainIds:
EIP155, EIP3220

Chain protocols:
open protocol, XIPs

CROSSCHAIN SECURITY:
CONSENSUS LAYER

Who runs as miners for the native chains.

What consensus algorithm is used for the blockchains.

What finality does the consensus algorithm supply given the configuration.

What are the risks of blockchain rollbacks and forks.

CROSSCHAIN SECURITY:
RELAYER LAYER

Carry assets / messages / events / commands across chains.

Is an off-chain operation.

Can be permissioned or permissionless.

Permissioned: Governed by the integrity and truthfulness of the relayer administrators.

Permissionless: Guarded by asset staking, randomness, and multi-party computing.

CROSSCHAIN SECURITY:
SMART CONTRACT LAYER

The smart contract private key guarded with Hardware Security Module (HSM), Key Management System (KMS), hardware wallet, offline wallet, or secure vault technology.

Shared ownership with a multi-signature wallet.

Denounce the ownership of the smart contract.

Has drawback of no updatability.

CROSSCHAIN SECURITY: ORACLE LAYER

External to source chain, target chain and relayers.

Choose a trusted oracle service.

More work needs to be done in this area.

CROSSCHAIN SECURITY:
WEB SERVICE LAYER

Dapps have a web service layer that aggregate user actions and transform them into blockchain transaction raw data.

All cybersecurity considerations for the web should be followed.

Separate private key storage and transaction signing from any web services.

CROSSCHAIN SECURITY:
ADMINISTRATOR ACCOUNT

Administrator account hacking has happened multiple times

Deploy smart contract with hardware wallet or offline wallets

CROSSCHAIN SECURITY: USING MPC

Use MPC (multi-party computing) to safeguard the private key of for smart contract or lock account.

Shard a private key into multiple segments and each entity has a portion of the private key.

The private key is never created or stored.

Each MPC node signs the transactions individually.

The group signed transaction is verified.

CROSSCHAIN SECURITY: STAKING AND SLASHING

The security of the crypto assets will need to be safeguarded by assets staked by the bridge nodes.

Prevent collusion and wrongdoing by the bridge operators.

Similar to the PoS (proof of stake) blockchain consensus model Bridge.

Inactivity slashing.

Fraudulent slashing.

FACTORS TO CONSIDER FOR CROSSCHAIN EMERGENCY HANDLING

Pausing the bridge

Taking snapshot of blockchain states

Capping the bridge

(crosschain quota)

Effective upgrade path

Staking and slashing mechanism

Smart Contract Development

- Extensions (Smart contract modeling)
- Upgradeability
- New Releases & API Security
- Access Controls
- Role-Based Access Controls

Policy Objectives

Monetary Policy

Information Security, Cybersecurity, Data Privacy

Information Security, Cybersecurity, Data Privacy

- Goals, Hacks and Vulnerabilities, Best Practices

Policy Directives for
Monetary Policy

- Critical Infrastructure, NIST, ISO, SOC 2-3 Compliance

Questions