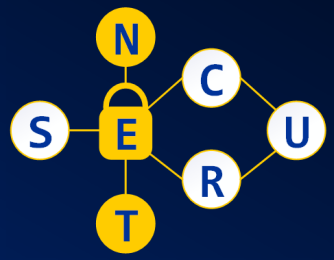


Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands

Funded by the European Union

Blockchain Usage in Distributed System Security

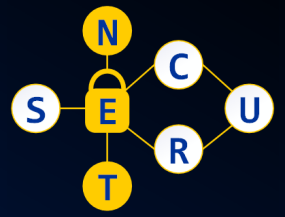
Dr. Vaidotas Drungilas

Funded by the European Union Horizon Europe programme under Grant Agreement No. 101217315. 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.

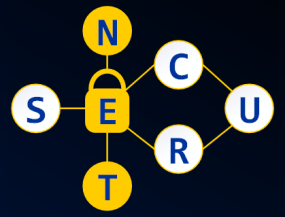
ABOUT ME

- PhD studies on topic combining Blockchain, AI and collaboration.
- Working in KTU for 10+ years.
- Teaching about databases, software development and more.

Scope of the Presentation

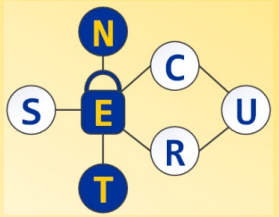


1. Blockchain basics and blockchain integration benefits and difficulties.
2. Common use cases for blockchain and distributed application software development
3. Blockchain applications in security domain.



Blockchain Essentials

Distributed Ledger Technology



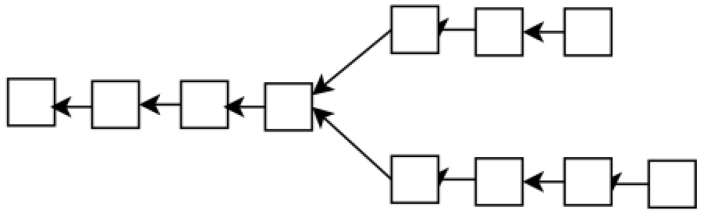
A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions, or geographies, accessible by multiple peers

THE DLT TYPES

- Blockchain
- Tangle
- Hashgraph

Blockchain

- Blockchain is a decentralized, distributed database that is shared across all the parties participating in the network.
- One key difference between a typical database and a blockchain is how the data is structured. A blockchain collects information together in blocks, that hold sets of information.
- Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain.



Antonopoulos, A.M.: Mastering Bitcoin: Unlocking Digital Cryptocurrencies.
O'Reilly Media, Inc., Sebastopol (2014)

Simplified Blokchain Block Structure

- Block header, timestamp and nonce
- Reference to previous block
- Ledger (transactions)
- Smart contracts*

* If support is available

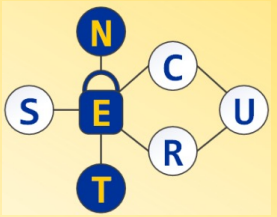
Blockchain Essentials

- Hashing
- Distributed network
- Nodes
- Immutability
- Transparency
- Consensus

Consensus algorithms

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Proof of Capacity (PoC)
- Byzantine Fault Tolerant (BFT)

Public Blockchains



In this type of blockchains, ledgers are visible to everyone on the network.

It allows anyone to verify and add a block of transactions to the blockchain.

Public networks have incentives for people to join and free for use. Anyone can use a public blockchain network.

Private Blockchains

The private blockchain is within a single organization.

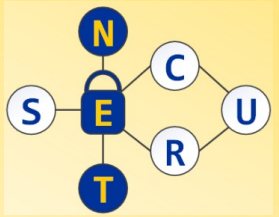
It allows only specific people of the organization to verify and add transaction blocks.

However, not everyone on the internet is generally allowed to view.

HYPERLEDGER

ripple

Consortium Blockchains



In this Blockchain variant, only a group of organizations can verify and add transactions.

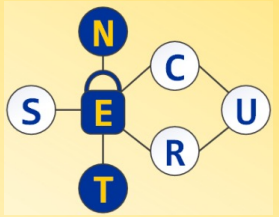
Ledger can be open or restricted to select groups of participants.

Consortium blockchain is used cross-organizations and is controlled by pre-authorized nodes.

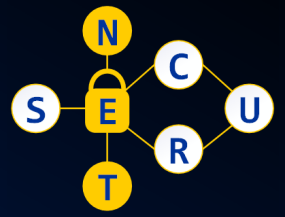
Quorum

corda

Blockchain Type Comparison



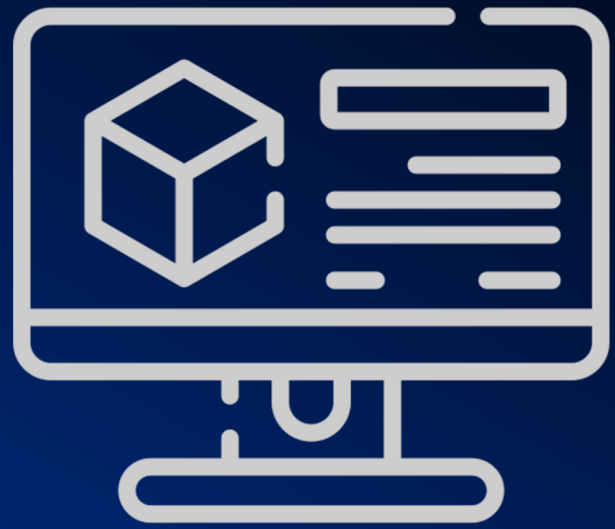
	PUBLIC	PRIVATE	CONSORTIUM
ACCESS	Anyone	Multiple organizations	Multiple organizations
PARTICIPANTS	Permissionless Anonymous	Permissioned Known Identities	Permissioned Known Identities
SECURITY	Consensus Mechanism Proof of Work/Proof of Stake	Pre-approved participants Voting/multiparty Consensus	Pre-approved participants Voting/multiparty Consensus
TRANSACTION SPEED	Slow	Lighter and Faster	Lighter and Faster



Software Development with Blockchain

SMART CONTRACTS

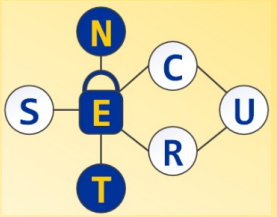
- Smart contract is a deployed program that can be executed on the blockchain network following the principle of trigger causing an appropriate reaction.
- Smart contracts could theoretically cover entire software applications.
- Currently most smart contracts are like traditional contracts for creating legally binding agreements between certain parties.



SMART CONTRACT DEVELOPMENT

- Distributed Applications (DApps) have their backend code running on a decentralized peer-to-peer network, as opposed to typical applications where the backend code is running on centralized servers.
- A DApp can have frontend code and user interfaces written in any language that can make calls to its backend.
- DApps have been popularized by distributed ledger technologies (DLT) through the use of smart contracts.

Platforms Supporting Smart Contracts



Ethereum

Hyperledger

Corda

Tezos

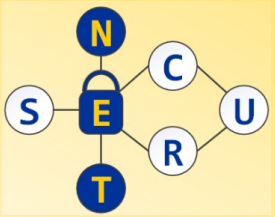
Stellar

EOS

Hashgraph

Tron

Programming languages for smart contracts



Solidity

Golang

JavaScript

Java

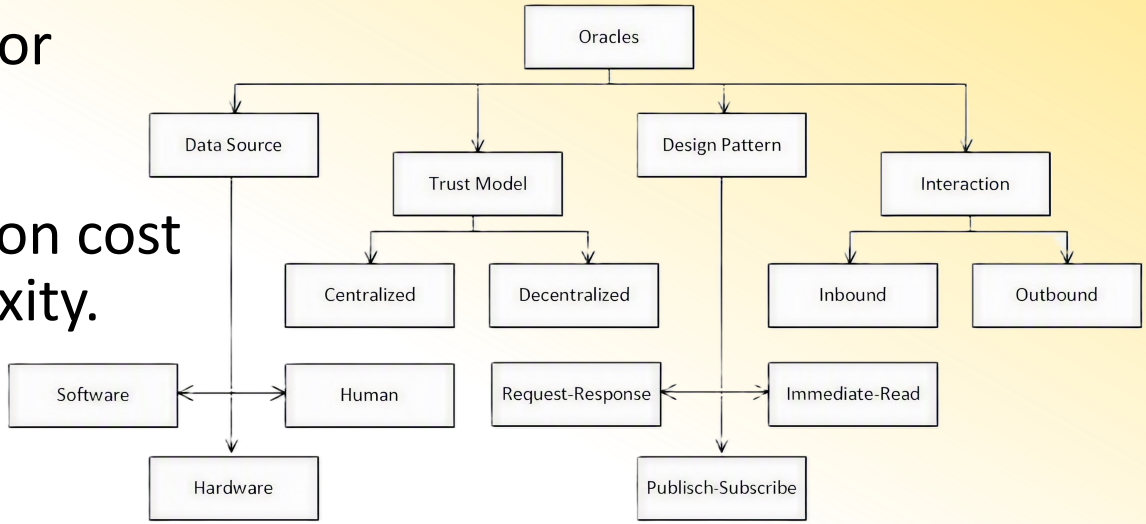
Node.js

Vyper

Blockchain Oracles

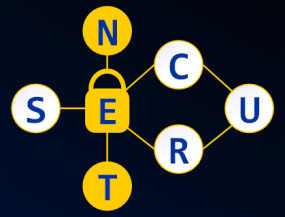
A blockchain oracle is a third-party service providing or obtaining information for smart contracts.

Reduction of smart contract execution cost with increased architectural complexity.



H. Al-Breiki, M. H. U. Rehman, K. Salah, and D. Svetinovic, "Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges," doi: 10.1109/ACCESS.2020.2992698.

Blockchain Oracle Integration

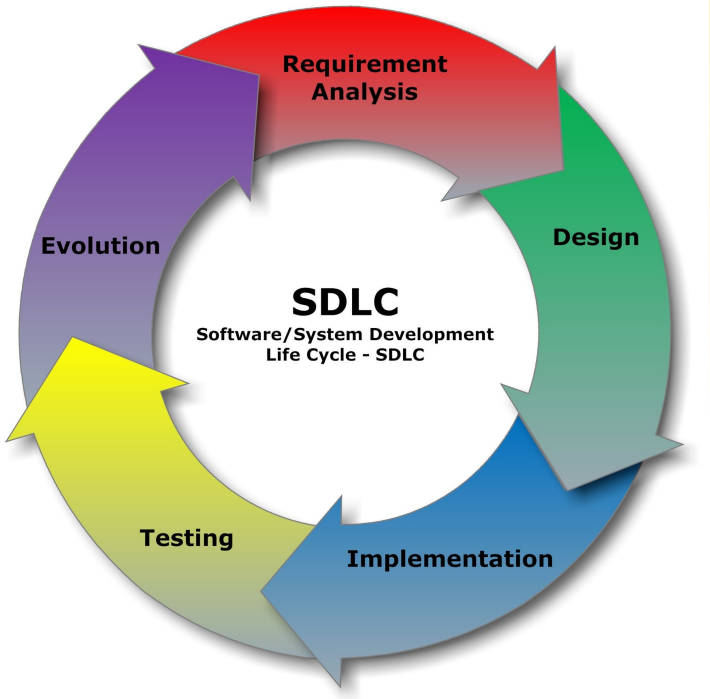


Oracle development and support increases maintenance costs.

Increased potential for security vulnerabilities and attack surface.

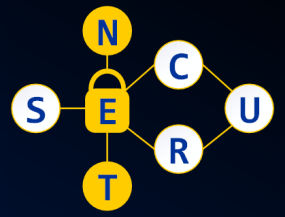
Lack of distribution might decrease main benefits of blockchain.

DApp Development Cycle



Post, G., & Anderson, D., (2006). *Management information systems: Solving business problems with information technology*. (4th ed.). New York: McGraw-Hill Irwin.

Blockchain application checklist

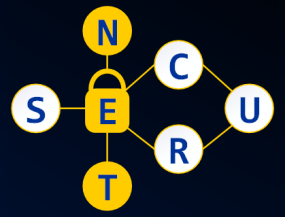


1. Requirement to store state
2. Multiple distributed parties collaborating
3. Lack of trust between parties
4. Speed is less important that structural integrity.

Performance Metric	Private Blockchain (Ethereum, 6 Nodes)	MySQL Database
Maximum Transaction Size	6,688 bytes	65,535 bytes
Throughput	~3 bytes/ms	< 1 second
Execution Time	< 2027 ms	1.22 ms (average)

S. Chen, J. Zhang, R. Shi, J. Yan, and Q. Ke, ‘‘A comparative testing on performance of blockchain and relational database: Foundation for applying smart technology into current business systems,’’

Example sources of distrust leading to Blockchain adoption



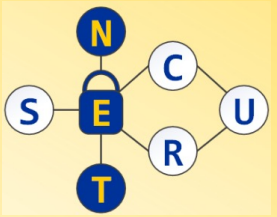
- Distrust of data integrity
- Distrust in central authority
- Malicious participants
- Security considerations

Blockchain application for security

Blockchain for security main application areas

- Identity verification
- Communication and network security
- Supply chain and forensics
- Information sharing
- Collaboration and rewards

European Blockchain



- European Commission approved applications: covering verification of documents, products and digital identities.
- Projects with multiple use cases and participation by KTU

European Commission | ebsi European Blockchain

https://ebsi.eu/projects

Internet of things security concerns

- Large numbers of distributed devices
- Limited security capabilities on embedded systems
- Vulnerable sensor networks and communication links
- Single-point-of-failure risks in centralized control architectures

IoT blockchain applications

- Data collection and sharing
- Equipment safety
- Cross-domain access auditing

Defense domain security concerns

- Strict logging and tracking of materials and supply chains
- Emphasis on secure authentication and data transfer
- Obvious sources of distrust
- Increasing amount of IoT devices

Defense security applications

- Korea - Procurement
- France, Ukraine, Korea - Sensitive information storage
- China - Equipment management, cyber infrastructure

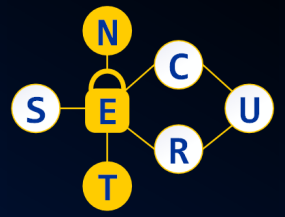
Honorable mentions

- Healthcare
- Police operations
- Distributed AI

References

- S. Lee and S. Kim, "Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges," in *IEEE Access*, vol. 10, pp. 2602-2618, 2022, doi: 10.1109/ACCESS.2021.3136328.
- R. Huo *et al*., "A Comprehensive Survey on Blockchain in Industrial Internet of Things: Motivations, Research Progresses, and Future Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 88-122, Firstquarter 2022, doi: 10.1109/COMST.2022.3141490
- Hasan, M., Hossain, G. M. N., Moure, S. H., & Sardar, M. (2024). Ensuring the Integrity of the Police Complaint Files Using Blockchain Technology. *2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP)*, 238-243. https://doi.org/10.1109/tiacomp64125.2024.00048
- González, J. A., García, A., & Baeza, V. M. (2026). Blockchain as a Cybersecurity Enabler in Federated Networks for Resilience and Interoperability. *J. Cybersecur. Priv., 6*, 54. https://doi.org/10.3390/jcp6020054
- Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for Modern Applications: A Survey. *Sensors (Basel, Switzerland), 22*. https://doi.org/10.3390/s22145274
- Liu, M., Yeoh, W., Jiang, F., & Choo, K. (2021). Blockchain for Cybersecurity: Systematic Literature Review and Classification. *Journal of Computer Information Systems, 62*, 1182 - 1198. https://doi.org/10.1080/08874417.2021.1995914
- Shang, S., Zhou, A., Tan, M., Wang, X., & Liu, A.-D. (2022). Access Control Audit and Traceability Forensics Technology Based on Blockchain. *2022 4th International Conference on Frontiers Technology of Information and Computer (ICFTIC)*, 932-937. https://doi.org/10.1109/icftic57696.2022.10075123

Key takeaways



- Blockchain is great when you use it correctly
- Blockchain integrations if difficult, costly and requires careful consideration
- From the security perspective blockchain might only play a small part of overall security picture.