ITU – NBTC Training
On

“Building Distributed Ledger Technologies (Blockchain) Projects”

5 – 8 November 2019,
Bangkok, Thailand

ITU – NBTC Training

Session 5: Security Issues in DLTs

Objective: To provide an overview of security issues in DLTs

6 November 2019,
Bangkok, Thailand

ITU – NBTC Training – Session 5

Overview of this 90-minute session:

- **User errors and private key management:** 15 minutes
- **Overview of 51% attacks:** 5 minutes
- **Social threats:** 10 minutes
- **Infrastructure threats:** 10 minutes
- **Technological threats:** 10 minutes
- **Smart contract vulnerabilities:** 15 minutes
- **Reviewing key terms and topics:** 10 minutes
- **Question and answer:** 15 minutes

ITU – NBTC Training – Session 5

Overview of this 90-minute session:

- **User errors and private key management:** 15 minutes
- **Overview of 51% attacks:** 5 minutes
- **Social threats:** 10 minutes
- **Infrastructure threats:** 10 minutes
- **Technological threats:** 10 minutes
- **Smart contract vulnerabilities:** 15 minutes
- **Reviewing key terms and topics:** 10 minutes
- **Question and answer:** 15 minutes

ITU – NBTC Training – Session 5

- **Part 1 User errors and private key management:** 15 minutes
  - Issues
    - Loss of private keys
    - Phishing / keystroke logging
    - Sending funds to the wrong address
  - Solutions
    - Paper wallets
    - Hardware wallets
    - Multi-signature accounts
    - Shamir secret sharing
    - Transaction vouchers

ITU – NBTC Training – Session 5

Part 1.1

Issues

- **Loss of private keys**
- Phishing / keystroke logging
- Sending funds to the wrong address

ITU – NBTC Training – Session 5

Loss of private keys

Because of the nature of public key cryptography, you are the sole owner of your private key.

If you lose it, you lose access to your data – there is no central entity that can reset your password or provide administrative access.

ITU – NBTC Training – Session 5

Part 1.1

Issues

- Loss of private keys
- **Phishing / keystroke logging**
- Sending funds to the wrong address

ITU – NBTC Training – Session 5

Phishing and keystroke logging

Phishing - A fake email from someone pretending to be your insurance company or employer requesting that you sign an important document online with your private key.

Keystroke logging - A keylogger, sometimes called a keystroke logger or system monitor, is a type of surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard. Keylogger software is also available for use on smartphones, such as Apple's iPhone and Android devices.

Keyloggers are often used as a spyware tool by cybercriminals to steal personally identifiable information (PII), login credentials and sensitive enterprise data.

ITU – NBTC Training – Session 5

Phishing and keystroke logging

If someone copies your private key through a fake log-in portal or by logging your keystrokes, they have access to all of your funds and data related to that account.

- *This amounts to essentially stealing your digital identity – and no one can help return your funds to you once they are stolen from your account.*

ITU – NBTC Training – Session 5

Part 1.1

Issues

- Loss of private keys
- Phishing / scams
- **Sending funds to the wrong address**

ITU – NBTC Training – Session 5

Sending funds to the wrong address

Once you sign a transaction and funds have left your account, there is no way to return the funds.

With complex alpha-numeric public addresses used to identify accounts, it is very easy to accidentally copy and paste the wrong address, resulting in an irreversible fund transfer.

ITU – NBTC Training – Session 5

Part 1.2

Solutions

- Paper wallets
- Hardware wallets
- Multi-signature accounts
- Shamir secret sharing (SSS)
- Namespaces and aliases
- Transaction vouchers / fixed invoices

ITU – NBTC Training – Session 5

Part 1.2

Solutions

- **Paper wallets**
- Hardware wallets
- Multi-signature accounts
- Shamir secret sharing (SSS)
- Transaction vouchers / fixed invoices

ITU – NBTC Training – Session 5

Paper wallets

According to CoinDesk:

A paper wallet is simply a public and private key printed together. It is an offline wallet, and is usually regarded as a type of “cold storage” (extra-secure storage that does not make contact with the hackable internet), although it has some important differences that make its presence in that category debatable (more on this further down).

As the name suggests, paper wallets are usually made out of paper, although technically they could also be made of plastic or any other substance on which information can be durably printed

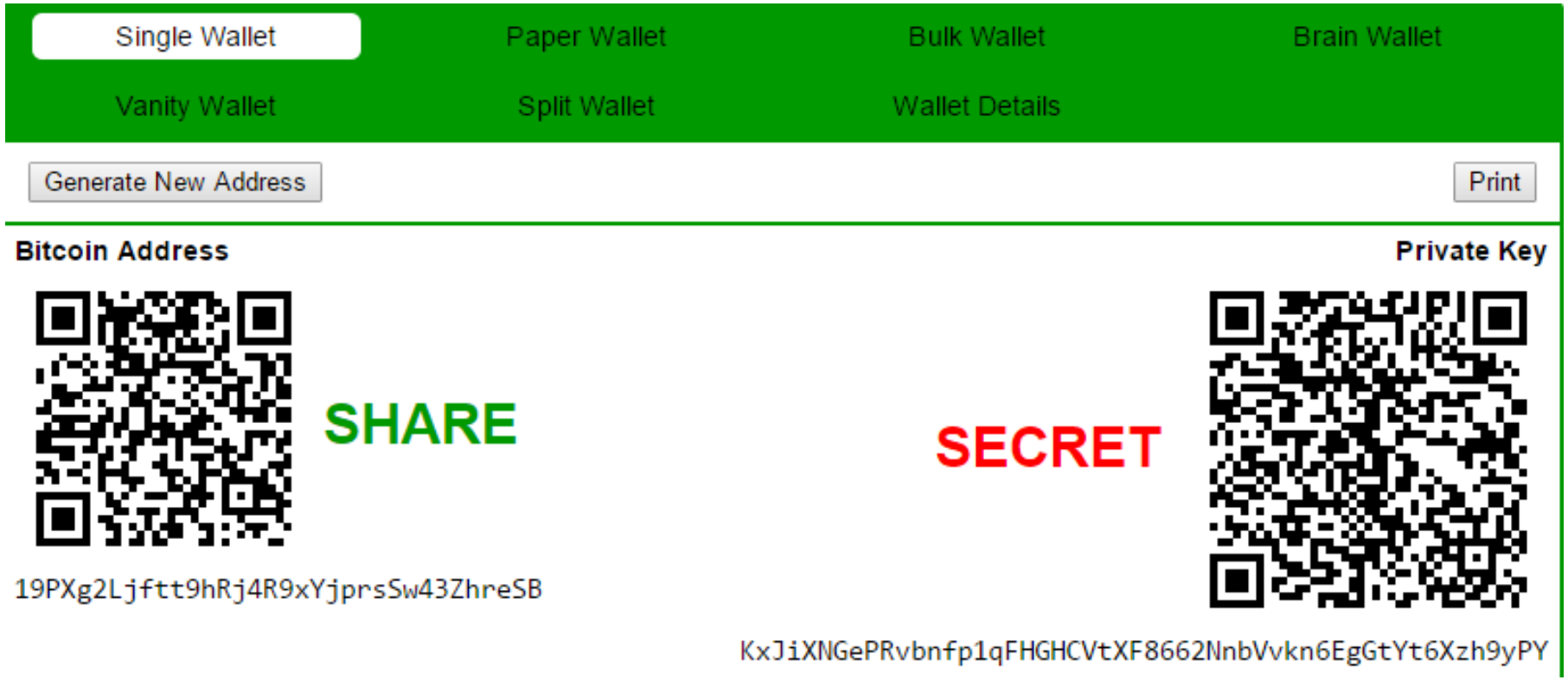
The key generation is usually done in your browser, so they are never transmitted on the internet. To be safe, you should clear your browser after printing. And never store an image of the paper wallet on your computer or phone.

Pro: no trusting of a 3rd party
Con: if you lose the paper or someone finds your hiding place, your account is gone

ITU – NBTC Training – Session 5

Paper wallets

According to CoinDesk:



ITU – NBTC Training – Session 5

Part 1.2

Solutions

- Paper wallets
- **Hardware wallets**
- Multi-signature accounts
- Shamir secret sharing (SSS)
- Transaction vouchers / fixed invoices

ITU – NBTC Training – Session 5

Hardware wallets

According to Bitcoin Wiki:

A **hardware wallet** is a special type of wallet which stores the user's private keys in a secure hardware device. Many times these devices can store multiple types of cryptocurrencies at once so that you need only 1 PIN to sign transactions.

They have major advantages over standard software wallets:

- private keys are often stored in a protected area of a microcontroller, and cannot be transferred out of the device in plain text
- immune to computer viruses that steal from software wallets
- can be used securely and interactively, private keys never need to touch potentially-vulnerable software
- much of the time, the software is open source, allowing a user to validate the entire operation of the device

Pro: secure

Con: if you lose your PIN and your back-up private seed, you still lose your coins!

ITU – NBTC Training – Session 5

Hardware wallets

ITU – NBTC Training – Session 5

Part 1.2

Solutions

- Paper wallets
- Hardware wallets
- **Multi-signature accounts**
- Shamir secret sharing (SSS)
- Transaction vouchers / fixed invoices

ITU – NBTC Training – Session 5

Multi-signature accounts

According to Bitcoin Wiki:

Multisignature (multisig) refers to requiring more than one key to authorize a transaction. It is generally used to divide up responsibility for possession of value on the blockchain.

Pro: multiple private keys required, so if only 3 out of 5 keys are available, you can still send funds

Con: many platforms require trusting a 3rd party service provider or creating a specifi smart contract to manage the multi-sig functionality

ITU – NBTC Training – Session 5

Part 1.2

Solutions

- Paper wallets
- Hardware wallets
- Multi-signature accounts
- **Shamir secret sharing (SSS)**
- Transaction vouchers / fixed invoices

ITU – NBTC Training – Session 5

Shamir secret sharing (SSS)

According to MIT:

Shamir secret sharing - refers to dividing a private key into **n** pieces that is easily reconstructable using **k** pieces, where even a small amount of information about one of **k** pieces reveals nothing about the full private key.

Common misconception:

“Wouldn’t someone be able to brute force one of the k pieces since my private key has been divided into smaller pieces?”

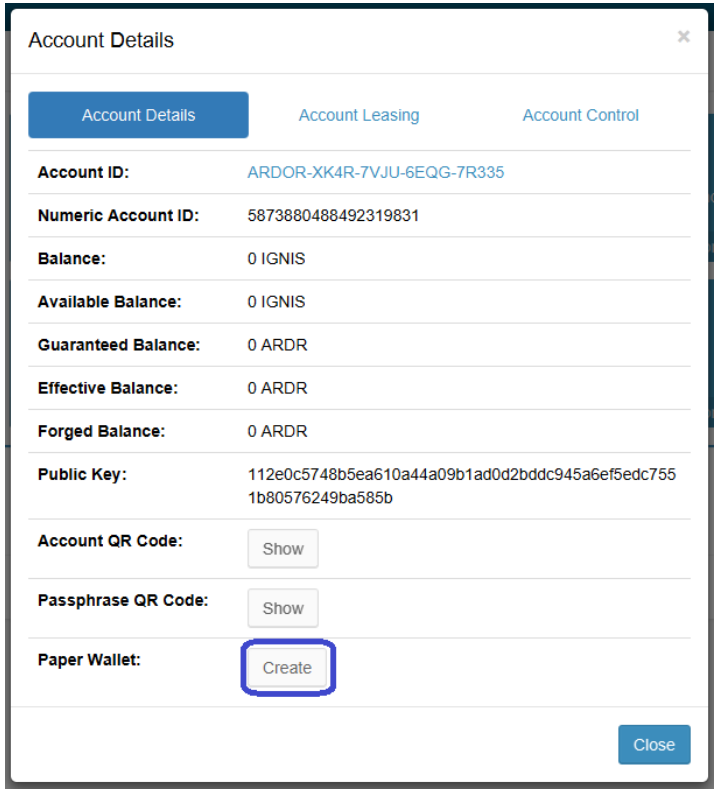
NO

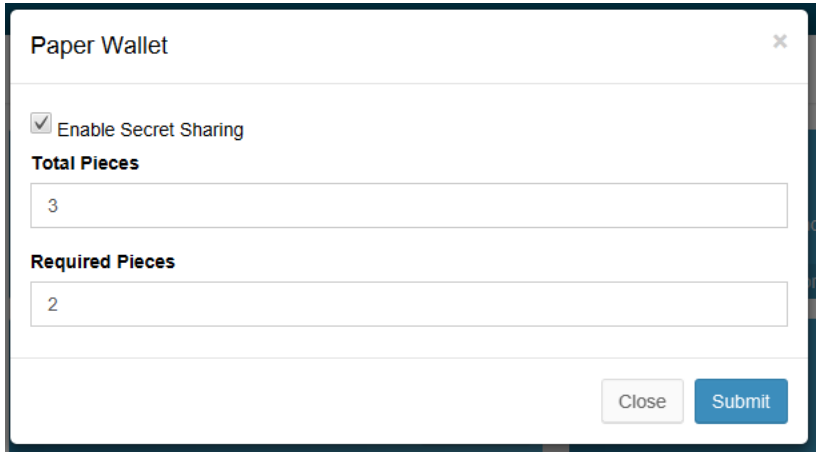
- Each of the new pieces generated in the SSS process are just as long as the original private key.
- No loss of security in the cryptographic security of the passphrase itself.

ITU – NBTC Training – Session 5

Shamir secret sharing (SSS)

Example of auto-SSS generator on Ardor:





ITU – NBTC Training – Session 5

Part 1.2

Solutions

- Paper wallets
- Hardware wallets
- Multi-signature accounts
- Shamir secret sharing (SSS)
- **Transaction vouchers / fixed invoices**

ITU – NBTC Training – Session 5

Transaction vouchers / fixed invoices

Transaction vouchers / fixed invoices - refers to creating an invoice that is addressed to one specific public address and signed by both the sender and receiver prior to transaction execution.

Public key cryptography ensures every public address has a unique private key associated with it. If you entered the incorrect address, then when your intended receiver attempts to sign the transaction – their private key won't match the faulty address you entered. Simply discard the voucher/invoice and request a new transaction.

Pro: ensures funds always go where they are meant to
Con: slower since both parties must sign the transaction

ITU – NBTC Training – Session 5

ITU – NBTC Training – Session 5

Overview of this 90-minute session:

- **User errors and private key management :** 15 minutes
- **Overview of 51% attacks:** 5 minutes
- **Social threats:** 10 minutes
- **Infrastructure threats:** 10 minutes
- **Technological threats:** 10 minutes
- **Smart contract vulnerabilities:** 15 minutes
- **Reviewing key terms and topics:** 10 minutes
- **Question and answer:** 15 minutes

ITU – NBTC Training – Session 5

- **Overview of 51% attacks:** 5 minutes

A 51% attack is when more than half of the block producing validating nodes of the DLT or blockchain network collude to tamper with the historical integrity of the blockchain by trying to force a new version of the history as the “true” one.

ITU – NBTC Training – Session 5

➢ Overview of 51% attacks:

- In proof of work
  - Miners don't need to be actual users of the network, they can simply attack the network by investing in the necessary computer hardware and then repurposing this hardware later.
    - Cost of 51% attacking most PoW networks is quite low, but is an ongoing cost
- In proof of stake
  - Stakers / Forgers need to actually purchase tokens to participate in consensus, therefore an attack on the network would be an attack on their own holdings.
    - Cost of 51% attack on PoS networks is generally higher than PoW, but is a one time cost
- In consortiums / BFT
  - If half the companies maintaining the ledger decide it is in their benefit to begin manipulating the network, they can collude to do so.

ITU – NBTC Training – Session 5

Overview of this 90-minute session:

- **User errors and private key management:** 15 minutes
- **Overview of 51% attacks:** 5 minutes
- **Social threats:** 10 minutes
- **Infrastructure threats:** 10 minutes
- **Technological threats:** 10 minutes
- **Smart contract vulnerabilities:** 15 minutes
- **Reviewing key terms and topics:** 10 minutes
- **Question and answer:** 15 minutes

ITU – NBTC Training – Session 5

Part 3.1

Social threats

- Collusion
- Hash wars
- Sybil attack

ITU – NBTC Training – Session 5

Part 3.1

Social threats

- **Collusion**
- Hash wars
- Sybil attack

ITU – NBTC Training – Session 5

Collusion

Secret or illegal cooperation or conspiracy to cheat or deceive others

ITU – NBTC Training – Session 5

Collusion

- Proof of work
  - Mining pools – a group of miners who work together to share the costs and rewards of participating in the consensus process
- Proof of stake
  - Staking / forging pools – similar to mining pools, but in POS
  - Individual whales collude with one another
- Byzantine fault tolerance
  - Industry players work together to manipulate the market

ITU – NBTC Training – Session 5

Part 3.2

Social threats

- Collusion
- **Hash wars**
- Sybil attack

ITU – NBTC Training – Session 5

Hash wars

Hash wars, or a contentious hard fork - refers to the process of trying to supplant an existing ledger with a new version by using hash power to attack the competing network

According to CoinSutra:
Hash Rate, also **Hash Power**, is the measuring unit that measures how much **power** the **Bitcoin** network is consuming to be continuously functional. By continuously functional I mean how much **hash power** is it consuming to generate/find blocks at the normal mean time of 10 minutes.

Example from CoinDesk: Bitcoin vs. Bitcoin Cash vs Bitcoin SV vs Bitcoin ABC

ITU – NBTC Training – Session 5

Part 3.2

Social threats

- Collusion
- Hash wars
- **Sybil attack**

ITU – NBTC Training – Session 5

Sybil attack

A type of attack in peer-to-peer networks in which a node in the network operates multiple identities actively at the same time and undermines authority/power in reputation systems.

Sybil attack

- In proof of work and proof of stake
  - Miners and stakers/forgers generally do not need to register their names or identity, so a network could be run entirely by one individual or one group.
  - Performing some level of KYC at the outset can help avoid this, but truly anonymous or pseudonymous networks have a difficult time proving sybil-resistance.
- In consortiums / BFT
  - **Since most private permissioned networks will consist of a consortium of companies or individuals who signed up to participate, these types of networks are generally sybil-resistant by design.**

Definitively proving resistance against a sybil attack remains one of the most powerful arguments against most public blockchain networks that do not perform any KYC.

ITU – NBTC Training – Session 5

Overview of this 90-minute session:

- **User errors and private key management:** 15 minutes
- **Overview of 51% attacks:** 5 minutes
- **Social threats:** 10 minutes
- **Infrastructure threats:** 10 minutes
- **Technological threats:** 10 minutes
- **Smart contract vulnerabilities:** 15 minutes
- **Reviewing key terms and topics:** 10 minutes
- **Question and answer:** 15 minutes

ITU – NBTC Training – Session 5

Part 4

Infrastructure threats

- Extreme weather
- Power outages
- Calculated attack

ITU – NBTC Training – Session 5

Part 4.1

Infrastructure threats

- **Extreme weather**
- Power outages
- Calculated attack

ITU – NBTC Training – Session 5

Extreme weather

- If the majority of nodes for a DLT system are located geographically close to one another, then a major weather event could knock out a substantial portion of the infrastructure for securing the network, leaving it vulnerable.
  - For private permissioned networks run by small consortiums, this is a legitimate concern.
  - For public permissionless networks where a small number mining pools or forging/staking pools are responsible for the majority of validation and block production, this is also a legitimate concern.

  Decentralization has to do with decentralizing control of the historical data, but also with geographic decentralization of the network's infrastructure.

ITU – NBTC Training – Session 5

Part 4.2

Infrastructure threats

- Extreme weather
- **Power outages**
- Calculated attack

ITU – NBTC Training – Session 5

Power outages

- Similar to extreme weather.
- **It is worth noting that DLTs using POS and BFT can run on a raspberry pi computer and 10-15W solar panel, so there is the potential to keep the networks running "off the grid."**
- **This threat is likely more relevant for POW networks because of their high electricity demands.**

ITU – NBTC Training – Session 5

Part 4.3

Infrastructure threats

- Extreme weather
- Power outages
- **Calculated attack**

ITU – NBTC Training – Session 5

Calculated attack

- If a company, nation state, or mining/staking/forging pool operator, decides to set up a DLT and fails to geographically disperse their nodes, then an actual physical attack on their facilities could be sufficient to compromise the entire network.

ITU – NBTC Training – Session 5

Overview of this 90-minute session:

- **User errors and private key management:** 15 minutes
- **Overview of 51% attacks:** 5 minutes
- **Social threats:** 10 minutes
- **Infrastructure threats:** 10 minutes
- ➢ **Technological threats:** 10 minutes
- **Smart contract vulnerabilities:** 15 minutes
- **Reviewing key terms and topics:** 10 minutes
- **Question and answer:** 15 minutes

ITU – NBTC Training – Session 5

Part 5

Technological threats

- Brute force
- Bad data
- Quantum computing

ITU – NBTC Training – Session 5

Part 5

Technological threats

- **Brute force**
- Bad data
- Quantum computing

ITU – NBTC Training – Session 5

Brute force

- **A brute force attack is an attempt to crack a password or an encryption passphrase through repeated trial and error.**
- Hackers set up scripts to run thousands of guesses on end until they find the passphrase for a specific account.
  - A 4 digit PIN would take 5 milliseconds to crack (with unlimited guesses)
  - One Bitcoin private key would take approximately centuries of running a computer continuously to brute force.
  - **If you store funds in a wallet that has a password or passphrase that you are required to set up yourself, ensure it is secure!**
    - **Using a strand of 12 random unassociated words is a general best practice.**

ITU – NBTC Training – Session 5

Part 5

Technological threats

- Brute force
- **Bad data**
- Quantum computing

ITU – NBTC Training – Session 5

Bad Data

- **DLT and blockchain DO NOT guarantee good data inputs.**
- **The DLT and blockchain simply ensure the historical data on the ledger is tamperproof.**
  - Many IoT use cases still run in to problems if someone simply fakes the system
    - Example: imagine a smart contract that automatically disburses payments when a particular weight of sand is on the scale at the shipping docks:
      - Instead of putting sand on it, the supplier just dumps a pile of rocks and dirt to achieve the necessary weight.
      - The smart contract sees the weight on the scale, and disburses payment.
      - *Your DLT shows the correct weight received, but you received the wrong materials!!*

ITU – NBTC Training – Session 5

Part 5

Technological threats

- Brute force
- Bad data
- **Quantum computing**

ITU – NBTC Training – Session 5

Quantum computing

- **Quantum computers are not limited to 2 states; they encode information as quantum bits.**
- Quantum computers are super fast and super powerful
  - With a functional quantum computer you could:
    - Brute force every passphrase for everyone using a DLT
    - Reveal private information by undoing all encryption of all data on the DLT

ITU – NBTC Training – Session 5

Quantum computing

- Quantum computers at scale are still relatively "science fiction," but significant progress continues to be made in this area.
- **Quantum computing would be a threat to every single banking database, government server, etc. in their current forms.**
  - **The entire economy would be at risk**
  - **Perhaps DLT vulnerabilities would not be the biggest concern.**
- There are many projects getting major press coverage for claiming to work on "post-quantum" or quantum proof cryptography, but none worth noting.
- **Watch the work of NIST's ongoing review of post-quantum algorithms for securing against quantum computers.**

ITU – NBTC Training – Session 5

Overview of this 90-minute session:

- **User errors and private key management:** 15 minutes
- **Overview of 51% attacks:** 5 minutes
- **Social threats:** 10 minutes
- **Infrastructure threats:** 10 minutes
- **Technological threats:** 10 minutes
- ➢ **Smart contract vulnerabilities:** 15 minutes
- **Reviewing key terms and topics:** 10 minutes
- **Question and answer:** 15 minutes

ITU – NBTC Training – Session 5

Part 6

Smart contract vulnerabilities

- Contracts
  - Stateful contracts
  - Stateless contracts
- Transaction execution
  - Stateful contract execution
  - Stateless contract execution

ITU – NBTC Training – Session 5

Part 6.1

Smart contract vulnerabilities

- Contracts
  - **Stateful contracts**
  - Stateless contracts

ITU – NBTC Training – Session 5

Stateful contracts

- Contract with specified states
  - Data lives within the contract

Stateless contracts

- Contract without specified states
  - Data lives within the input and output transactions

ITU – NBTC Training – Session 5

Standard transaction flows

Stateful contracts

Frontend => Web3 => Ethereum Network => Web3 => Frontend

Stateless contracts

Frontend => Web3 => Ethereum Network => Backend => Frontend

- When a user interacts with our contract from the frontend (using something like MetaMask) we watch for incoming transactions on the backend and process them.

ITU – NBTC Training – Session 5

Stateful contracts

```
contract DataStore {
    mapping(address => mapping(bytes32 => string)) public store;

    event Save(address indexed from, bytes32 indexed key, string
value);

    function save(bytes32 key, string value) {
        store[msg.sender][key] = value;
        Save(msg.sender, key, value);
    }
}
```

Cost of this contract: 181,000+ GAS

ITU – NBTC Training – Session 5

Stateless contracts

```
contract DataStore {
    function save(bytes32 key, string value) {}
}
```

Cost of this contract: 35,000+ GAS

ITU – NBTC Training – Session 5

Stateful contracts

- Pros:
  - Fully customizable to your precise needs
- Cons:
  - Difficult to upgrade a contract since balances are stored within the old contract
  - A mistake in the contract code can compromise the funds stored within the contract (i.e. Ethereum DAO, Ethereum Parity Wallet Freeze, and so on..)
  - Not necessarily compatible with other custom contracts/token types

ITU – NBTC Training – Session 5

Stateless contracts

- Pros:
  - Easy to upgrade
  - Cheaper to run
  - Generally function as an automation layer for existing token types, thereby ensuring compatibility with other businesses and developers building on the platform
- Cons:
  - Relies on a robust set of pre-defined tokens and transaction types
  - Less flexibility in the design of your contract

ITU – NBTC Training – Session 5

Part 6.2

Smart contract vulnerabilities

- Transaction execution
  - Stateful contract execution
  - Stateless contract execution

ITU – NBTC Training – Session 5

Stateful contract execution

- Execution of a program that occurs on all nodes that changes a set of bits representing value information stored on-chain within the contract itself. All nodes that contain the contract must execute the program in order to change a set of bits representing value information.

Stateless contract execution

- Execution of a program that occurs on an individual node (or subset of nodes) that changes a set of bits representing value information stored on-chain but apart from the contract.

Stateful contract execution

- Pros:
  - All nodes on the network execute and validate contracts, so you can trust the output assuming you trust the smart contract itself.
  - Even if the node of the person who deployed the contract is offline, the contract will continue functioning as long as a majority of nodes on the network execute.
- Cons:
  - Parallel operations are nearly impossible.
  - The network is only as fast as the slowest node.
  - Connecting to off-chain data is difficult since data can rapidly change in certain industries, resulting in nodes querying external data sources at different times.
  - Difficult to upgrade a contract since every node is storing a stateful copy.
  - More energy intensive.

ITU – NBTC Training – Session 5

Stateless contract execution

- Pros:
  - Parallel operations are straightforward.
  - Easy to upgrade by simply turning off the old node and deploying a new contract and updating contract reference IDs in future requests.
  - Simple to set up DLT oracles that interface with off-chain and legacy systems.
  - The contract itself doesn't store token balances so there's less incentive to attack the contract.
- Cons:
  - Requires a level of trust for the person operating the node on which the contract is deployed.
    - Mitigation measures exist, but this simple fact remains.
  - If this one node goes offline, then the contract won't execute.

ITU – NBTC Training – Session 5

Overview of this 90-minute session:

- **User errors and private key management :** 15 minutes
- **Overview of 51% attacks:** 5 minutes
- **Social threats:** 10 minutes
- **Infrastructure threats:** 10 minutes
- **Technological threats:** 10 minutes
- **Smart contract vulnerabilities:** 15 minutes
- ➢ **Reviewing key terms and topics:** 10 minutes
- **Question and answer:** 15 minutes

ITU – NBTC Training – Session 5

Reviewing key terms and topics

Private keys

- Issues
  - Loss of private keys
  - Phishing / keystroke logging
  - Sending funds to the wrong address
- Solutions
  - Paper wallets
  - Hardware wallets
  - Multi-signature accounts
  - Shamir secret sharing
  - Transaction vouchers

ITU – NBTC Training – Session 5

Reviewing key terms and topics

51% attacks

- What is it?
- What does it look like for
  - PoW?
  - PoS?
  - BFT?

ITU – NBTC Training – Session 5

Reviewing key terms and topics

Social threats

- Collusion
- Hash wars
- Sybil attack

ITU – NBTC Training – Session 5

Reviewing key terms and topics

Infrastructure threats

- Extreme weather
- Power outages
- Calculated attack

ITU – NBTC Training – Session 5

Reviewing key terms and topics

Technology threats

- Brute force
- Bad data
- Quantum computing

ITU – NBTC Training – Session 5

Reviewing key terms and topics

Smart contacts

- Stateful contract
- Stateless contract
- Stateful contract execution
- Stateless contact execution

ITU – NBTC Training – Session 5

Overview of this 90-minute session:

- **User errors and private key management:** 15 minutes
- **Overview of 51% attacks:** 5 minutes
- **Social threats:** 10 minutes
- **Infrastructure threats:** 10 minutes
- **Technological threats:** 10 minutes
- **Smart contract vulnerabilities:** 15 minutes
- **Reviewing key terms and topics:** 10 minutes

➢ **Question and answer:** 15 minutes

ITU – NBTC Training – Session 5

Question and answer

Thank You