Co-funded by the European

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Blockchain, and Decentralized Application Development

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

CHESS: CYBER-SECURITY EXCELLENCE HUB IN ESTONIA AND SOUTH MORAVIA

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Estonia (as an advanced digital society) and South Moravia (as a Czech ICT powerhouse) are teaming up to support the Europe's safe transition to a digital society
- Developing a joint cross-border cybersecurity research and innovation strategy
  - Focusing on six challenge areas:
    - Internet of Secure Things
    - Security Certification
    - Verification of Trustworthy Software
    - Security Preservation in Blockchain
    - Post-Quantum Cryptography
    - Human-centric Aspects of Cybersecurity
- *Updates: https://chess-eu.cs.ut.ee*

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

About Me

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Mubashar Iqbal
  - PhD in Computer Science from University of Tartu, Estonia
    - Topic: Reference Framework for Managing Security Risks using Blockchain
      - https://dspace.ut.ee/handle/10062/83826
  - Lecturer of Information Security
- Information Security Group
  - https://infosec.cs.ut.ee
  - Research areas
    - Information security and privacy, blockchain, internet of things, intelligent infrastructure, digital forensics, digital twins

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Agenda

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Blockchain
- Cryptocurrency
- Blockchain Characteristics
- Blockchain Components
- Security Methods in Blockchain
- Do You Need a Blockchain?
- dApp Development
- Guide to Write, Compile and Deploy Smart Contracts

Slides: https://shorturl.at/swyMO

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

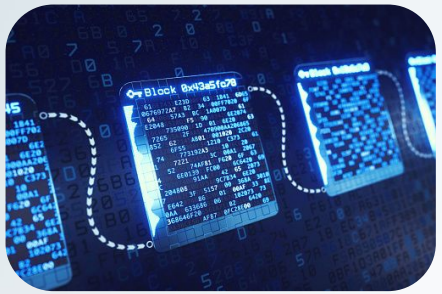
Co-funded by the European

Blockchain

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Distributed and decentralized ledger technology
- Immutable record of transactions in blocks

- Blocks form a chain
  - Connect with each other with a unique cryptographic hash
- First block in blockchain is genesis block
- Each block has its configuration
  - Block header
  - Block body



UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Blockchain - Who invented it?

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Bitcoin *(digital cryptocurrency)*
  - Authored in white paper in 2008 by *Satoshi Nakamoto*
  - Launched in 2009
  - Devised the first blockchain database to keep transactions records
- Satoshi Nakamoto
  - Pseudonymous person or persons
  - Maybe an organization
  - Two years later (April 2011) *disappears* from the web

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Milton Friedman speaking about e-Cash in *1999*

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- *Milton Friedman was an economist and statistician*
- *Received the Nobel Memorial Prize*

https://www.youtube.com/watch?v=tsJk2VtgUKI

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Blockchain before Bitcoin

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Bitcoin is built on earlier works:

- Peer-to-peer/distributed computing
- Cryptography and Merkle Trees
- Cryptographically linking blocks
  - Stuart Haber and W. Scott invented in *1991*
- Smart contracts
  - Nick Szabo in 1997 introduced the idea of smart contracts
- Digital currency
  - Nick Szabo in 2005 introduced *bitgold* as a form of digital money

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

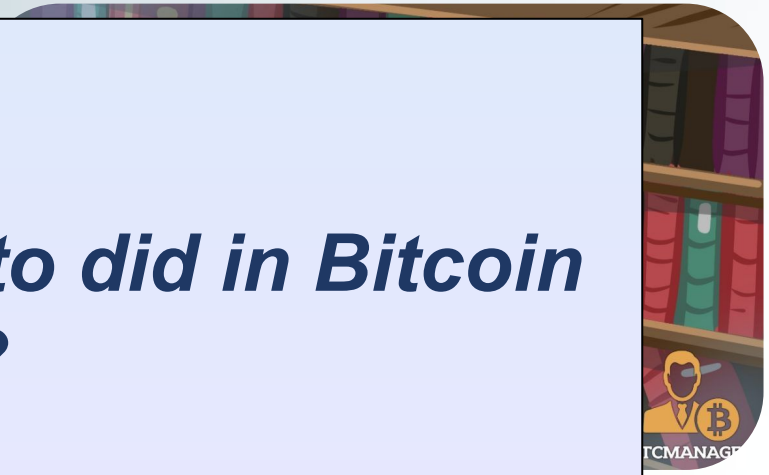
Blockchain before Bitcoin

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Bitcoin is built on earlier works:

- Pe
- Cry
- Cry
  -
- Sm
  -
- Dig
  - Nick Szabo in 2005 introduced *bitgold* as a form of digital money

What different Satoshi Nakamoto did in Bitcoin cryptocurrency?



Co-funded by the European

Blockchain before Bitcoin

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Bi

-
-
-
-
-
  - Nick Szabo in 2005 introduced *bitgold* as a form of digital money

Decentralized distributed *consensus mechanism* and *incentive layer*

- Proof of work
- Crypto mining
- Crypto economics

Satoshi put together the already available technology along with consensus mechanism and introduced an incentive layer

- It overcomes the *centralization* and *double-spending issues* in digital currency

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Cryptocurrencies

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Cryptography-based digital money/currency
- Exchanges of assets (funds) without third-party or centralized control authority (e.g., banks or other financial institutions)

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Bitcoin

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Satoshi Nakamoto authored in 2008 and implemented in 2009
- First cryptocurrency
- First implementation of blockchain technology
- Bitcoin is the *most traded cryptocurrency*
  - Bitcoin market value is ~*$507.42 B* (13th June, 2023)

Block explorer: https://www.blockchain.com/explorer/blocks/btc

Co-funded by the European

Ethereum

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Vitalik Buterin invented in 2015
- Ethereum took the blockchain to next level, usually relate to a Blockchain 2.0
- Introduced smart contracts in their platform
- Ethereum uses Ether cryptocurrency

Block explorer: https://www.blockchain.com/explorer/blocks/eth

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Initial Coin Offerings

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- ERC20 tokens
- Raise funds
  - To provide some service, app or as an investment opportunity
- Top ICOs based on raised funds
  - *EOS - $4.1 B*
    - Smart contracts
  - Telegram - $1.7 B
    - Encrypted messaging & Blockchain ecosystem
- Many involved in *scams* or *ponzi* schemes

ERC20 token generator: https://www.smartcontracts.tools/token-generator/create/ethereum

University of Tartu · Universitas Tartuensis · 1632

Co-funded by the European

Blockchain Characteristics

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Decentralized
- Distributed
- Immutable
- Tamper-evident
- Provenance
- Pseudo-anonymous

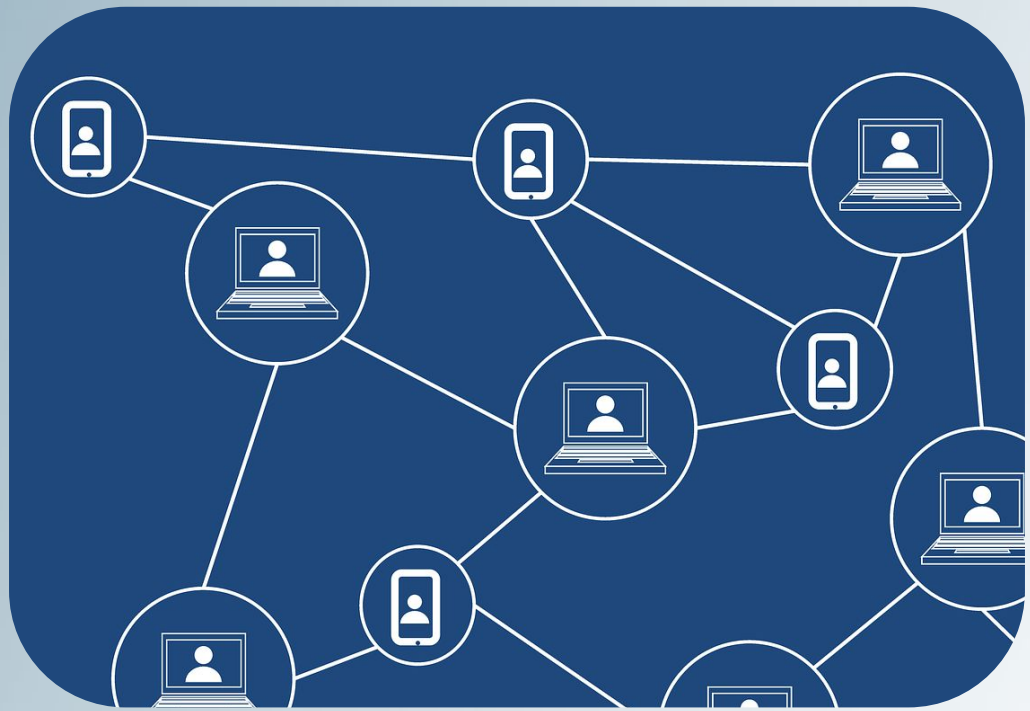
UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Blockchain Components



UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Nodes

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Network stakeholders
  - Nodes form the infrastructure of a blockchain
- Nodes are connected to each other
  - Constantly exchange the latest ledger with each other so all nodes stay up to date
- Store, spread and preserve the data
  - Nodes broadcast and spread transaction history to other nodes that may need to synchronize with the blockchain

Nodes Types

- Full nodes
- Validator nodes
- Miner nodes
- Archive Nodes
- Light Nodes

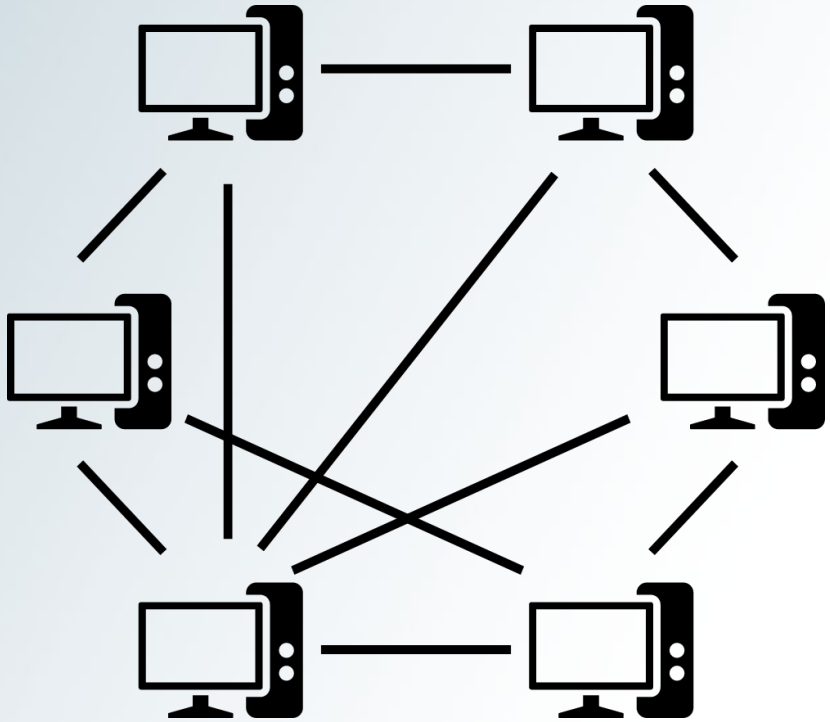
UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Peer-to-Peer Network

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Distributed application architecture
- Group of computers linked together
  - Equal permissions and responsibilities for processing data
- Peers share their resources
  - Processing power, disk storage, network bandwidth
- Works without the dedicated centralized servers or hosts

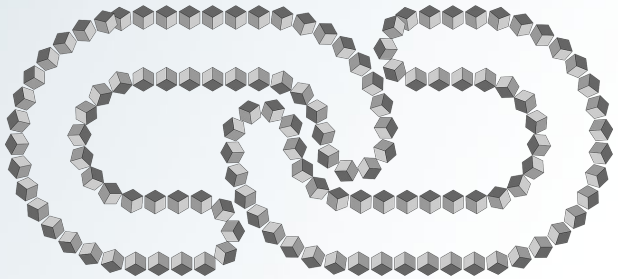


UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Ledger

- Collection of transactions
  - Replicated, shared, and synchronized digital data
  - Spread across several nodes on a peer-to-peer network
- Maintain cryptographic audit trail
  - Record transactions in an immutable manner
  - Traceable and irreversible
- No single point failure



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

University of Tartu · Universitas Tartuensis · 1632

Co-funded by the European

Consensus

- Agreement on a single true state of the ledger
  - Add new block to the chain
- Fault-tolerant
- Solve the double-spending problem
  - Authenticity of transaction
  - Creates a secure environment

Consensus mechanisms

- Proof of work
- Proof of stake
- Delegated proof of stake
- Practical Byzantine fault tolerant
- Proof of burn

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

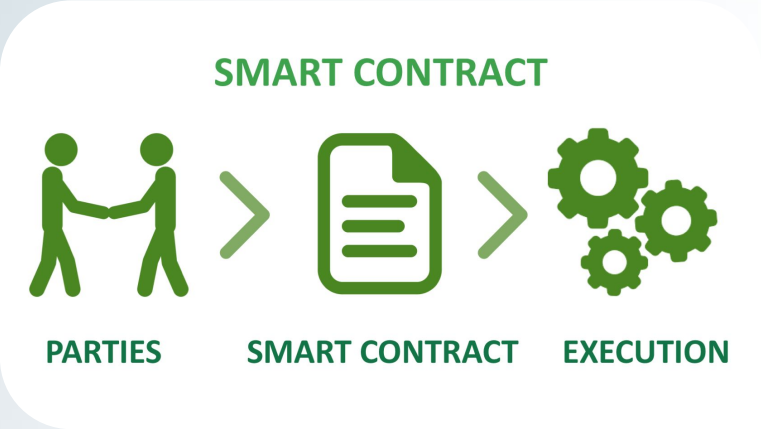
University of Tartu 1632 Universitas Tartuensis

Co-funded by the European

Smart Contracts

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Computer program stored on a blockchain
  - Execute when predetermined conditions are met
- Automate a workflow
  - Agreement between buyer and seller being directly written into lines of code
    - Trust, transparency, and security
  - Reduction of trusted intermediators, cost effective
  - Irreversible, trackable transactions



UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

https://academy.shrimpy.io/post/the-best-smart-contract-platforms
https://ethereum.org/en/developers/tutorials/understand-the-erc-20-token-smart-contract

Co-funded by the European

Cryptography

- Protect digital data, enable secure communication
  - Confidentiality, integrity, authenticity, non-repudiation
- Cryptography types
  - Secret/symmetric key cryptography
  - Asymmetric/public key cryptography
  - Hash functions
    - Irreversible, one-way functions, e.g., SHA

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

University of Tartu
Universitas Tartuensis 1632

Co-funded by the European

Crypto Economics

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Economic interaction in adversarial environments
  - Combinations of cryptography, computer networks and game theory
  - Solve crypto puzzle (e.g., mining)
    - Economic incentives
- Emerge in decentralized marketplaces and applications
  - Foster trust
  - Keep nodes honest

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Crypto Wallets

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Store public and private keys
- Send and receive transactions
- Track the cryptocurrency balance
- Wallet can be:
  - Paper wallet
  - Hardware wallet
  - Software wallet

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Blockchain Types

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Permissionless / public
  - Requires no permission to join the Blockchain network
  - Open to all and transactions are visible to everyone
  - More transparent but slow transactions speed
- Permissioned
  - Requires permissions to join the Blockchain network
  - Only pre-defined nodes can participate in consensus mechanism
  - Fast, privacy oriented but less transparent
- Private / Hybrid
  - Controls and network governance assigned to one designated authority
  - Blockchain activity is only visible to chosen participants
  - More privacy oriented, scalable but less decentralized

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Comparison of Blockchain Platforms

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

	Bitcoin	Ethereum	Hyperledger-fabric	Corda
Type	Permissionless	Permissionless	Permissioned	Permissioned
Smart contract	Yes	Yes	Yes	Yes
SC language	Scrypt	Solidity	Go, Java, NodeJs	DAML
Consensus	PoW	PoS	PBFT, CFT	Transaction validity & uniqueness
Cryptocurrency	Bitcoin (BTC)	Ether (ETH)	–	–
Transactions/s	7 TPS	8-9 TPS	Thousands	Thousands
Confidentiality	No	No	Yes	Yes
Applications	Cryptocurrency only	Multiple applications	Multiple applications	Financial applications

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Security Methods in Blockchain

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Public-Key Cryptography

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Wallets and transactions
  - When a user creates a wallet on a Blockchain, they are generating a public-private key pair
  - Public-key
    - Public to everyone and used to check the balance in the respective wallet
    - Receive coins (cryptocurrency)
  - Private key
    - Proves an ownership and send coins from the wallet
- Transaction requires a signature from the private key of the sending wallet

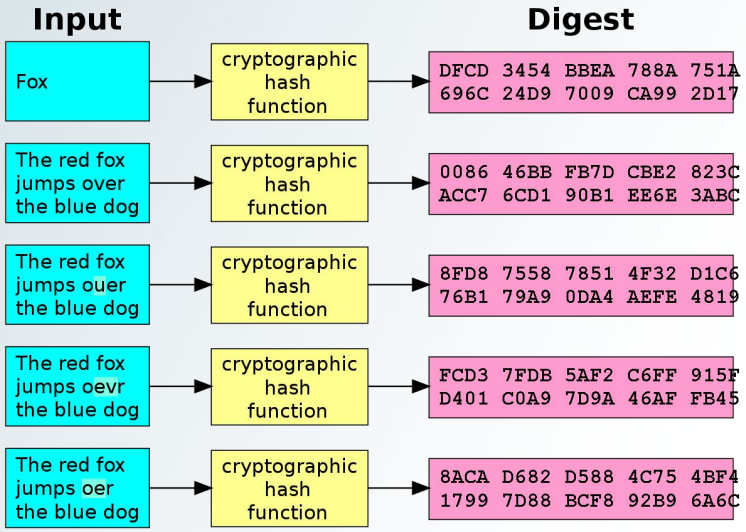
UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Cryptographic Hashing

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Every next block is connected to previous hash by a cryptographic hash
- If 1 bit of data change in a block, it would alter the hash output of all previous blocks
  - It would invalidate the ledger
- Different Blockchain platforms use different hashing mechanisms
  - Bitcoin uses a cryptographic hash function called SHA-256
  - Ethereum uses keccak256
- Cryptographic hash functions are utilized for mining in the blockchain

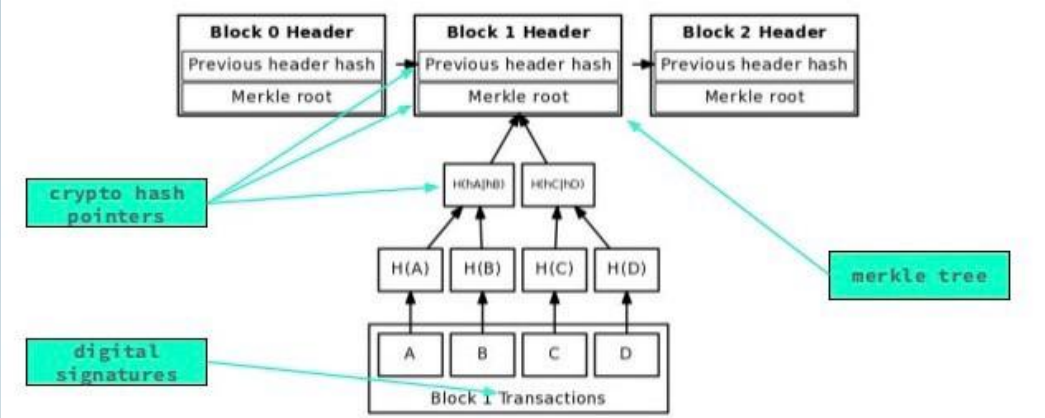


UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Merkle Trees

- Merkle trees organize transactions in a block
- Verify the integrity of the transaction
  - Transactions in a given block have been tampered or not
  - To trace the specific transaction that is being tampered
- Makes transactions traversal easy within the block



Merkle tree connecting block transactions to block header merkle root

Co-funded by the European

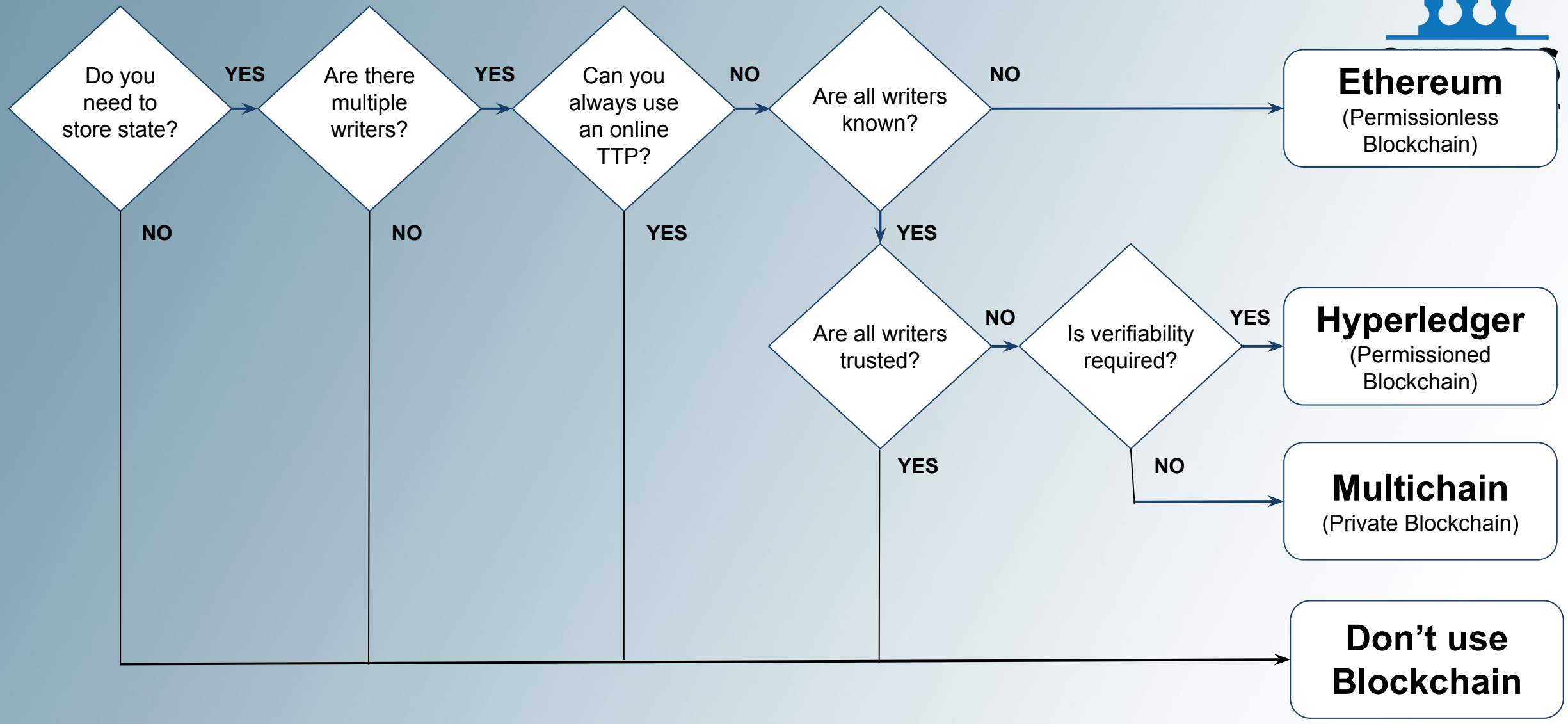
CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Do you need a blockchain?

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European



Wüst K. and Gervais A. (2017) *Do you need a Blockchain?*
IACR Cryptology ePrint Archive, 2017.

Co-funded by the European

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Why would you consider to use blockchain?

Let's take 2 minutes to brainstorm and think what would be your reasons to consider Blockchain?

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Is Blockchain a Security?

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

*"If you think **technology** can solve your **security problems**, then you don't understand the **problems** and you don't understand the **technology**"* ***Bruce Schneier***

If you think **blockchain** is a **security**, then you don't understand the **security** and you don't understand the **blockchain**

Co-funded by the European

Security Risks Mitigated and Appeared

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Blockchain as a ***countermeasure solution***

- Data tampering
- Denial of service
- Single point failure
- Repudiation
- Man in the middle
- …

Security risks that can ***appear in blockchain-based solutions***

- Sybil attack
- Double-spending attack
  - 51% attack
- Deanonymization attack
- Quantum computing threats
- …

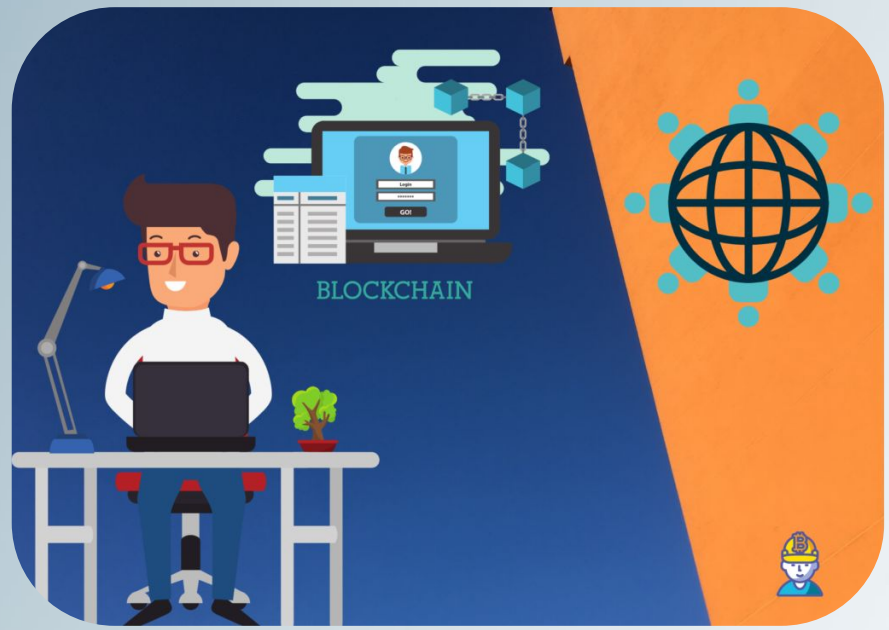
UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

dApp Development



UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Tools

- Solidity
  - Writing Ethereum-based smart contracts
- Remix IDE
  - Web-based IDE for writing smart contracts
    - https://remix.ethereum.org
- Ganache
  - Local blockchain network
- Metamask
  - Crypto wallet
- Web3.js
  - To interact with Ethereum node
- Node Js and NPM

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

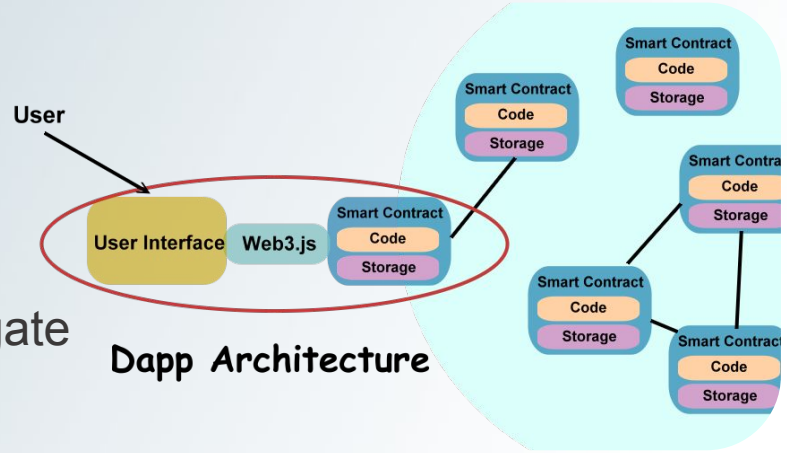
University of Tartu
Universitas Tartuensis 1632

Co-funded by the European

dApp Development Setup

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Install NodeJs and NPM
  - https://nodejs.org/en/
- Terminal (e.g., command prompt, git bash)
  - NodeJs (node -v)
  - NPM (npm -v)
- Ganache cli
  - npm install -g ganache-cli
    - Start ganache
      - ganache
- Web3.js
  - Create a separate folder (e.g., KI_BC_Workshop) and navigate to it
  - npm init
  - npm install web3
    - https://web3js.readthedocs.io/en/v1.5.2/getting-started.html
  - or use https://cdn.jsdelivr.net/npm/web3@1.5.2/dist/web3.min.js



UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Code

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

- Web interface
  - index.html
- Web 3 settings and contract connection
  - dapp.js
  - Websocket connection with local ethereum network (*ws://127.0.0.1:8545*) using *Ganache*
- Smart contract
  - StudentCourseRegistration.sol

Code: *https://shorturl.at/bPS78*

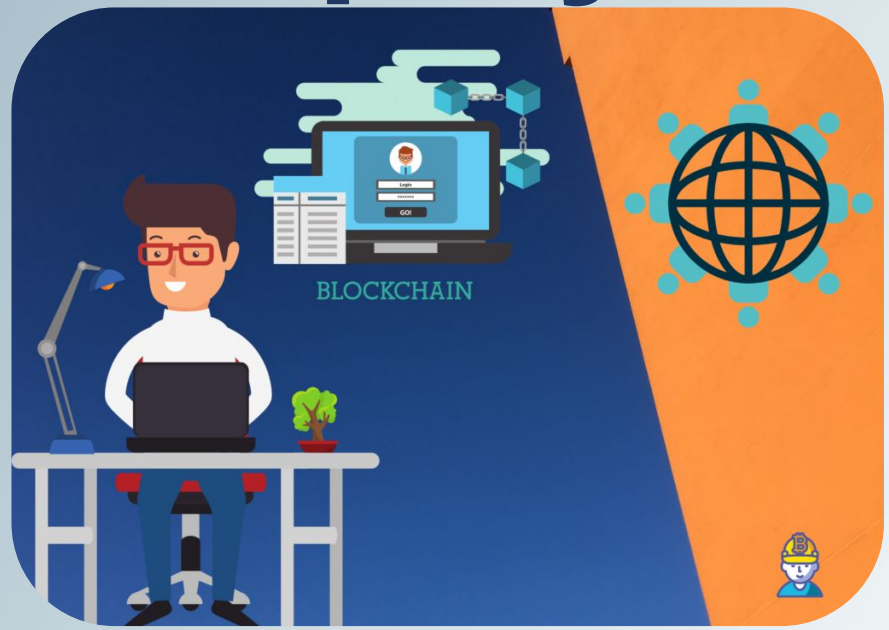
UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Guide to Write, Compile, and Deploy dApp

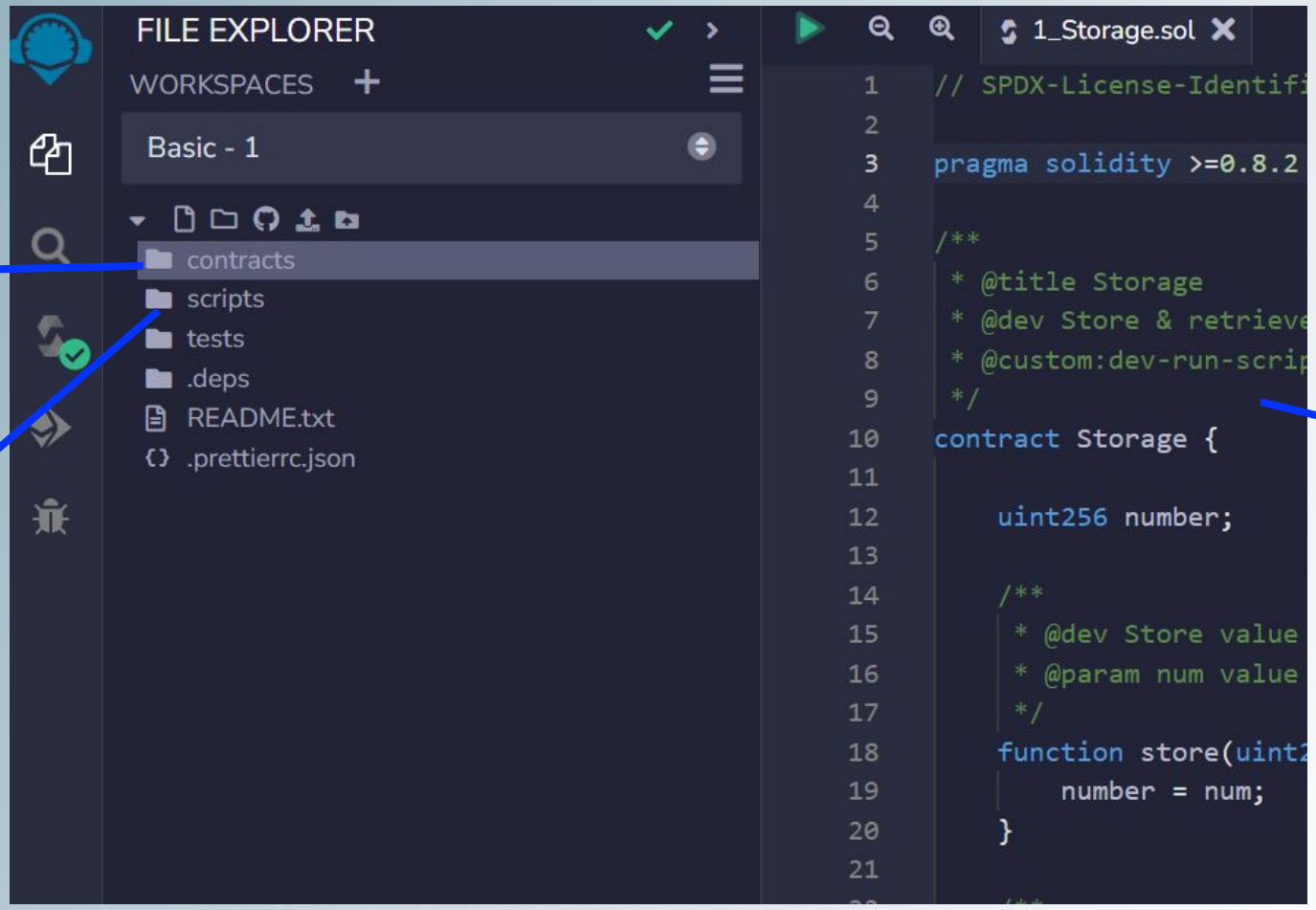


UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Remix IDE

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia



Smart contracts files

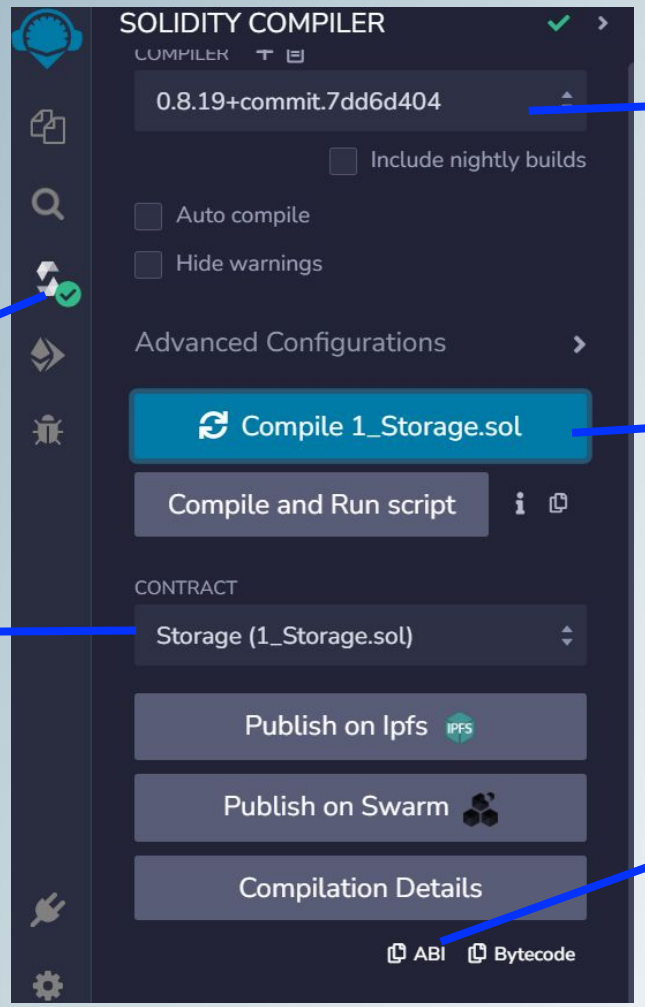
Smart contracts deployment scripts

Smart contracts code explorer

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Remix IDE



Compiler version

Compile smart contract

Solidity compiler

Smart contract to compile

Application binary interface

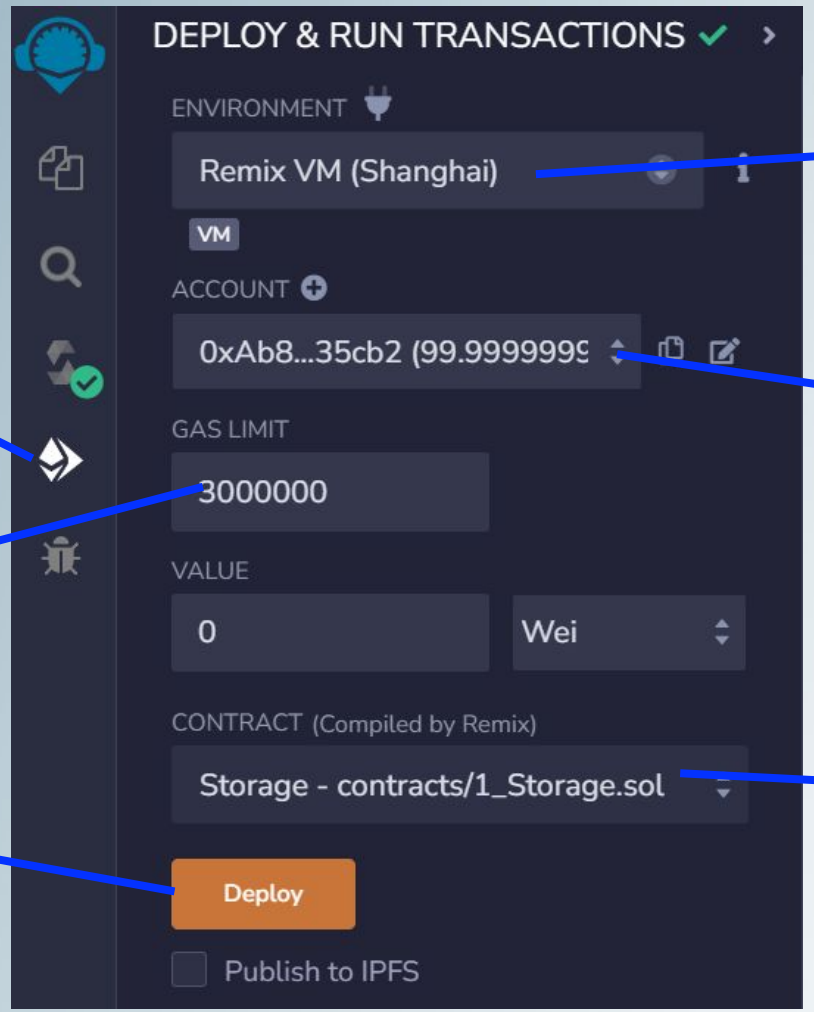
CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

University of Tartu 1632 Universitas Tartuensis

Co-funded by the European

Remix IDE

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia



Smart contract deployment environment

Smart contract owner account (deployment account)

Compiled contract

Deploy compiled smart contract and run transactions

Default gas limit

Deploy compiled contract

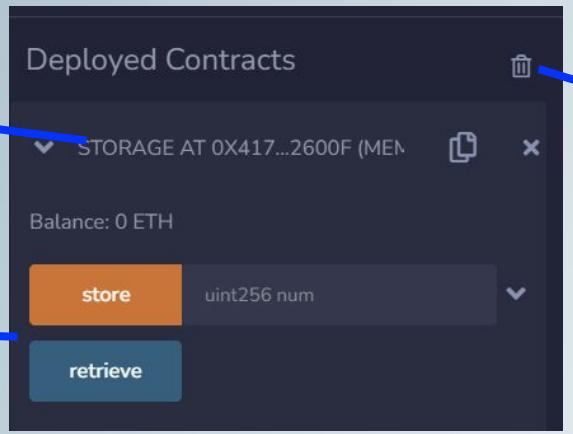
UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Remix IDE

Deployed smart contract address

To perform smart contract implemented actions



Delete deployed smart contract

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

UNIVERSITY OF TARTU · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European

Further Reading

Iqbal M., Matulevičius R. (2019) Blockchain-Based Application Security Risks: A Systematic Literature Review. In: Advanced Information Systems Engineering Workshops. CAiSE 2019. Lecture Notes in Business Information Processing, vol 349. Springer, Cham. https://doi.org/10.1007/978-3-030-20948-3_16

Iqbal M., Matulevičius R. (2019) Comparison of Blockchain-Based Solutions to Mitigate Data Tampering Security Risk. In: Business Process Management: Blockchain and Central and Eastern Europe Forum. BPM 2019. Lecture Notes in Business Information Processing, vol 361. Springer, Cham. https://doi.org/10.1007/978-3-030-30429-4_2

M. Iqbal and R. Matulevičius, (2021) Exploring Sybil and Double-Spending Risks in Blockchain Systems. In IEEE Access, vol. 9, pp. 76153-76177. https://doi.org/10.1109/ACCESS.2021.3081998

M. Iqbal, R., Matulevičius, (2021) Blockchain as a Countermeasure Solution for Security Threats of Healthcare Applications. In: Business Process Management: Blockchain and Robotic Process Automation Forum. BPM 2021. Lecture Notes in Business Information Processing, vol 428. Springer, Cham. https://doi.org/10.1007/978-3-030-85867-4_6

M. Iqbal, Reference framework for managing security risks using blockchain, (2022), available at https://dspace.ut.ee/handle/10062/83826 *(PhD thesis)*

Co-funded by the European

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Thank You!

Q & A

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.