Software Engineering Challenges in Blockchain-Based Decentralized Systems

WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

LECTURE: **Davor Svetinovic**

EQUIS ACCREDITED AACSB ACCREDITED ASSOCIATION OF MBAS ACCREDITED

My Research Background

I have participated in a wide variety of complex multi-disciplinary research projects, e.g.,:

- Sustainable cities modelling and development (systems)
- Smart grid cyber security (systems)
- Data mining of software repositories (analytics)
- Software system evolution and cloning (analytics)
- Blockchain engineering (systems / analytics)
- Decentralized AI (systems / analytics)

My Blockchain Technology Background

- Interested in Bitcoin / Blockchain Technology since 2009
- Various teaching and research projects since 2010
  - Bitcoin C port/library, Bitmessage, Electrum, Multibit, Dogecoin, Ethereum
  - Cryptocurrency for CO2 emissions trading
  - Solar mining cryptocurrency (solar energy signature)
  - Automated Bitcoin energy trade (IoT, smart cars, smart meters, etc.)
  - Intelligent trading challenges, no central price signal, exchanges, GCC market
  - Blockchain analytics (community detection, forensics)

Money

Functions

- Unit of account
- Medium of exchange
- Store of value

- Properties:
  - Fungible
  - Durable
  - Divisible
  - Portable
  - Limited in supply
  - Acceptable

First Contribution

Photo by Karolina Grabowska from Pexels

"Physical" Transfer of Assets (and Value) in the Cyberspace

Source: https://coinmarketcap.com/currencies/bitcoin/

Second Contribution: “Anonymous” Decentralized Entities

WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

	#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
☆	1	Bitcoin BTC Buy	$61,808.96	4.11%	12.41%	$1,162,884,586,025	$45,471,142,388 736,878 BTC	18,845,000 BTC	
☆	2	Ethereum ETH Buy	$3,859.44	1.40%	7.03%	$454,236,879,655	$18,594,942,813 4,828,286 ETH	117,945,259 ETH	
☆	3	Binance Coin BNB Buy	$477.92	2.45%	13.00%	$80,470,824,269	$2,478,539,066 5,178,699 BNB	168,137,036 BNB	
☆	4	Cardano ADA	$2.20	0.62%	2.65%	$72,480,998,935	$3,154,570,061 1,432,094,471 ADA	32,904,527,669 ADA	
☆	5	Tether USDT Buy	$0.9993	0.03%	0.10%	$68,544,240,857	$81,807,542,217 81,861,045,870 USDT	68,589,070,064 USDT	
☆	6	XRP XRP	$1.14	0.08%	6.25%	$53,371,231,689	$4,476,133,429 3,931,569,321 XRP	46,878,114,887 XRP	
☆	7	Solana SOL	$158.13	2.43%	0.82%	$47,498,124,872	$2,828,989,571 17,884,253 SOL	300,272,746 SOL	

Source: http://coinmarketcap.com/

Bitcoin

- **Protocol** – a decentralized peer-to-peer network
- **Blockchain** – a public transaction ledger
- **Consensus mechanism** – a decentralized mechanism of providing trust through proof of work (mining)
- Currency issuance and payment verification system

Blockchain Technology – Underlying Implementation Constructs

- Hash functions (any string -> fixed length string) with security properties: collision free, hiding, and puzzle-friendly
- Hash pointers
- Hash pointer linked lists (blockchains)
- Hash pointer binary trees (Merkle trees)
- Digital signatures and public identities

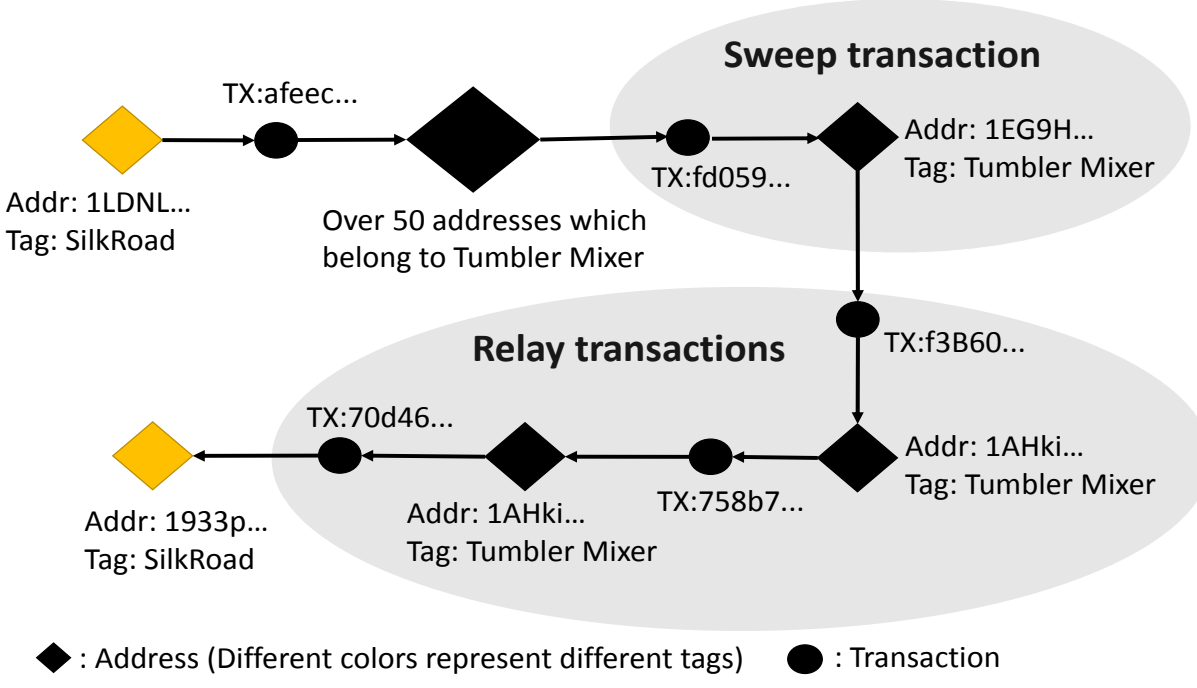
Presentation-Related Publications

- T. Chang and D. Svetinovic*, "Improving Bitcoin Ownership Identification Using Transaction Patterns Analysis," in **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, vol. 50, no. 1, pp. 9-20, Jan. 2020, doi: 10.1109/TSMC.2018.2867497.
- I. Alqassem, I. Rahwan and D. Svetinovic*, "The Anti-Social System Properties: Bitcoin Network Data Analysis," in **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, vol. 50, no. 1, pp. 21-31, Jan. 2020, doi: 10.1109/TSMC.2018.2883678.
- M. H. u. Rehman, K. Salah, E. Damiani and D. Svetinovic*, "Trust in Blockchain Cryptocurrency Ecosystem," in **IEEE Transactions on Engineering Management**, 2020, doi: 10.1109/TEM.2019.2948861.

*corresponding author

Project #1: Need for Ever More Privacy!

- T. Chang and D. Svetinovic, "Improving Bitcoin Ownership Identification Using Transaction Patterns Analysis," in **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, vol. 50, no. 1, pp. 9-20, Jan. 2020, doi: 10.1109/TSMC.2018.2867497.



Project #1: Users Get Creative to Protect Privacy

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

- *Peel Transaction:* The most common type of transaction. No matter what the number of inputs in a transaction is, there will always be two output addresses.
- *Sweep Transaction:* A transaction combines multiple inputs into one output. This type of transaction makes it easier for entities to process and control their bitcoins.
- *Distribution Transaction:* Distributing transactions usually have any number of inputs and more than three output addresses. This kind of transaction is commonly related to one single party or organization trying to pay multiple parties, e.g., gambling rewards or pooled mining rewards.
- *Relay Transaction:* This kind of pattern only includes one input and one output. It can be used to move bitcoins from one party to another without leaving any correlated information behind, such as the change address or other input addresses.
- *Self-Spending Transaction:* An input address also appears as an output in the same transaction, the number of self-spending addresses in one transaction can be many.
- *Peeling Chain Transaction:* A series of peel transactions. The change address is used as the input to a subsequent peel transaction.

Project #1: Contributions

- The **largest study so far** conducted on the clustering of Bitcoin addresses (at the publishing time)—the dataset used in this paper contains over 46 million Bitcoin addresses and 46.5 million transactions.
- A **new clustering approach** was developed based on a novel combination of known-address clustering with transaction patterns.
- The proposed approach was compared to the existing known-address clustering, and the results showed that our approach produced **significantly more homogeneous clusters** (lower “impurity”), which better predict shared transactions validated against the test set.
- **Scalable approach** that can handle large datasets.

Project #2: It’s all a bit Social!

- I. Alqassem, I. Rahwan and D. Svetinovic*, "The Anti-Social System Properties: Bitcoin Network Data Analysis," in **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, vol. 50, no. 1, pp. 21-31, Jan. 2020, doi: 10.1109/TSMC.2018.2883678.

Project #2: Analyzing Bitcoin as a Social Network

WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

- Despite the different purposes of the various social networks and Bitcoin transaction network, one **can observe universal dynamics** such as the densification power law, shrinking diameter, and modular structure.
- However, we **also found that Bitcoin deviates in important ways due to anonymity-seeking behavioral patterns of its users**. As a result, the network exhibits a two-orders-of-magnitude larger diameter, sparse tree-like communities, and an overwhelming majority of transitional or intermediate accounts with incoming and outgoing edges but zero cumulative balances.

Project #2: System Perspective

- From the systems perspective, it was observed that some of these (anti-)social incentives are affecting critical system properties, such as security and privacy.
- The social incentives are leading to formation or disintegration of certain network communities. This in turn is leading to the improper use or the intentional misuse of the overall system.
- These community alterations present serious threats to a subset of the system properties that we identified: decentralization, longevity (of the system that's supposed to evolve over next hundreds of years), trust, participation incentive, privacy, security, and usage ethics.

Project #2: Thus…

We realized what we knew all along:

it is all not that much about the blockchain

as it is about the consensus!

And not just the consensus at the technical level of adding new transactions to the blockchain, but about the general consensus what we are using all these systems for.

And the system-level consensus is not just about privacy and security but about an even more expensive construct: **trust**.

And Trust is Very Expensive

Key Network Statistics (source: https://digiconomist.net/bitcoin-energy-consumption accessed Oct 16, 2021)

Description Value

Bitcoin's current estimated annual electricity consumption (TWh) **175.10 TWh**

Annualized global mining revenues **$21,156,404,372 (**Total value of mining rewards (including fees) per year.)

Annualized estimated global mining costs **$8,755,116,628** (Assuming a fixed rate of **5 cents per kilowatt-hour**.)

Current cost percentage **41.38%** (Estimated ratio of electricity costs to total miner income.)

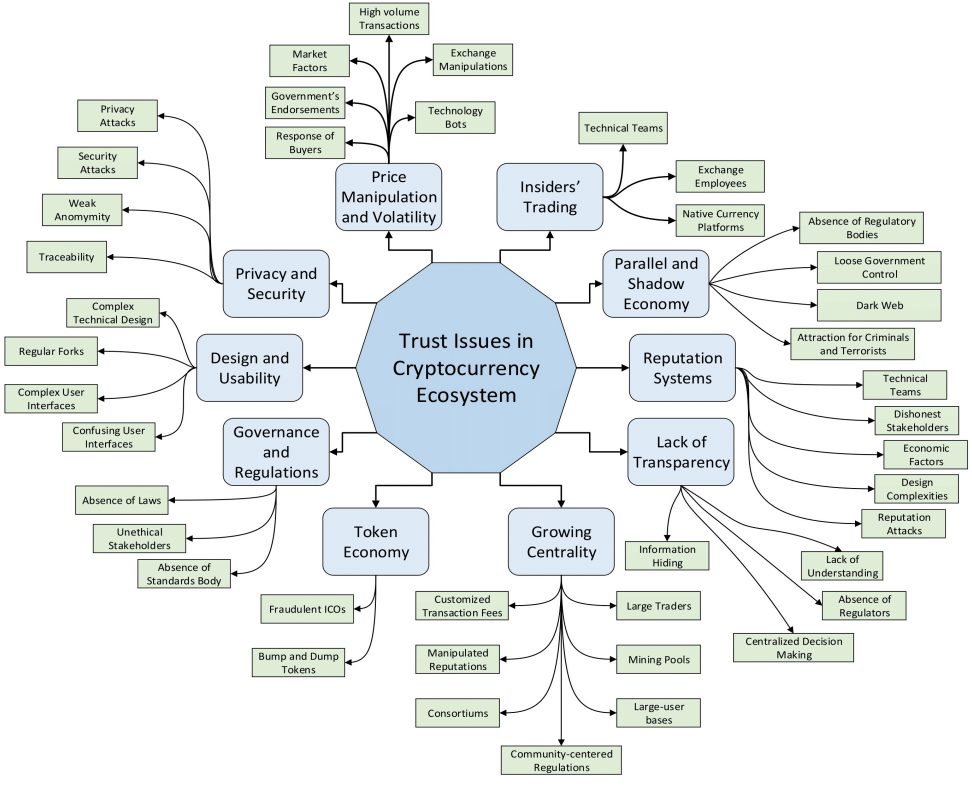
vs. Austria has the total consumption of **64.60 billion kWh (TWh)**

of electric energy per year. Per capita this is an average of 7,227 kWh. (**vs. 1765.42 kWh / Bitcoin transaction)**

Austria can partly provide itself with self-produced energy. The total production of all electric energy producing facilities is 61 bn kWh. That is 94% of the country's own usage. The rest of the needed energy is imported from foreign countries. Along with pure consumptions the production, imports and exports play an important role. Other energy sources such as natural gas or crude oil are also used. (source: https://www.worlddata.info/europe/austria/energy-consumption.php)

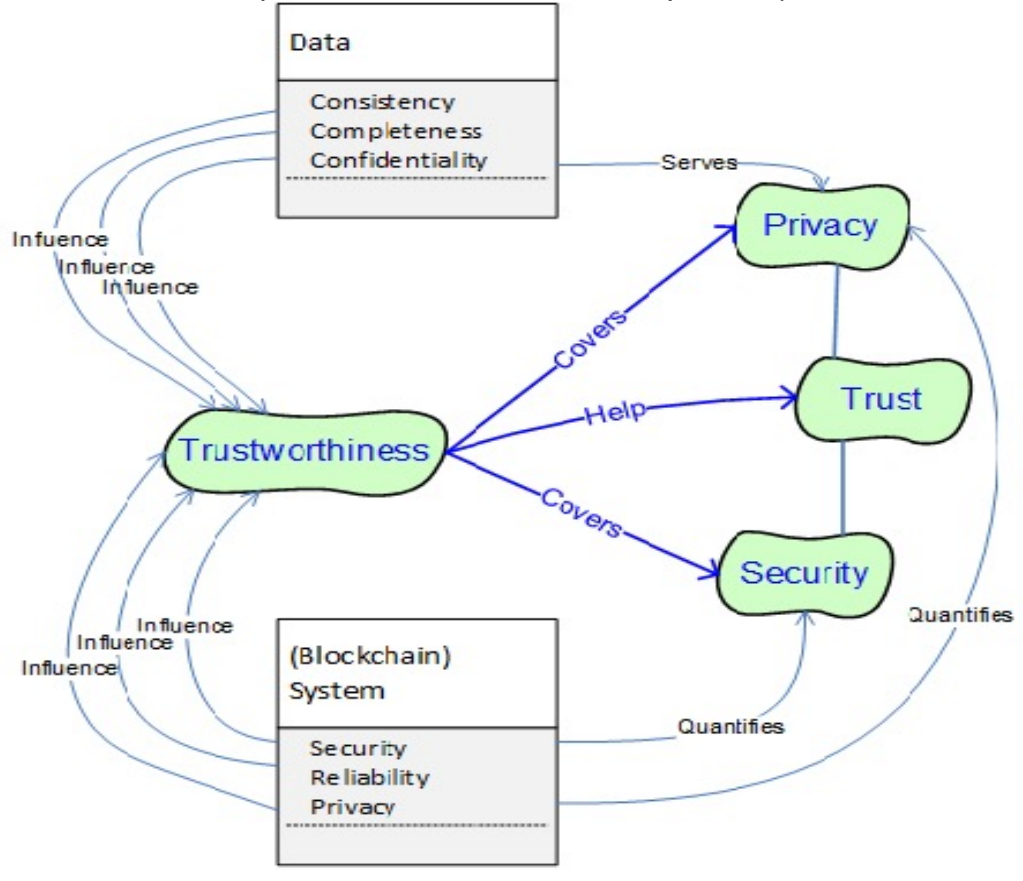
Project #3: Trust in Cryptocurrency Ecosystems / Blockchain Oracles

- M. H. u. Rehman, K. Salah, E. Damiani and D. Svetinovic*, "Trust in Blockchain Cryptocurrency Ecosystem," in **IEEE Transactions on Engineering Management**, 2020, doi: 10.1109/TEM.2019.2948861.



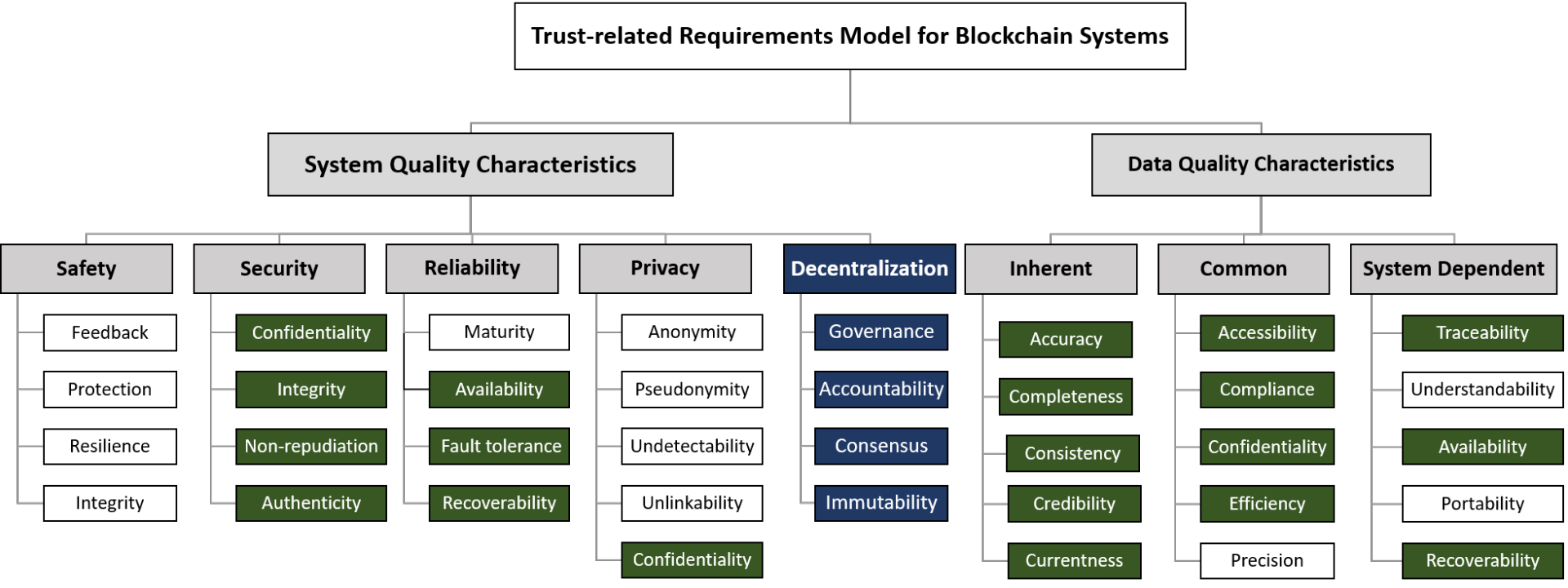
Project #4: Trust RE in Blockchain Systems

- H. Albreiki, M. H. Rehman, K. Salah, H. Kaindl, Y. Yu, E. Damiani, D. Svetinovic, "Trust-Related Requirements Elicitation and Specification for Blockchain Systems", **IEEE Transactions on XXX** (Status: Under Revie



Project #4: Trust RE in Blockchain Systems

- H. Albreiki, M. H. Rehman, K. Salah, H. Kaindl, Y. Yu, E. Damiani, D. Svetinovic, "Trust-Related Requirements Elicitation and Specification for Blockchain Systems", **IEEE Transactions on XXX** (Status: Under Review).



Blockchain Trust 1/2

- Operating correctly is critical for security/privacy/**trust**.
- **Energy and effort** invested in building the blockchain **must be there** to preserve security/privacy/trust (avoid alternative versions of the blockchain)
- **(Random) work to build a chain + network selection of the longest (most difficult) chain = Nakamoto's (practical) solution to Bysantine Generals' Problem => core blockchain security/trust mechanism**
- Given how expensive all of this is… what about the various applications of blockchain technology?

Blockchain Trust 2/2

- Many are nothing more but standard centralized systems: “Private” or “money-less” blockchains -> have “fun” with standard software/hardware security/privacy issues
- However, for fully public, decentralized, and incentivized blockchains -> we are not really sure what we are dealing with yet in terms of trust: **Economics (?) ++ Software ++ Hardware ++ ???**
- Consensus is implemented in software and ensured by hardware. Economic incentives must be done right, and “absorb” all the software/hardware “bugs.” We believe **??? unknown** might be the missing “social” constructs which we were not able to identify so far beyond…

The Important Social Blockchain Trust Threats

WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

- Social threats
- Planting rogue entities
- Creating dissent
- Spreading wrong information
- Creating arguments
- Legalization
- Regulation, etc.
- And at the same time **ongoing blockchain convergence with AI** (with its own trust, ethical, fairness issues) **and IoT** (with its own privacy, security, and trust issues).

So, what should we do?

Blockchain-AI Infrastructures for Trust in Socio-Technical Systems

WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

- We are already implementing AI-Blockchain-IoT platforms (e.g., singularitynet), which is good, but we don't have even basic trust concepts and issues resolved.
- What is trust? Unfortunately, from the engineering perspective there is no even a well-defined technical requirements model. (We worked on it)
- Critical to tackle all components in parallel: hardware security/trust, software security/trust, social security/trust, explainable AI and emerging behavior security/trust.
- We must develop a **trust infrastructure** that can **absorb the large costs** and **enable integration of complex AI applications** that will (at least in theory) replace traditional social trust-related services.

Decentralized Blockchain-Based Federated Machine Learning Applications

WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

- AI is creating **many new exciting socio-technical systems engineering challenges** to facilitate development of new emergent, adaptable, AI-based systems. **Lots of bias and fairness issues**.
- In particular, **ultra-long term** nature of such systems must be taken into account. We lack software engineering techniques for development of such systems.
- **Make social science findings and results engineering ready**. Learn how to implement them using trust-focused decentralized Federated Learning Applications.
- Recently published: M. H. u. Rehman, A. M. Dirir, K. Salah, E. Damiani and D. Svetinovic*, "TrustFed: A Framework for Fair and Trustworthy Cross-Device Federated Learning in IIoT," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2021.3075706.

WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Institute for Distributed Ledgers and Token Economy

https://www.wu.ac.at/en/tecon

The Institute focuses on the cutting-edge research in the **fundamentals of blockchain technology and the applications to economics, law, business, and social sciences.**

Research Institute for Cryptoeconomics

https://www.wu.ac.at/en/cryptoeconomics/team

The institute focuses on interdisciplinary analysis and applications of cryptoeconomics and blockchain technology.

VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Prof. Davor Svetinovic
Department of Information Systems and Operations Management
Institute for Distributed Ledgers and Token Economy
Vienna University of Economics and Business
T +43-1-313 36-4255
davor.svetinovic@wu.ac.at
wu.ac.at/tecon
davors.com