The Standards People

Security Implications for Successful Adoption of Smart Contracts

Presented by: **Tooba Faisal**

For: **EU Cyber Security week**

29.10.2020

Agenda

- Smart contracts: An introduction
- Applications of smart contracts
- Security challenges related to smart contracts
- Designing secure smart contracts

Smart contracts

Smart Contracts: An Introduction

Software codes installed on Permissioned Distributed Ledgers (PDLs)

PDLs : Distributed Immutable data structures where all the participants keep a copy of the ledger

Properties

- Immutable
  - Once recorded cannot be changed or amended
- Auto-executable
  - Triggered by software condition
- Transparent
  - Because they are installed on PDLs – all the participants of the ledger keep the same copy

Significance Examples

Certificate Authorities

Certificate Authorities (CA) are certificate issuer entities for websites. These certificates are authenticated by the browsers

Problems

- Single point of failure – a CA typically keeps record of all the trusted entities, and it has happened in the past* when a CA mistakenly or by cyber attack issued certificates to malicious parties
  - Solution: Distributed Trust through PDLs and Smart Contracts – since the trust is divided among several nodes in a PDL, (ex: a smart contract is invoked with record of every certificate issued)

* http://158.64.76.181/bitstream/10993/35468/1/blockchain-based-pki.pdf

Service Level Agreements (SLAs)

SLAs are the service contracts between the service provider and the consumer - Smart contracts can create service agreements which are:

- ✓ Accountable – service quality promised in the SLAs must be honored.
- ✓ Automated – service contracts are executed without any human intervention and penalties and rewards are paid automatically
- ✓ Transparent – service contracts are visible to both the parties.

* https://dl.acm.org/doi/10.1145/3411043.3412506

Smart contracts – Security challenges

Transparency

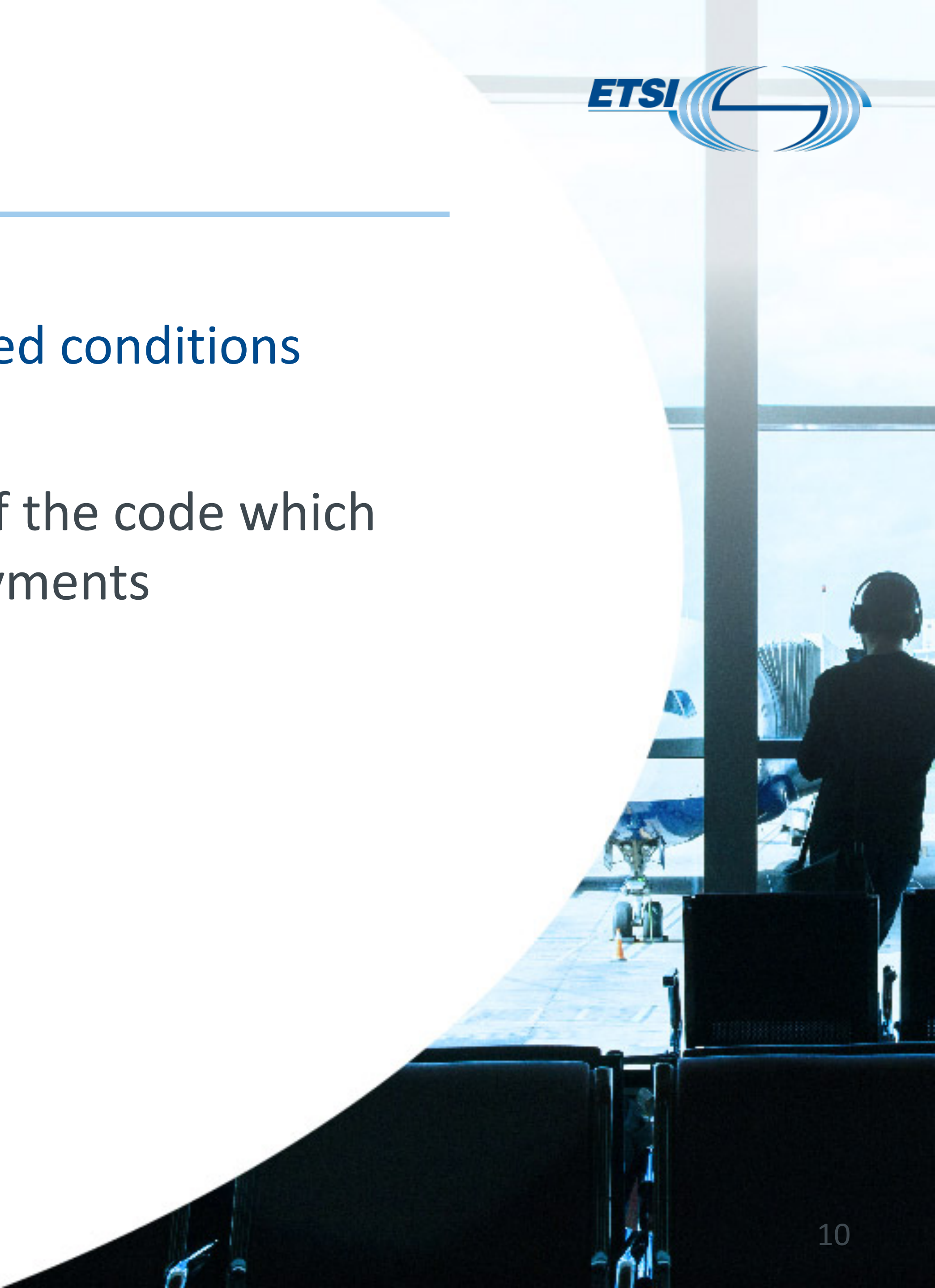
Because PDLs are transparent, smart contracts and all their respective transactions are visible to all the parties of the contract.

- Contracts are visible in a PDL, if a visibility domain is not specified, can cause contracts to be visible to unintended parties within the PDL.

Auto-executable

Smart contracts are self-executable – Pre-programmed conditions trigger these contracts.

- Erroneous code can trigger unwanted functions of the code which may cause monetary losses such as unwanted payments



Immutable

Smart contracts are immutable – because they are installed on a PDL, cannot be changed or amended:

- Smart contract can not be removed - old and dormant contracts if not secure can be dangerous
- If a smart contracts has some errors in a code it can leave back doors open- means they may be callable by unauthorized contracts

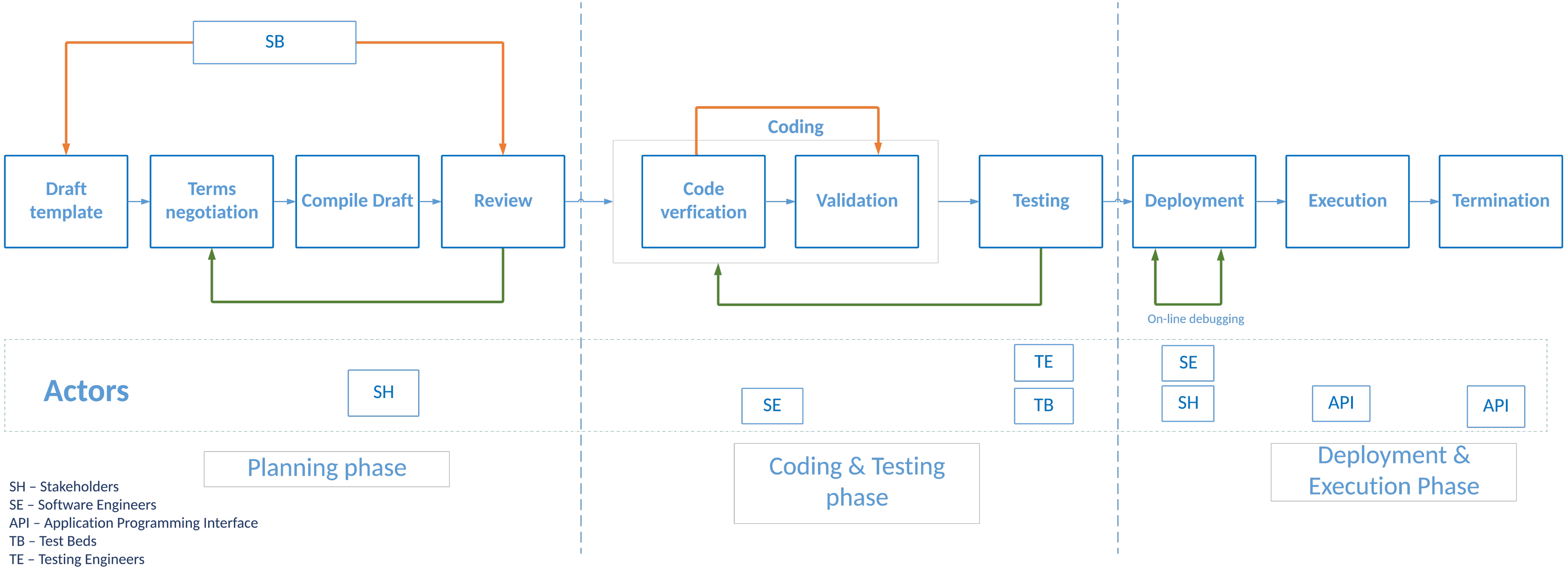
Designing secure smart contracts

Approaches

To design water-tight secure contracts. In ETSI-PDL 004 we discuss in detail

- Access control – a smart contract must be called by authorized parties only.
- Smart contract development life cycle – planning, development and deployment stages must be defined clearly.
- Three-pass approach

Smart Contract Development Life cycle



SH – Stakeholders
SE – Software Engineers
API – Application Programming Interface
TB – Test Beds
TE – Testing Engineers
SB – Standardisation Bodies

Three-Pass Approach

To mitigate the dangers smart contracts posses

- Execution clauses – absence of such clauses can make the newly deployed contracts dormant
- Penetrable clauses – such clauses can cause the contracts unauthorized contracts to access the smart contracts -
- Termination clauses – Eternal contracts can be dangerous hence must be terminated exclusively. Presence of a termination clause inside the contract must be checked before deployment.

Conclusion

Securing smart contracts is important

- Smart contracts are a potential solution for future accountable, transparent and autonomous contracting mechanism
- They provide a methods to create traceable audit mechanism
- Securing smart contracts are of important to secure future generation contracts
- Security of smart contracts can be achieved by careful planning.