Legal aspects of blockchain and digital assets – Issues of Technology and Law

12 February 2026 09:00

ELTE Faculty of Law, Aula Magna

The aim of Interdisciplinary international conference on technological and legal issues organized by Attila Menyhárd, professor at the Department of Economics and Technology Law, is to provide a broad overview of current legal issues that hinder, restrict, or even prevent IT developments in the industrial, financial, and service sectors.

Key topics:

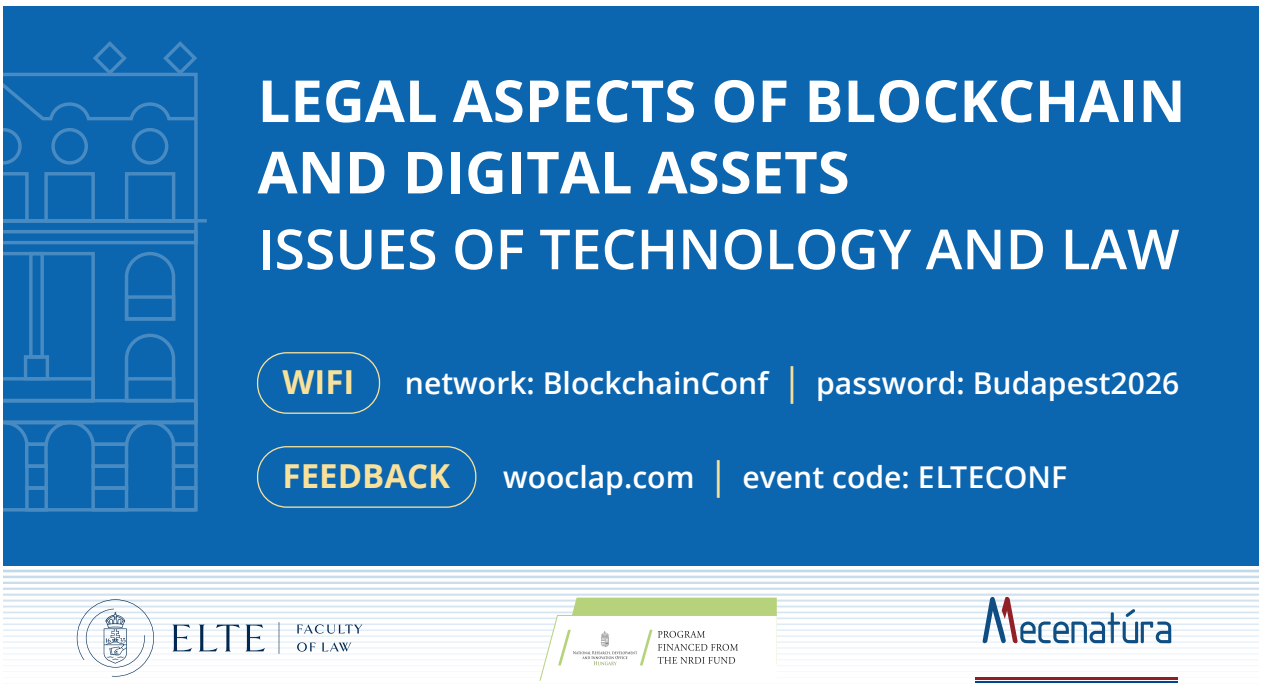
Technology: AI, blockchain

Law: Law of Technology

Assets, Crypto Assets

Financial Sector

Costumer Protection



IN MEDIAS RES: ASSETS

Data Ownership: Where We Are, and Where We Are Heading

Tamás Parti
Vice President, Hungarian Chamber of Civil Law Notaries, Head of its Data Research Unit

Data ownership: where we are, and where we are headed…

Tamás Parti PhD.,12.02.2026.
tamas.parti@ptki.hu, //hu.linkedin.com/pub/dir/Tamas/Parti
Wallpaper: Albrecht Dürer, Melencolia I.

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Problem Statement

- The data economy - and the digital data and data-based assets traded within it - is built on digital data. The existence of the data economy and data trading is evident; at the same time, property rights are a fundamental feature of both the economy and commerce. It follows that property-law regimes must also respond to these phenomena, which entails the property-law adaptation of digital data and data-based assets.
- By "digital assets" we typically mean cryptocurrencies, tokens, and NFTs, which play an important role in today's digital markets. However, the broader universe of digital assets - together with data and data-based assets - is far more diverse and continues to expand, including digital data themselves, which are traded, for example, for data-research purposes. The concept of "digital assets" therefore needs to be understood in a wider sense.
- Their economic relevance is increasing both at the level of national economies and globally, while legal regulation worldwide continues to face persistent challenges – especially as regards their treatment within property law. With a few exceptions, the law still does not treat digital data and data-based assets as part of property/wealth; rather, only the rights relating to them are typically recognized as an element of property.
- The rapid diversification of digital phenomena contrasts sharply with the law's limited conceptual capacity to capture and regulate them. Although regulatory approaches vary significantly across legal systems, they remain fragmented and lack a coherent conceptual framework capable of reflecting the complexity of digital phenomena and structuring them into consistent regulatory narratives.
- The underlying problem is not regulatory diversity but conceptual misalignment: ***digital data and information*** are treated as interchangeable, each being interpreted through the other, while legal narratives emphasize the informational characteristics of digital phenomena
- Existing regulatory narratives - largely because they approach digital-data phenomena through the lens of information - typically classify them as intangible assets. Yet digital data themselves are distinctly physical phenomena and, based on their intrinsic properties, do not belong to the set of intangible phenomena; rather, they should be placed in the category a kinde of tangible (physical) assets.
- This conceptual deficit constitutes a major obstacle to effective regulation. It is particularly evident in the persistent difficulties surrounding the property-law treatment of digital data and data-based assets.

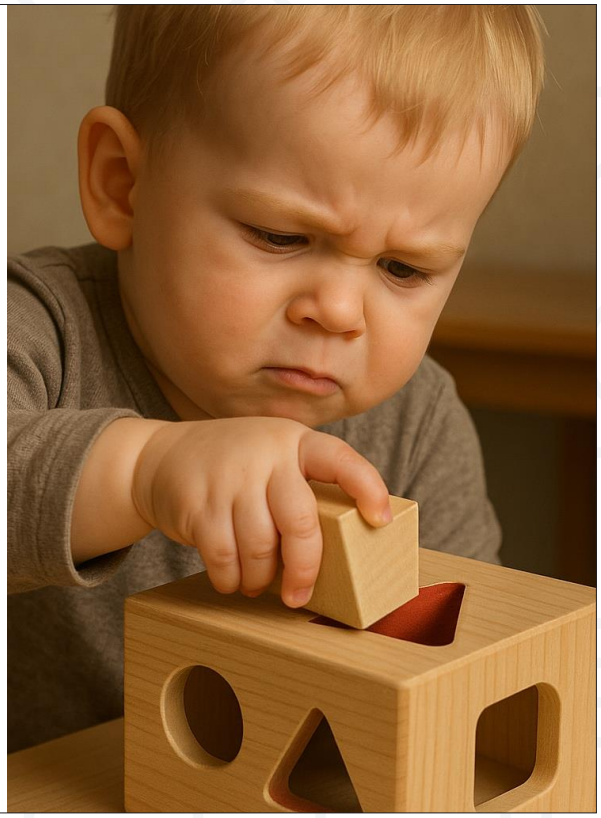
Data definitions in the European Union's key data regulatory instruments:

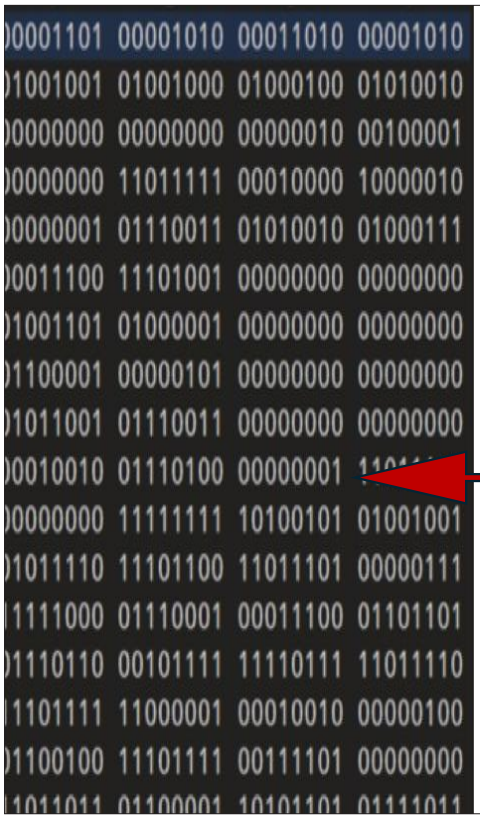
- - ***GDPR***: Article 4. Definitions (1): ***'personal data' means any information*** *relating to an identified or identifiable natural person*
- a ***DATA ACT***: "***Data' means any digital representation of acts, facts or information*** *and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording - and for example* ***we know who may data holder be****, but* ***we don't know where they get the data from*** *or* ***where their rights to the data come from****.*
- *a* ***Data Governance Act****: 'Data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording;*
- ***INDIRECT regulation of data as a commodity*** — Directives 2019/770/EU and 2019/771/EU on certain aspects of contracts for the supply of digital content and digital services ***focus on goods that contain digital data, digital content, or digital services, rather than on the data itself***
- **ALI – ELI Principles for Data Economy - Data transactions and Data Rights** :"(a) '***Data' means information recorded*** *in any machine-readable format suitable for automated processing, stored in any medium or as it is being transmitted…* ***or*** ***"electronic record means information.."*** *–* ***UNIDROIT's principle*** *2.(1))*

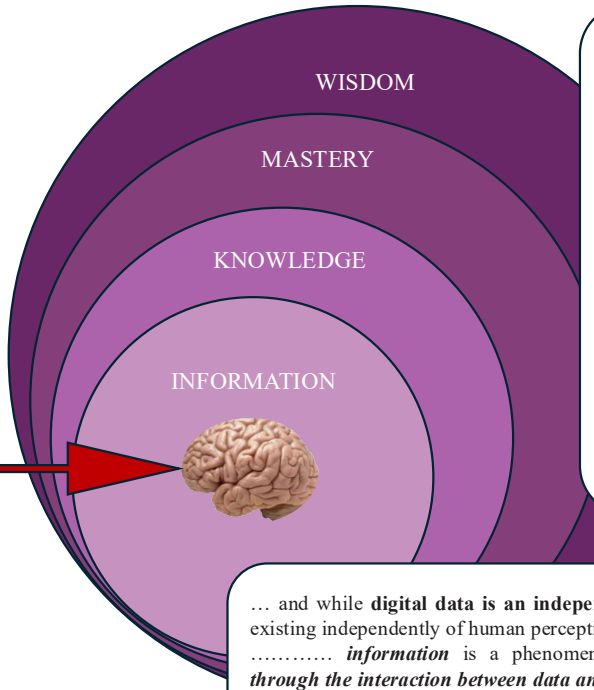
… And at this point, all of us – not only civil law, but common law as well - run into a conceptual/doctrinal problem……

- The law has not yet developed a complete conceptual toolkit for digital phenomena that would allow it to interpret digital assets effectively, in light of the diversity of legal-system approaches.

- In short, we are still not able to articulate digital phenomena with sufficient precision for legal regulation and for coherent regulatory narratives.







– Digital information is the ***result of the interaction between digital data and the human brain.***

– Information is created when humans ***interpret / understand data.***

– ***Each*** specific piece of ***digital information*** is always grounded in ***a fixed data context*** that cannot be interpreted in any other way (*e.g., an image depicting a sunflower cannot be interpreted as the text of a poem*).

… and while **digital data is an independent entity of physical reality**, existing independently of human perception and legal recognition, ……. ……. ***information*** is a phenomenon that arises and ***exists only through the interaction between data and the human mind*** that interprets it, and therefore ***cannot easily be understood independently of the human individual***. It is thus not surprising that ***many legal approaches*** to the digital phenomena from the perspective of information ***are grounded in personal rights, and consider it as intangible object.***

Treating digital data and digital assets as property requires more than analogy - it requires alignment with the foundational principles of property law.

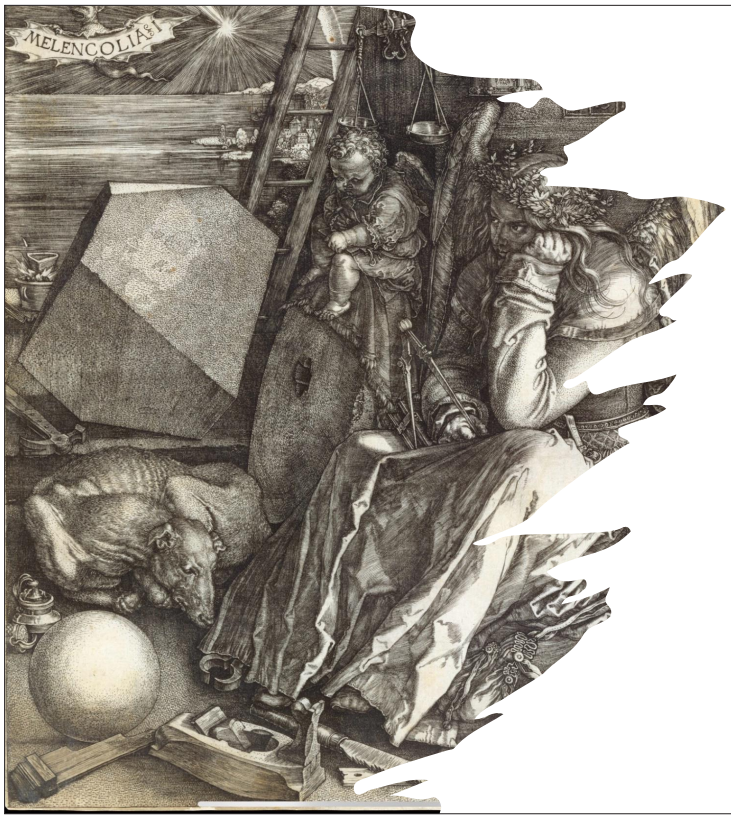
- In comparative terms, there is no single uniform system of property law across jurisdictions, but many legal systems rely on broadly similar underlying principles. In general, an asset (i.e., an object capable of being the subject of proprerty rights) should be:
- *- definable;*
- *- identifiable by third parties;*
- *- capable of being held, controlled, or transferred by third parties;*
- *- sufficiently stable / persistent;*
- *- economically valuable.*
- *Property regimes typically presuppose features such as:*
- *- erga omnes effect (the "absolute" character of property rights);*
- *- exclusivity;*
- *- transferability (at least in principle);*
- *- publicity (transparency) vis-à-vis third parties;*
- *- and, depending on the system and the asset, embodiment/corporeality may also matter.*
- ***The principles of numerus clausus and publicity are widely regarded as characteristic features of property regimes (Sjef van Erp).***

Breakthroughs – common law in advantage

- ***Two typical examples*** of breakthroughs in Europe — a kind of "hacking" of the Civil Code – Sectoral regimes are bringing tokenised, data – based assets within the property system.
- ***§ 2(3) German eWpG*** (Electronic Securities Act):"Ein elektronisches Wertpapier gilt als Sache im Sinne des § 90 des Bürgerlichen Gesetzbuchs."("An electronic security is deemed to be a thing within the meaning of § 90 of the German Civil Code.")
- ***Code monétaire et financier***, 1° and 2°:(French Financial and Monetary Code — "For the purposes of this chapter, digital assets shall mean: …")
- ….. And, ***common law legislation are already ahead:***
- The Property (Digital Assets etc) Act 2025, in force since 2 December 2025, adopts an *explicitly agnostic approach. It provides that: "A thing (including a thing that is digital or electronic in nature) is not prevented from being the object of personal property rights merely because it is neither (a) a thing in possession, nor (b) a thing in action."*

.. What can we gain from the property-law regulation of digital data and data-based phenomena?

- ***Conceptual clarity***: distinguishing data from information eliminates dogmatic uncertainty.
- ***Entry of property law into the digital domain***: data and data-based assets can be clearly classified as part of the property estate.
- ***Enforceability***: stronger legal enforcement, including tracing, recovery, and restitution.
- ***Market confidence and stability***: a predictable legal status leads to lower risk and greater investment willingness.
- ***Financing capability***: data-based assets can be used as collateral, held in deposit, or serve as objects of asset management.
- ***Insolvency and succession compatibility***: such assets can be included in insolvency, bankruptcy, and inheritance proceedings.
- ***Finally, it should not be overlooked that***, as a consequence of the social function and obligations inherent in ownership, these assets could likewise become subject to the property-related social obligations accompanying ownership. ……..



- Thank you for your attention
- tamas.parti@ptki.hu, //hu.linkedin.com/pub/dir/Tamas/Parti
- *Wallpaper: Albrecht Dürer, Melencolia I.*

Tokenization of Securities and Real-World Assets: New Clothes for Old Concepts?

António Garcia Rolo
Universidade de Lisboa

Introduction

- Cryptoassets, tokens, digital assets are digital representations of rights, obligations and/or value whose ownership and transferability is determined through blockchain or another DLT.
- The key characteristics of cryptoassets is therefore the way their ownership and legitimacy to transfer are determined.
- Blockchain technology has a revolutionary potential but it is merely a new form of private registry.
- Tokenisation is not a separate phenomenon from wider cryptoassets.

What is Tokenisation?

- Tokenisation is often defined as the representation of financial or RWAs in the form of a cryptoasset/token, i.e., represented on a blockchain or another DLT.
  - New form of representation of a legal relationship, bundle of rights or obligations, or physical assets. Blockchain is used to determine ownership and legitimacy to transfer.
- Obvious advantages – enabling access of ownership of several assets, democratisation of finance and fast transfer of assets, especially when costly RWA are involved.
- Not a straightforward concept, with various different empirical phenomena seen as “tokenisation”.

Types of Tokenisation

- Direct or native tokenisation – tokens are primary form of asset representation.
  - Some tokenised securities or CBDCs.
- Indirect tokenisation – tokens represent rights on an intermediary structure controlling the assets and backed by the assets.
  - Tokenised SPV shares, tokenised fund units, commodity-backed stablecoins.

Complete Tokenisation

- Incomplete tokenisation – tokens do not fully embody the legal rights of the underlying asset and serve as an information sharing instrument.
  - Mirroring assets.
  - No claim under law.

Legal Approaches to Complete Tokenisation

Acknowledgment of Tokenised Securities

- Explicit or implicit recognition that securities law applies to tokenised securities.
- No legal framework for securities tokenisation.
- Default approach in the EU under MiCA's technological neutrality stance.
- DLT Pilot Regime develops that route.

Bespoke Direct Tokenised Securities Frameworks

- Legal acts and frameworks that directly address the procedural and legal aspects of tokenisation and recognise tokenised securities as an autonomous category of securities representation.
  - The token is the exclusive formal representation of the security.
  - Integration with market infrastructure.
- France - CMF foresees direct tokenisation and treats tokenised financial instruments as a standalone category. Article L.211-3: "*financial instruments issued in France and subject to French law can be registered in a registry book held by the issuer or by an intermediary, or through a distributed ledger technology*".
- Germany - 2021 Electronic Securities Act allows for the issuance of crypto-securities (*Kryptowertpapiere*), imposes market infrastructure requirements and allows conversion.
- Spain – 2023 Securities Market Law – securities can be represented by DLT, with market infrastructure requirements and allowing original tokenisation and conversion.

Provisional Concluding Remarks

- Cryptoassets and tokens usually represent some traditional legal relationship – they are always legally relevant even in the absence of a bespoke regime.
- With or without a bespoke framework, and both from an empirical and legal point of view, tokenised securities represent a new set of clothes with the same content as traditional securities – is it a technological jump comparable to the jump from paper-based securities to registry securities?
- Tokenised securities are as much things as registered or title securities and can be neatly placed in the continental tradition of titles of credit as representations of more or less complex bundles of rights and/or obligations.

Direct Tokenisation of Real-World Assets

- If tokenisation of securities is a mere technological update, is direct RWA tokenisation where real legal innovation lies? It's not that simple
- Indirect tokenisation of RWA, through an SPV, stablecoin or another contractual arrangement is not problematic in most jurisdictions per se.
- Direct tokenisation of RWA such as moveable assets, commodities or real estate implies holding an *in rem* right over an asset and having a direct claim. This is legally much more challenging and requires changes to basic civil and property law.

Direct Tokenisation of Real-World Assets

- Liechtenstein: General Admissibility of Tokenised Assets?
  - 2020 Token and Trusted Technology Service Provider Act introduced changes to core civil law tenets and is open to direct tokenisation of almost any class of assets, defining token as a representation of "*claims or rights of memberships against a person, rights to property or other absolute or relative rights*". Wide enough to include almost any right and/or obligation with the exception of personal rights.
  - Token container model? Yes, but does not override civil law provisions completely.
- Dubai: Licensable RWA Tokenisation
  - VARA Regulations provide for the possibility of issuing asset-referenced virtual assets (ARVAs), i.e., virtual assets that represent direct, indirect, current, future or contingent ownership of any RWA, or entitlement to receive or share any value that originates from RWAs or that is directly or indirectly wrapped, duplicated, fractionalised, securitised or a derivative of any other ARVA.
  - Wide definition that allows direct tokenisation of almost any RWA, with regulations recognising it can represent a direct right of ownership over the reference asset.
  - Contrarily to Liechtenstein, no general admissibility, as VARA retains high degree of discretion to allow and license such ARVAs.

Second Conclusion

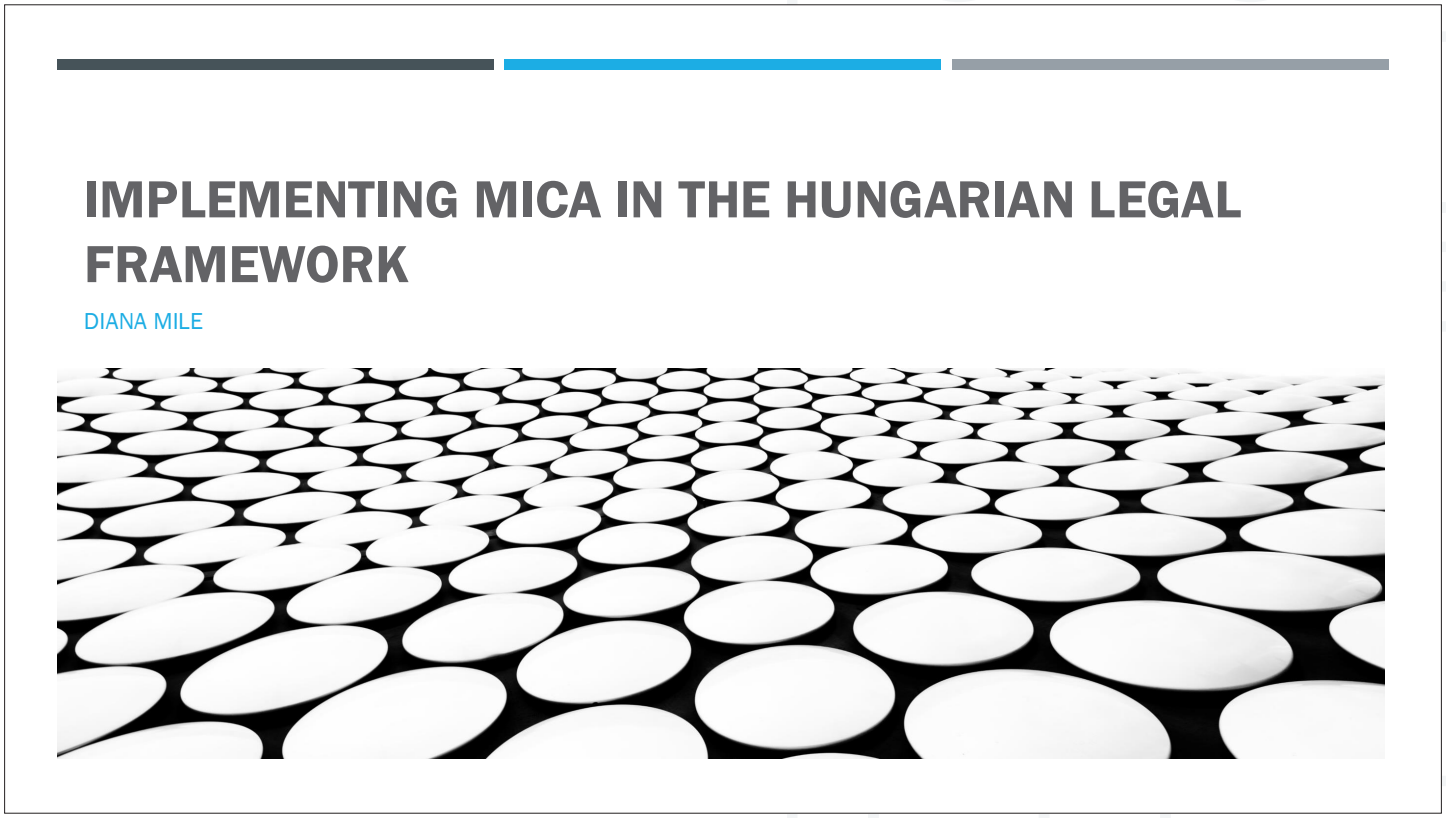
- Despite the promises of these RWA direct tokenisation frameworks, they have not gained a lot of traction to date over indirect tokenisation.
  - Direct RWA tokenisation might not even be beneficial for issuers and industry players may prefer to preserve some flexibility using indirect tokenisation strategies, which replicate, mostly, traditional securitisation.
- Direct RWA tokenisation would require an overhaul of traditional property rights and public land registries, which might be at odds with traditional State monopoly of property rights and land registry.
- In any case, with this lack of incentives, we might just watch the proliferation of indirect tokenisation schemes, some which replicate old securitisation models (and others not). Mostly new clothes for old concepts, but not only.

Köszönöm a figyelmet!

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Implementing MiCa in the Hungarian Legal Environment

Diána Mile
Attorney at Mile & Partners, Mile Law Office, Blockchain Hungary Association



CURRENT STATUS, KEY REGULATORY TENSIONS, AND LAW PRACTICE IMPLICATIONS

- EU's *Markets in Crypto-Assets Regulation* (MiCA) – harmonised EU crypto-asset law.
- MiCA entered into force with national application obligations by Dec 2024/Jul 2025.
- Hungary passed its own crypto law, *Act VII of 2024* (Crypto Act) and amendments (Act LXVII of 2025).

2026. 04. 17.

WHAT MICA REQUIRES

- MiCA creates **uniform authorisation & supervision** for crypto-asset service providers (CASPs) across EU.
- Focuses on **transparency, disclosure, licensing, investor protection** under a single EU rulebook.
- National law must not conflict; member states *cannot add extra authorisation layers or criminal sanctions* beyond MiCA.

2026. 04. 17.

HUNGARY'S NATIONAL APPROACH

- Hungary's *Act VII of 2024* (Crypto Act) was amended by *Act LXVII of 2025* introducing an **"exchange validation" regime**. (+ SARA Decree 10/2025)
- Requires a **validator certificate for every crypto-to-crypto/crypto-to-fiat transaction.**
- Criminal liability introduced for non-validated transactions — a novel, **stricter domestic enforcement layer**.

2026. 04. 17.

WHAT THE VALIDATOR ACTUALLY DOES

- Performs transaction-level validation
- Checks compliance before execution
- Not a licensing authority (SZTFH/SARA)
- Not a supervisory body under MiCA but dual structure (MNB/SZTFH)

2026. 04. 17.

WHAT DOES NOT FALL UNDER THE VALIDATOR REGIME?

- **Personal Use/Own Wallets:** Conversions where a natural person transfers or exchanges their own crypto-assets into other crypto-assets exclusively for their own, non-commercial purposes.
- **Non-Regular/Non-Commercial Transactions:** Crypto-asset conversion services that are not provided on a regular basis, or those that are conducted without consideration.
- **Decentralized Exchanges (DEX):** Transactions executed in a truly decentralized manner, particularly those utilizing smart contracts for liquidity pooling or bridging to ensure interoperability between DLT networks.
- **Covert Intelligence:** Transactions conducted by authorized authorities for specific, covert intelligence purposes.

2026. 04. 17.

COMMISSION INFRINGEMENT CASE

The **European Commission opened infringement proceedings** (INFR(2025)2174) against Hungary for non-compliance with MiCA.

Core complaints:

A national “exchange validation” regime **not foreseen in MiCA**.

Criminal sanctions beyond MiCA’s framework.

Hungary must respond within two months — else the case may escalate to a *reasoned opinion*.

2026. 04. 17.

MARKET & LEGAL IMPLICATIONS

The infringement notice **does not suspend Hungarian law** — validation obligations remain in force.

Validator partnership required

(national bottleneck)

combined with a slow initial registration of validators

Some CASPs have already **suspended or limited services** in Hungary due to compliance risk.

Law firms and compliance teams must monitor **state response and potential legislative change.**

2026. 04. 17.

THE "BITPANDA EFFECT"

Compliance is possible

Access to compliance is narrow

One validator = one pathway

Legal certainty becomes selective

2026. 04. 17.

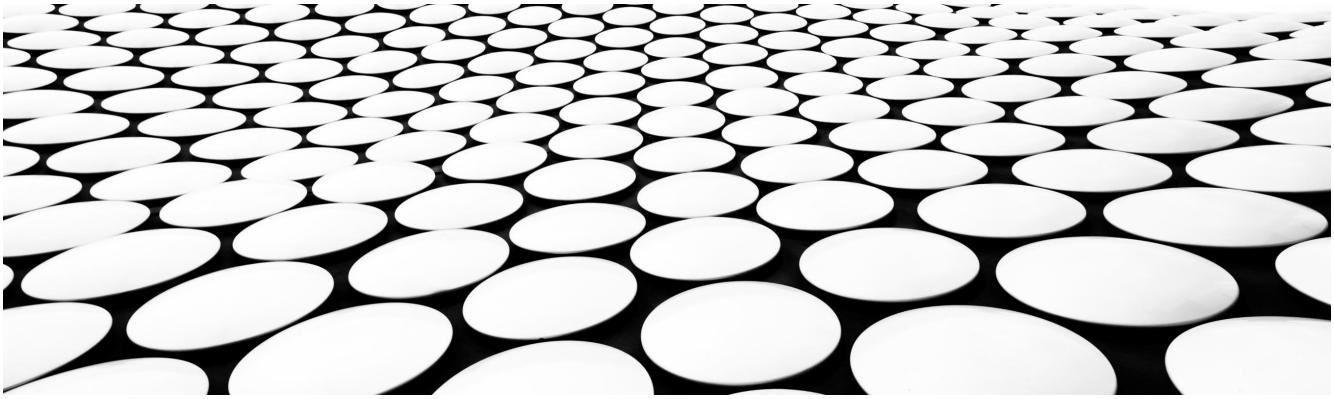
CLOSING TAKEAWAY — WHAT THIS CASE REALLY SHOWS

- MiCA was designed to remove national gatekeepers
- The Hungarian validator reintroduces one, or is it AML?
- Compliance is possible — but not equally accessible
- Possible amendments if Hungary adjusts law

2026. 04. 17.

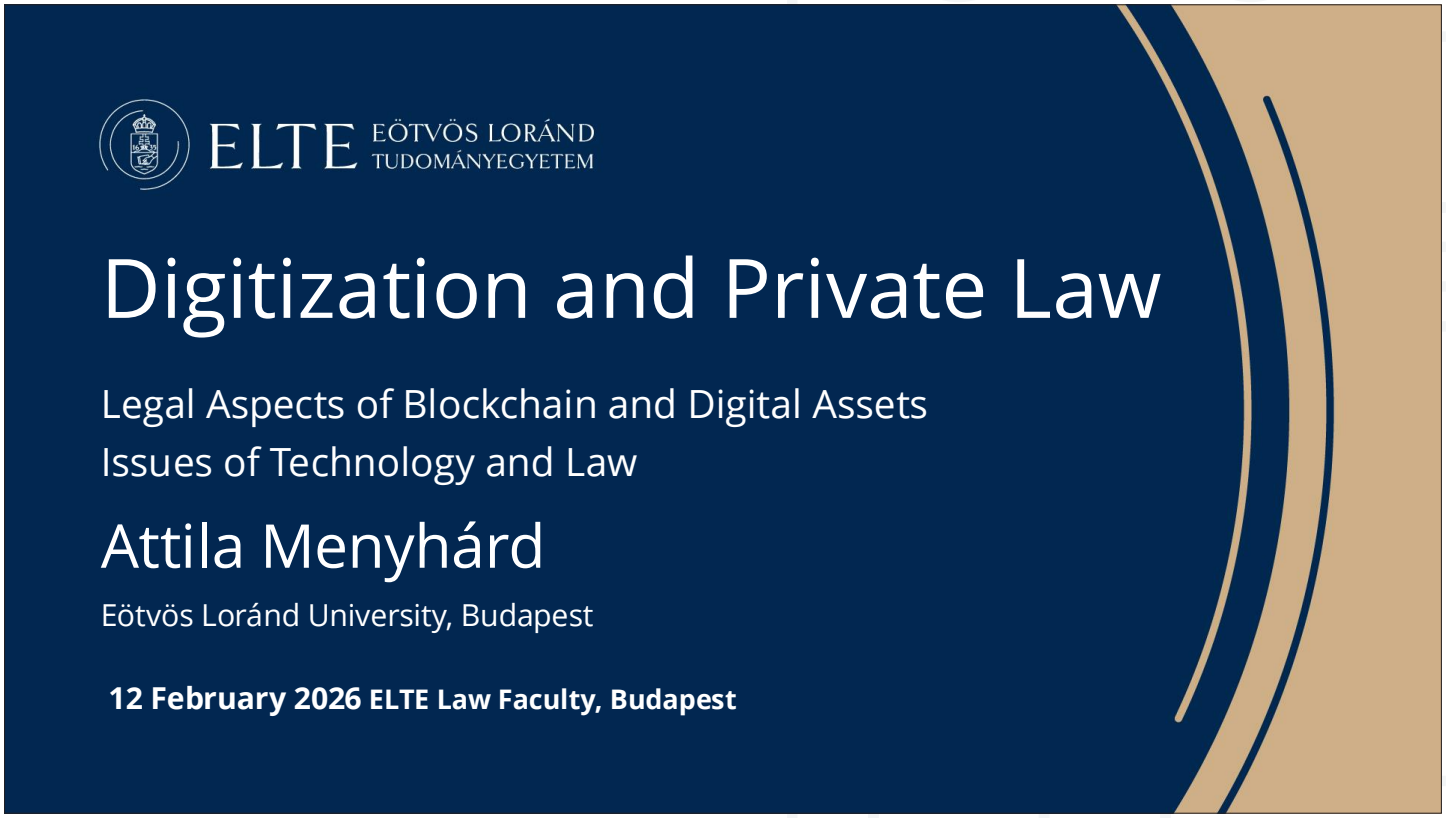
THANK YOU.
QUESTIONS AND REFLECTIONS WELCOME.

DIANA MILE

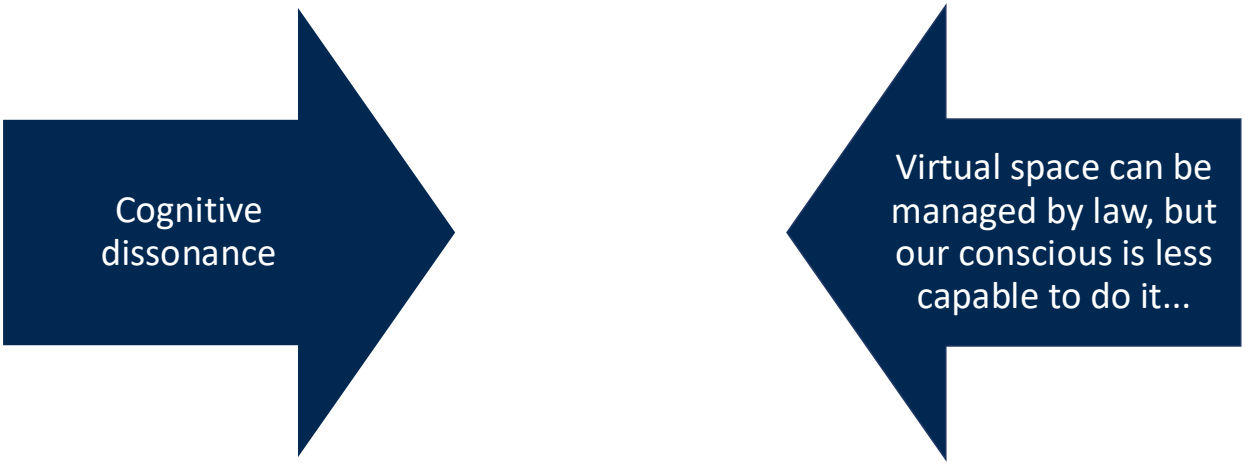


PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Digitization and Private Law
Attila Menyhárd
Professor, ELTE Law, organiser



Virtual and material reality



ELTE EÖTVÖS LORÁND TUDOMÁNYEGYETEM

Concepts that are to be reconsidered

Consent in digital environment and „informed" consent
Decision or resolution
Property
Transferability (of assets)
Role of written form and corporeability
Money and securities
Liability (no-fault liability regimes)
Personality
Sovereignty and technofeudalism?

ELTE EÖTVÖS LORÁND TUDOMÁNYEGYETEM

Thinking within the conceptual framework of fundamental rights

Compliance with fundamental rights is part of the legal compliance test

Decision-making is not transparent

- huge amounts of data traffic, reliance on algorithms, autonomous decision making

Opaque causal processes in the event of a disadvantage

Risk of discrimination

Risk of interference with privacy

Risk of loss of trust

Enforcing the rule of law criteria against gatekeeper OPSs

OPSs as part of legal enforcement regime

Protecting the vulnerable – not only the weaker party

Framework of consumer protection was a result of a compromise and should be reconsidered

- consumers are just a group of vulnerable persons

New framework of discussion: protecting fundamental rights (anti-discrimination, privacy, human dignity)

- vulnerability goes far beyond economic interests

Business can be vulnerable as well, equally to consumers

Protection of children may not fit in consumer policy framework

What about non-business and non-consumer players (like, e.g. politicians)?

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Why to go beyond the consumer protection policy framework?

Remedies should go beyond the consumer protection framework

as to the scope of the protected persons

the scope should be extended beyond contract law

not only torts but claims for unjust enrichment also should be considered

disgorgement of profit

Remedies should focus on the Online Service Provider (if relevant)

digital transformation changed the market

relational approach (B2C), which focuses on transaction, is less useful

Online Service Provider should be assumed as part of the system of legal enforcement („invisible handshake")

Framework of remedies (including liability framework) should be improved

Consequences in contract law

Contractual freedom is becoming relative

Separate legal treatment of consumer (B to C) and commercial (C to C) relationships

"From status to contract" (H. S. Maine) and back?

In consumer contracts, the general model is to control the content of the standard terms

- no actual consent in the original meaning
- focus on principles of rule of law

The rise of public enforcement (strong state intervention)

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Benefits of blockchain

Decentralisation is possible but not necessary

Real time communication

Performing contracts

Proof of title

Automated settlements

Real time review of documents for the parties as well as supervising authorities

Simple and registered communication between market players, e.g. banks and other market players like insurance companies

- important e.g. if collateral was provided as security and insurance covers the value of collateral

ELTE EÖTVÖS LORÁND TUDOMÁNYEGYETEM

Blockchain as a technology

Relevant primarily for digital assets

No central server is necessary (peer-to-peer network)

- communication technology (e.g. DAO, crowd funding)
- register of virtual assets (BTC and other "coins", NFTs)
- recording the transfer of registered property

Recording acquisitions in a ranking list, such as

- land registers and other registers
- rotation on printed securities

Stored transaction data cannot be deleted

- but we should be able to manage the deletion (GDPR)

ELTE EÖTVÖS LORÁND TUDOMÁNYEGYETEM

Digital assets

They are created, stored and transferred in virtual space

- on computer networks ("peer-to-peer") or
- in the cloud (cloud services)

They have legal value

We recognise a right of disposal over them

They are a significant economic factor

The law can handle such assets, because law does not allocate goods, but rights
the legal relationship is a social relationship

ELTE EÖTVÖS LORÁND TUDOMÁNYEGYETEM

Determining the applicable law: specificities

The cornerstone of private international law: qualification

Qualification is a two-way process

Virtual assets are not location-bound and can be dual in nature, personal and material (e.g. personal and non-personal data)

Specific problem: digital assets to which rights or other entitlements (e.g. copyrights) over physical objects are attached ("linked assets")

ELTE EÖTVÖS LORÁND TUDOMÁNYEGYETEM

Applicable law: proposals

For digital assets, the connecting factor (UNIDROIT DAPL)

- Primarily, private autonomy, i.e. determined by the parties who create
- secondly, the place of issuing the asset (if any)
- thirdly, the issuer's right (if there is an issuer)

Law of the forum (ELI/ALI Principles For a Data Economy, Art 38)

Hague Conference on Private International Law (HCCH): recently launched project

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

ESSENTIA OBLIGATIONIS: FINANCIAL SECTOR

The AI Act and its Impact on the Financial Sector, with a Particular Focus on the Categorization of AI Systems and the Resulting Obligations for Financial Institutions

Damián Palašta
Masaryk University, Brno

MUNI LAW

AI Act and the Financial Sector: Regulatory Logic

Mgr. Damián Palašta

Ph.D. Candidate, Institute of Law and Technology
Faculty of Law, Masaryk University
Lawyer, BioMedAI
Institute of Computer Science, Masaryk University

AI Act and the Financial Sector: Regulatory Logic

- AI Act designed to integrate with existing EU financial services law (**Recitals 9, 97; Articles 2(2), 74**)
- Ideally no parallel compliance regime for regulated financial institutions
- AI governance embedded into internal governance and risk management frameworks
- Objective: coherence between AI regulation and financial supervision

MUNI LAW

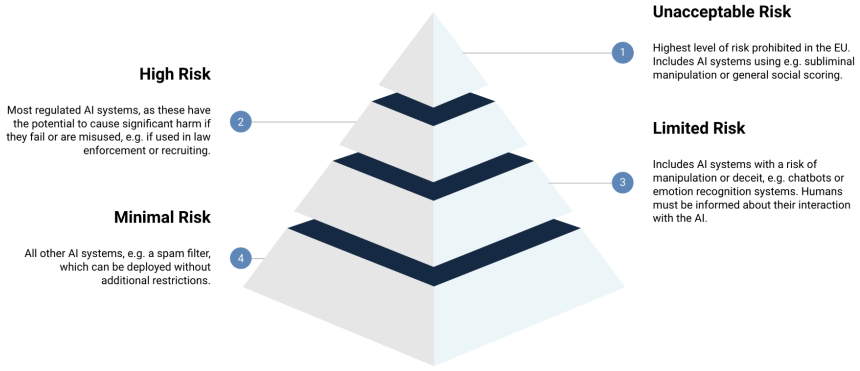
AI Literacy Obligation

- Providers and deployers must ensure sufficient AI literacy (Article 4(1))
- Applies to staff and other persons operating AI systems
- Required level assessed based on (Article 4(2)):
  - Technical Knowledge and experience
  - Training provided
  - Context of AI system use
  - Natural persons affected by the AI system
- AI Driving License?
- Omnibus change

MUNI LAW

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

System



https://www.trail-ml.com/blog/eu-ai-act-how-risk-is-classified

MUNI LAW

Prohibited AI Practices in Finance (Article 5 AI Act)

- Manipulation & deception (Art. 5(1)(a)):
  - AI may not use subliminal, manipulative or deceptive techniques to materially distort consumer behaviour, particularly where this impairs autonomy or causes significant financial harm; complements EU consumer protection law.
- Exploitation of vulnerabilities (Art. 5(1)(b)):
  - AI may not exploit vulnerabilities linked to age, disability or socio-economic situation (incl. extreme poverty); prohibits targeting vulnerable customers with high-risk or predatory financial products.
- Social scoring (Art. 5(1)(c)):
  - Prohibition of classifying natural persons over time based on social behaviour or personality traits where this leads to detrimental treatment in unrelated contexts or unjustified / disproportionate consequences.

MUNI LAW

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Prohibited AI Practices in Finance (Article 5 AI Act)

- Biometric categorisation (Art. 5(1)(g)):
  - AI may not infer sensitive attributes (race, political opinions, religion, trade union membership, sexual orientation) from biometric data; prevents discriminatory profiling and customer segmentation.
- Emotion recognition at work (Art. 5(1)(f)):
  - Financial institutions may not use AI to infer employees' emotions for management or productivity purposes.
- Fraud detection carve-out:
  - Predictive criminal risk assessment based solely on profiling is prohibited (Art. 5(1)(d)), but **transaction-based AI fraud detection remains permitted** (Recital 42)

High-Risk AI Systems – Classification (Article 6 AI Act)

- **Three ways an AI system qualifies as high-risk:**
  - **1. Product safety route (Article 6(1)(a)–(b))**
    AI is a product or safety component covered by Union harmonisation legislation (**Annex I**) **and** subject to third-party conformity assessment.
  - **2. Annex III route (Article 6(2))**
    AI systems explicitly listed in **Annex III** are presumed high-risk (e.g. creditworthiness assessment, insurance risk assessment).
  - **3. Profiling override (Article 6(3), last subparagraph)****
    Annex III AI systems **always** qualify as high-risk where they perform profiling of natural persons.
  - **Derogation from Annex III presumption (Article 6(3)):**
    Annex III systems may be excluded if they pose **no significant risk** and only perform narrow, preparatory or supportive tasks **without material influence**, **except** where profiling is involved.

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Annex III High-Risk AI Systems: Core Financial Sector Relevance

- Primary Annex III category for finance:
- Access to essential private services (Annex III, point 5)
  - Creditworthiness assessment & credit scoring (point 5(b))
    AI used to evaluate creditworthiness of natural persons
    Explicit exclusion: AI used solely for financial fraud detection
    Insurance risk assessment & pricing (point 5(c))
  - Life insurance
    Health insurance
- Legal effect:
  Systems listed under Annex III, point 5 are automatically classified as high-risk under Article 6(2) AI Act
  Subject to Article 6(3) derogation, unless profiling of natural persons is involved

Recital 42 AI Act – Profiling vs Fraud Analytics in Finance

- **Principle**:
  - Presumption of innocence – persons judged on actual behaviour, not AI-predicted behaviour (Recital 42)
- **Prohibition**:
  - AI predicting criminal offending based solely on profiling or personality traits(e.g. nationality, residence, debt level, type of car) (Recital 42; Article 5(1)(d))
- **Conditions required**:
  - Objective and verifiable facts; Reasonable suspicion; Human assessment
- **Financial carve-out:**
  - Prohibition does not cover AI fraud analytics– transaction-based, non-profiling systems assessing likelihood of financial fraud (Recital 42)

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Roles in the AI Value Chain

- Provider: develops or places AI system on the market under own name (Article 3(3))
- Deployer: uses AI system under its authority (Article 3(4))
- Importer and distributor: verification and compliance roles (Articles 3(6)–(7))
- **Role allocation determines scope of regulatory obligations**
  - (AI Act compliant SW is like GDPR compliant hard disk)

MUNI LAW

Provider Obligations for High-Risk AI

- Risk management system (Article 9)
- Data governance and training data requirements (Article 10)
- Technical documentation (Article 11)
- Quality management system (Article 17)
- Conformity assessment and CE marking (Articles 43, 49)

MUNI LAW

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Deployer Obligations in Finance

- Use AI system in accordance with provider instructions (Article 26(1))
- Monitoring of system operation (Article 26(2))
- Retention of automatically generated logs (Article 26(3))
- Human oversight obligations where applicable (Article 29)

Value Chain Shifts and Requalification

- Deployer or distributor becomes provider if (**Article 25(1)**):
  - Affixing own trademark to high-risk AI system
  - Making a substantial modification
- Requalified entity assumes full provider obligations (**Articles 16–23**)

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Interaction with Financial Regulation

- Quality management obligation deemed fulfilled via internal governance rules (Article 17(2))
- Technical documentation maintained within sector-specific records (Article 18)
- Log-keeping integrated into standard documentation procedures (Articles 19, 26)
- Monitoring obligations aligned with existing control mechanisms (Article 26)

Article 17(4) AI Act – Financial Sector Derogation

- General rule:
  - For regulated financial institutions, the obligation to establish a quality management system (QMS) for high-risk AI is deemed fulfilled by compliance with existing internal governance, arrangements and processes under EU financial services law (Art. 17(4)). (only providers)
- Practical effect:
  - No separate or parallel AI-specific QMS required for banks and insurers; AI compliance is embedded into existing governance frameworks (e.g. risk, compliance, internal control).
  - Key exceptions – AI-specific obligations remain, financial institutions must still independently comply with:
    - Risk management system (Art. 9)
    - Post-market monitoring (Art. 72)
    - Serious incident reporting (Art. 73)

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Fundamental Rights Impact Assessment

- Mandatory prior to deployment of high-risk AI in finance (**Article 27(1)**)
- Applies to credit scoring and insurance risk assessment
- Assessment must include (**Article 27(2)**):
  - Description of AI-supported processes
  - Categories of affected natural persons
  - Risks to fundamental rights
  - Human oversight measures
- Notification to market surveillance authority required (**Article 27(4)**)
- DPIA vs. FRIA, Technocratic vs. Right based approach

16 AI Act and the Financial Sector: Regulatory Logic

MUNI LAW

Supervision and Enforcement

- National financial supervisory authorities:
  - Designated as AI market surveillance authorities for high-risk AI systems used by regulated financial institutions (Article 74(6))
- Competence applies:
  - Where the AI system is directly connected to the provision of financial services (Article 74(6))
- Single Supervisory Mechanism (SSM):
  - National authorities supervising credit institutions must report without delay any AI-related findings relevant for prudential supervision to the European Central Bank (Article 74(7)
- Penalties:
  - Prohibited practices: up to EUR 35m or 7% turnover (**Article 99(3)**)
  - Other infringements: up to EUR 15m or 3% turnover (**Article 99(4)**)

17 AI Act and the Financial Sector: Regulatory Logic

MUNI LAW

MUNI LAW

Thank you

Mgr. Damián Palašta
palasta@ics.muni.cz

18 AI Act and the Financial Sector: Regulatory Logic

Artificial Intelligence and Deepfake-Enabled Fraud in the Banking Sector: Identification and Classification of Emerging Threats

Kristýna Mlčáková
Researcher, Institute of Law and Technology, Faculty of Law, Masaryk University, Brno

CENTER FOR INEQUALITY AND OPEN SOCIETY

AI and Deepfake-Enabled Fraud in the Banking Sector: Identification and Classification of Emerging Threats

Kristýna Mlčáková

Co-funded by the European Union
MINISTRY OF EDUCATION, YOUTH AND SPORTS
CHARLES UNIVERSITY
MUNI LAW
VŠE PRAGUE

Structure

- Introduction
- AI/deepfake-based frauds
- Enhanced frauds
- New types of frauds
- Fraud taxonomy
- Conclusion

2

CENTER FOR INEQUALITY AND OPEN SOCIETY

Introduction

- Rapid deployment of AI in financial services
- Rise of AI-enabled and deepfake-assisted fraud
- Shift from traditional fraud to technologically augmented schemes
- High relevance for law, regulation, and supervision

3

CENTER FOR INEQUALITY AND OPEN SOCIETY

State-of-art frauds

- Involvement of modern technologies
  - AI, deepfake, synthetic identity
  - New oportunities and attack surfaces
- Sophisticated types of frauds
- Unprecedented scale
- Accessibility and affordability
- Elevating the threat level
- 780% increase in Europe in 2023

4

CENTER FOR INEQUALITY AND OPEN SOCIETY

State-of-art frauds

- Why financial institutions
  - Relies also on remote work and outsourcing
  - Lucrative attack vector due to the amount of sensitive data and automation of tasks
- 2 types
  - **Enhanced** versions of traditional frauds
  - **New** types of frauds (e.g. synthetic identities)
- Methods – voice cloning, face swaping, documentation forgery

5

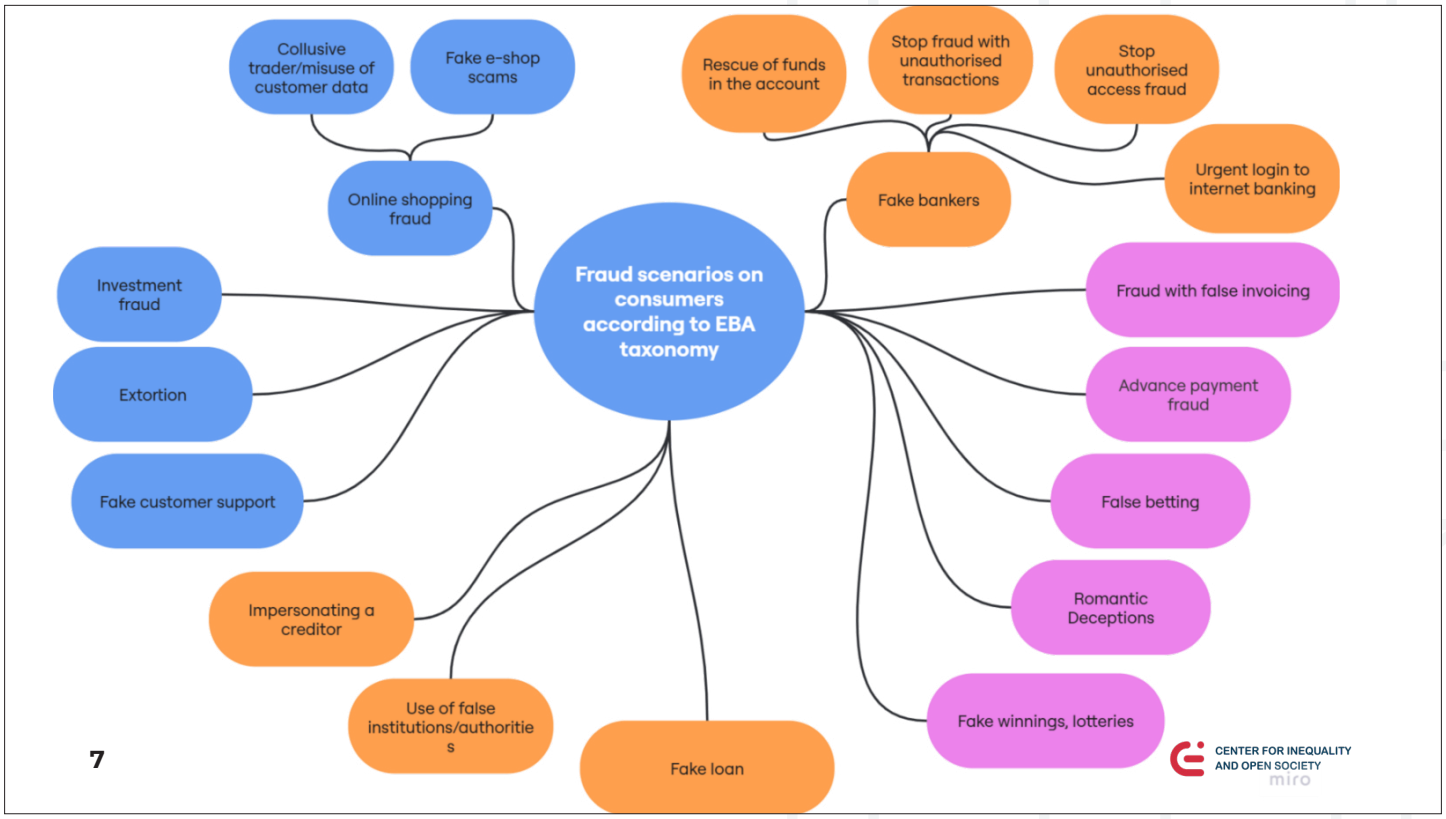
CENTER FOR INEQUALITY AND OPEN SOCIETY

Enhanced frauds

- Traditional types of frauds enhanced by AI or deepfake
- Leads to elevated level of sophistication and potential impacts
- Typically – impersonating authorities, relatives, investment frauds, fake websites/QR codes/apps, social engineering, etc.

6

CENTER FOR INEQUALITY AND OPEN SOCIETY



7

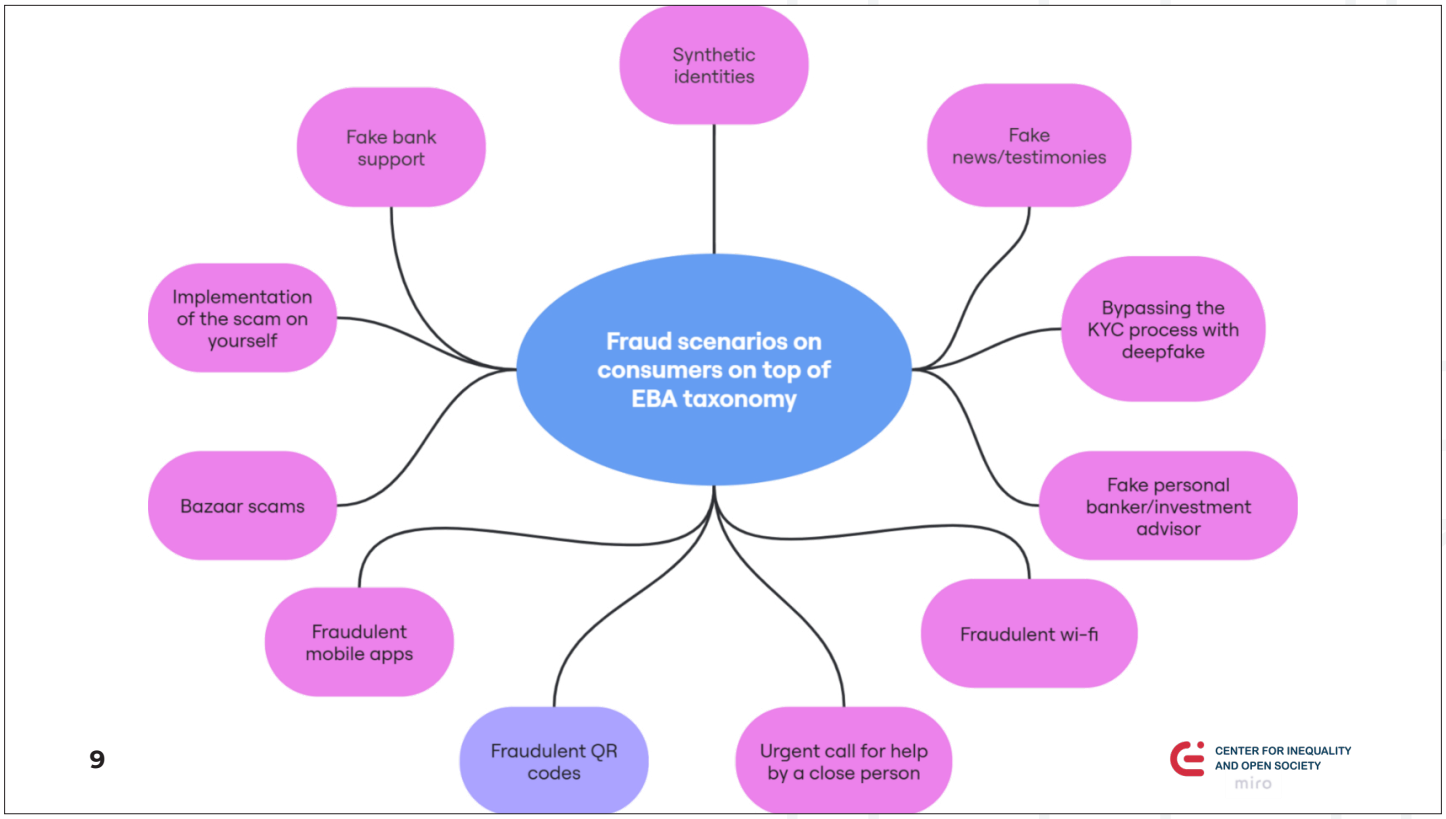
CENTER FOR INEQUALITY AND OPEN SOCIETY

New forms of frauds

- Voice cloning
- Face swapping and real-time deepfakes
- Synthetic identity generation
- AI-driven social engineering
- Biometric spoofing and bypass techniques

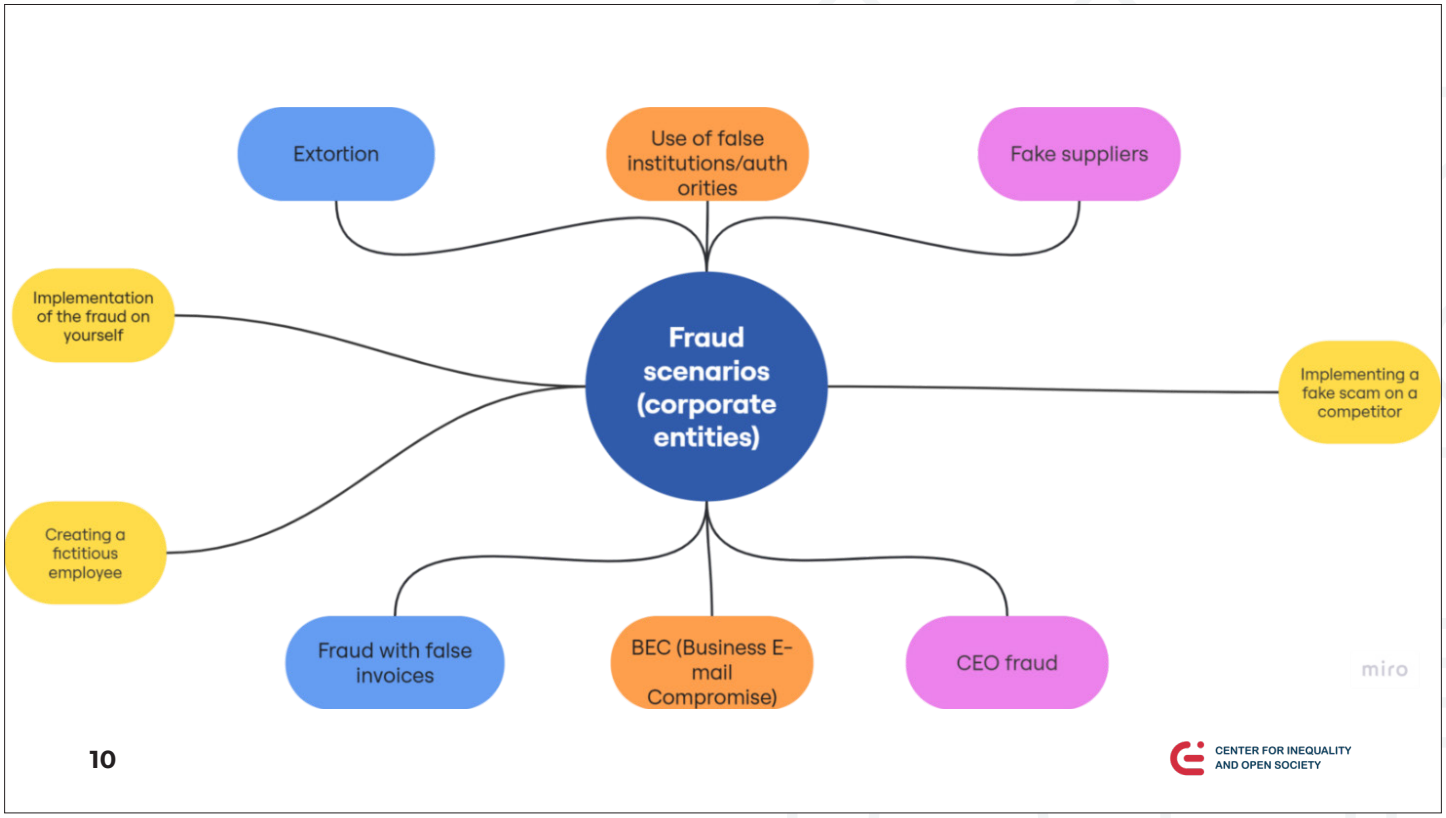
8

CENTER FOR INEQUALITY AND OPEN SOCIETY



9

CENTER FOR INEQUALITY AND OPEN SOCIETY
miro



Most relevant categories of AI frauds

- AI-Enhanced Impersonation Fraud
  - Voice cloning
  - Face swaping
  - CEO, CFO, bank staff, relatives, employees
  - => customer authentication, transaction approval

11

CENTER FOR INEQUALITY AND OPEN SOCIETY

12

CENTER FOR INEQUALITY AND OPEN SOCIETY

Most relevant categories of AI frauds

- Synthetic Identity and Hybrid Identity Fraud
  - Real + synthetic data
  - Cultivation of „legitimate“ baking profiles
  - Increased difficulty of detection
  - => KYC processes, onboarding, credit and account creation

13

CENTER FOR INEQUALITY AND OPEN SOCIETY

Most relevant categories of AI frauds

- Biometric Authentication Circumvention
  - Spoofing facial recognition
  - Replay and synthesis attacks on voice biometrics
  - AI-assisted liveness detection bypass
  - => Strong customer authentication (SCA), Mobile banking access
  - Biometrics shift from a solution to a vulnerability.

14

CENTER FOR INEQUALITY AND OPEN SOCIETY

Most relevant categories of AI frauds

- All types of phishing
  - Voice, e-mail, QR codes, etc.
  - Personalized forms
  - Very convincing
  - strange at first glance no more

15

CENTER FOR INEQUALITY AND OPEN SOCIETY

Existing taxonomy

- Baseline taxonomy of frauds – EBA taxonomy
- Primary purpose – supervisory reporting and statistics, risk monitoring
- One of the most complex fraud taxonomies
- Doesn‘t reflect the state-of-art technologies

16

CENTER FOR INEQUALITY AND OPEN SOCIETY

Limits of the EBA taxonomy

- Doesn‘t explicitly mention state-of-art technologies
- Same EBA category can now cover only traditional frauds
- Taxonomy captures what happened, not how it was technically enabled
- Limited ability to: distinguish automation, reflect scalability, capture biometric spoofing dynamics

17

CENTER FOR INEQUALITY AND OPEN SOCIETY

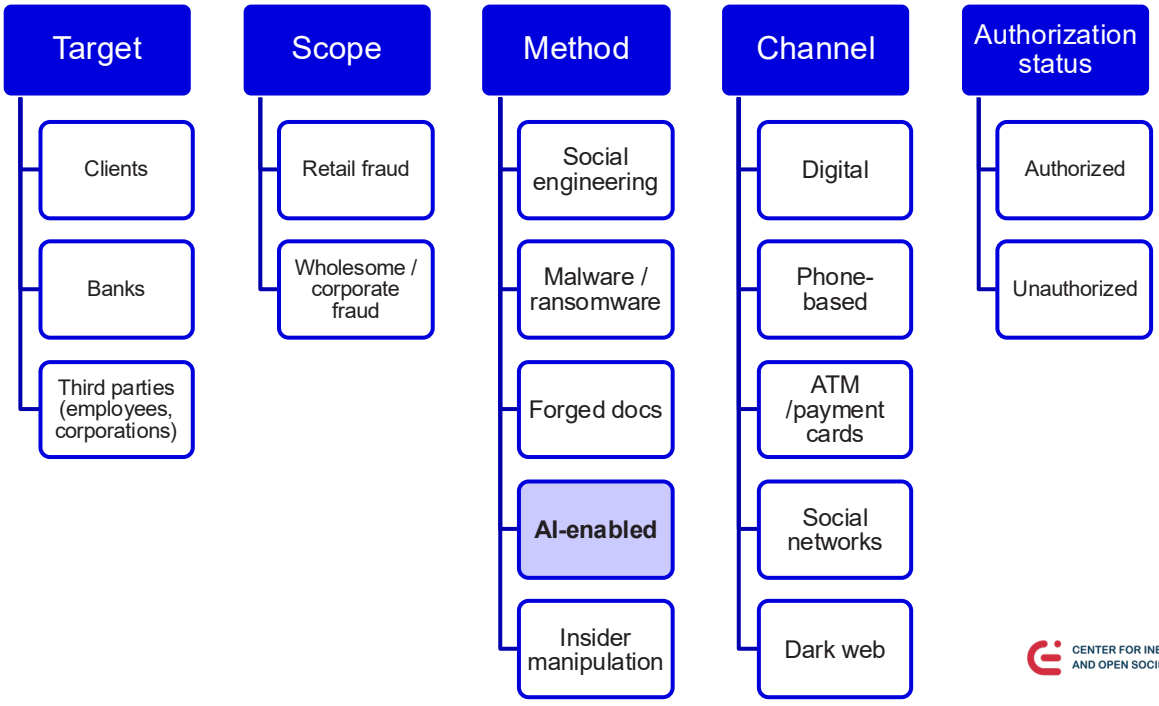
Taxonomy recommendation

- Regulatory taxonomies (EBA) classify outcomes
- AI-enabled fraud requires attention to
  - technical enablers
  - execution dynamics
- Empirical cases reveal patterns invisible in statistical reporting

18

CENTER FOR INEQUALITY AND OPEN SOCIETY

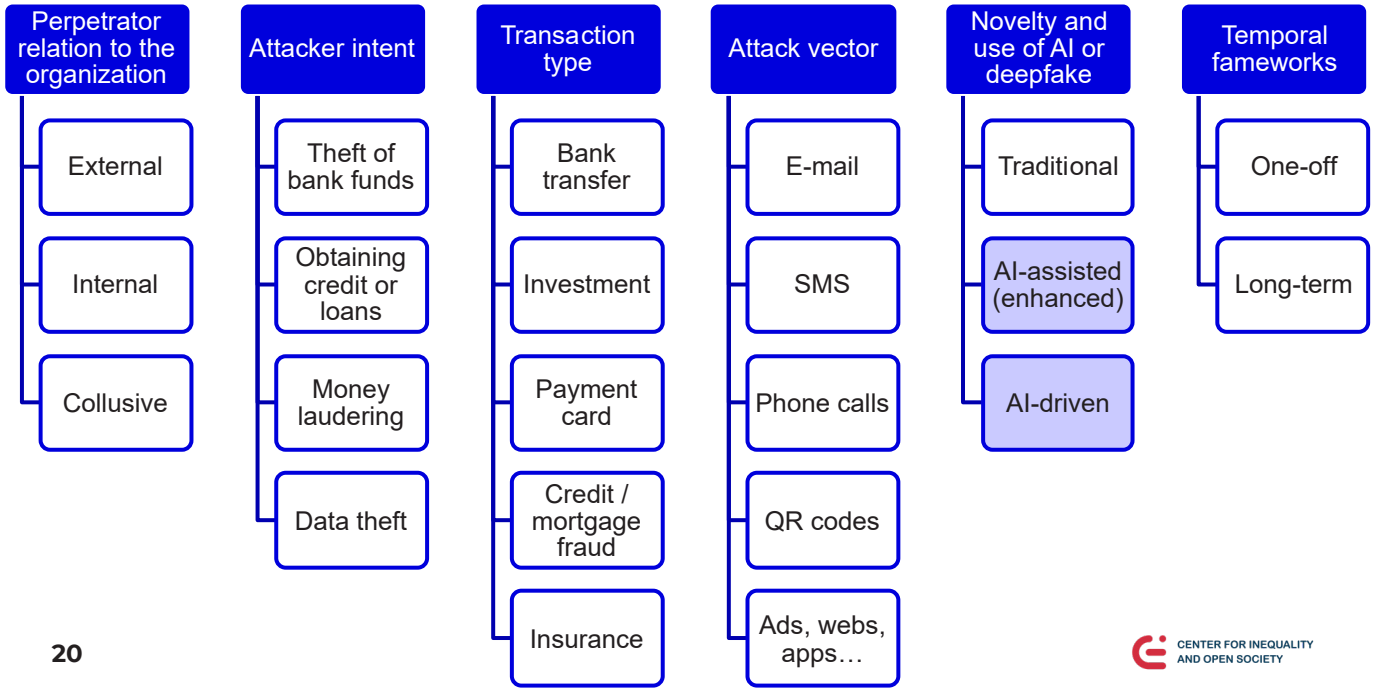
Possible categorization



19

CENTER FOR INEQUALITY AND OPEN SOCIETY

Possible categorization



20

CENTER FOR INEQUALITY AND OPEN SOCIETY

Conclusion

- AI and deepfake-enabled frauds differ qualitatively from traditional banking fraud
- Existing taxonomies capture outcomes, but not technological enablers
- A technology-oriented, multi-dimensional classification helps reveal new risk patterns
- AI-enabled frauds cut across victims, channels, authorization models, and instruments

21

CENTER FOR INEQUALITY AND OPEN SOCIETY

Thank you for your attention!

Kristyna.Mlcakova@law.muni.cz

22

CENTER FOR INEQUALITY AND OPEN SOCIETY

CENTER FOR INEQUALITY AND OPEN SOCIETY

cios@law.muni.cz

23

CENTER FOR INEQUALITY AND OPEN SOCIETY

Limits to Using AI to Evaluate Credit Risk in Light of the Provisions of the AI Act

János Székely
Associate Professor, Sapientia EMTE, Law Faculty, Cluj Napoca/Kolozsvár

Limits to Using AI to Evaluate Credit Risk in Light of the Provisions of the AI Act

SAPIENTIA
HUNGARIAN UNIVERSITY OF TRANSYLVANIA
Faculty of Sciences and Arts
Cluj-Napoca

János Székely PhD,
senior university lecturer

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Outline of the Presentation

1. Introductory Remarks. *Sedes Materiae*

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 – AI Act – is applicable (Article 113): from 2 August 2026; Chapters I and II from 2 February 2025; Chapter III Section 4, Chapter V, Chapter VII and Chapter XII and Article 78 from 2 August 2025 (except Art. 101); Art. 6(1) from 2 August 2027.
- Scope is extraterritorial: Article 2(1): inter alia '(a) providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union (...) (c) providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union (...).'
- Article 6 provides for the classification of AI systems, with Art. 6(1) containing the general conditions for high-risk AI, and Art. 6(2) lists AI applications that are high-risk by definition, when referring to Annex III; Art. 6(3) provides derogations from Art. 6(2).

2.1. The AI Act on Credit Scoring and Creditworthiness

- Recital (52): '(...) in addition, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for those purposes may lead to discrimination between persons or groups and may perpetuate historical patterns of discrimination, such as that based on racial or ethnic origins, gender, disabilities, age or sexual orientation, or may create new forms of discriminatory impacts. However, AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under this Regulation.'
- Recital (158): 'as regards AI systems provided or used by regulated and supervised financial institutions unless Member States decide to designate another authority to fulfil these market surveillance tasks. Those competent authorities should have all powers under this Regulation and Regulation (EU) 2019/1020 to enforce the requirements and obligations of this Regulation, including powers to carry our ex post market surveillance activities that can be integrated, as appropriate, into their existing supervisory mechanisms and procedures under the relevant Union financial services law. (...)'

2.2. The AI Act on Credit Scoring and Creditworthiness

- Regulation (EU) 2024/1689 Annex III para. (5)(b): 'High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas: (...) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud'.

3. The Natural Person—Legal Person Gap

	Natural person	Legal person
Credit Scoring	High-risk AI	Non-high-risk AI
Creditworthiness	High-risk AI	Non-high-risk AI
Fraud detection	Non-high-risk AI	Non-high-risk AI

Prima faciae problems with the risk-based approach in this solution:

- Recital (52) hints only at access to essential services (housing, electricity, telecommunication) and non-discrimination (a human right under Art. 14 of the ECHR).
- In the view of the EU regulator, such risks exist for natural persons, but not legal entities (which is a narrow view in light of ECtHR case-law in Granos Organicos Nacionales S.A. v. Germany, No. 19508/07 para. 45 – if reasonabile and proportional; Art. 34 'groups of indifviduals'). Also, Recital (2) of the Regulation states the aim of protecting undertakings, as well as legal persons.
- In what way does fraud-detection differ from establishing creditworthiness (supposing that fraudsters are less than creditworthy).

4.1. What Does the High-Risk AI Classification Entail?

- Recital (53): '(...) In any case, AI systems used in high-risk use-cases listed in an annex to this Regulation should be considered to pose significant risks of harm to the health, safety or fundamental rights if the AI system implies profiling within the meaning of Article 4, point (4) of Regulation (EU) 2016/679 or Article 3, point (4) of Directive (EU) 2016/680 or Article 3, point (5) of Regulation (EU) 2018/1725. (...)'
- Art. 6(2) of the Regulation result in all Annex III systems being high-risk.

4.2. What Does the High-Risk AI Classification Entail?

- Regulation (EU) 2024/1689 Art. 6(3): 'By derogation from paragraph 2, an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making.' Inter alia, when: '(b) the AI system is intended to improve the result of a previously completed human activity; (...) Notwithstanding the first subparagraph, an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons.'

4.3. What Does the High-Risk AI Classification Entail?

Requirements for the system (Chapter III, Section 2 of the Regulation) (*inter alia*)	Requirements for the providers and deployers (Chapter III, Section 2 of the Regulation) (*inter alia*)
Instituting a risk management system	Obligations under Section 2
Instituting strict data governance policies	+ Instituting a quality management system
Creating and maintaining the technical documentation	+ Preservation of records
Ensuring proper record keeping	+ Taking any corrective actions expediently
Ensuring transparency towards deployers and end-users	+ Cooperating with authorities
Ensuring human oversight	+ Designation of authorised representatives
Ensuring accuracy, robustness and cybersecurity	

5. Practical Hurdles to Compliance with the Regulation

- Opacity of AI models;
- Alogorhithmic bias

TECHNOLOGIA EX MACHINA: BLOCKCHAIN

"Just Sign Here" – the Challenge of Trust for Smart Contracts on Blockchain

Simon Thompson
Professor Emeritus, University of Kent

"Just Sign Here ... "

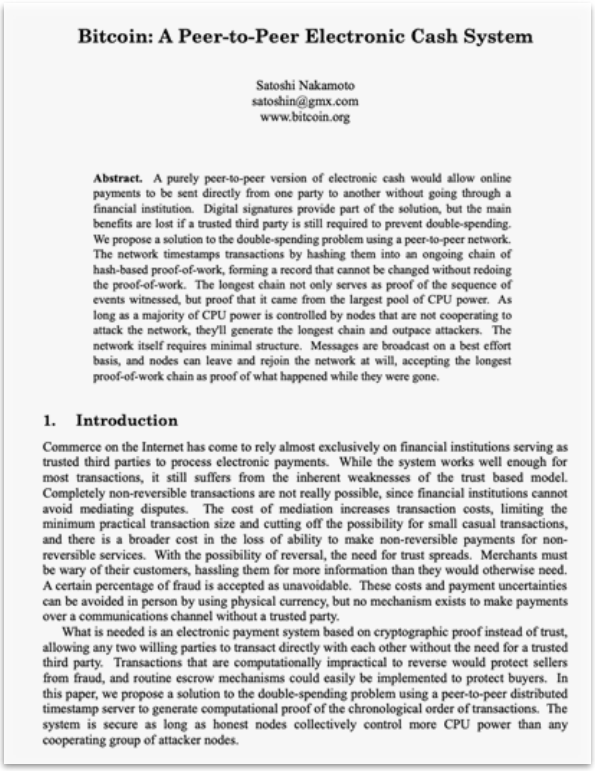
The challenge of trust for smart contracts on blockchain

Simon Thompson, University of Kent, UK and ELTE

The Bitcoin whitepaper, 2008

*"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as **trusted third parties** to process electronic payments.*

*What is needed is an electronic payment system **based on cryptographic proof instead of trust**, allowing any two willing parties to transact directly with each other without the need for a trusted third party."*



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

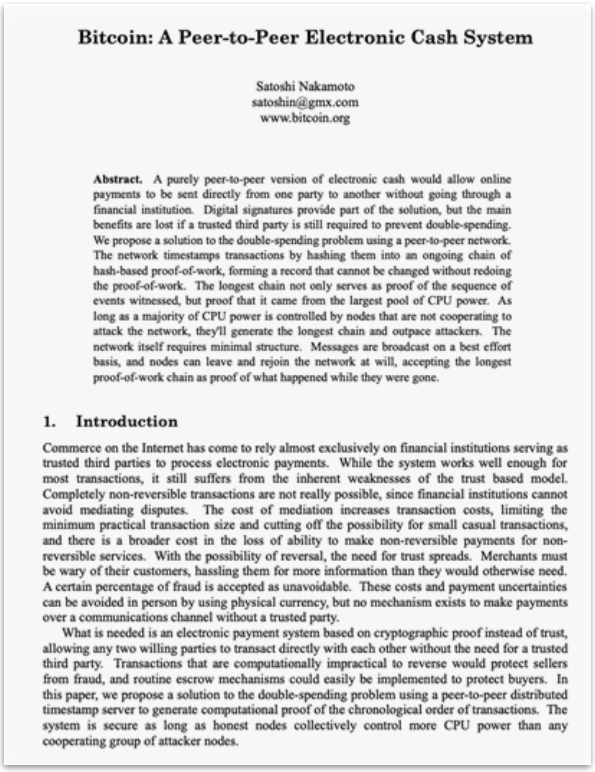
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

"In this paper, we propose a solution to the ... problem using a peer-to-peer distributed [system]"



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

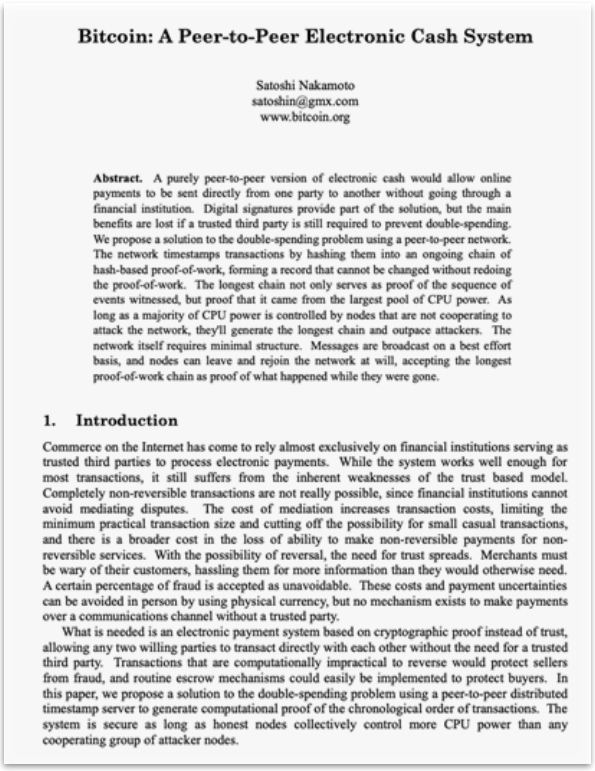
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

“ ... routine escrow mechanisms could easily be implemented to protect buyers ... ”



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

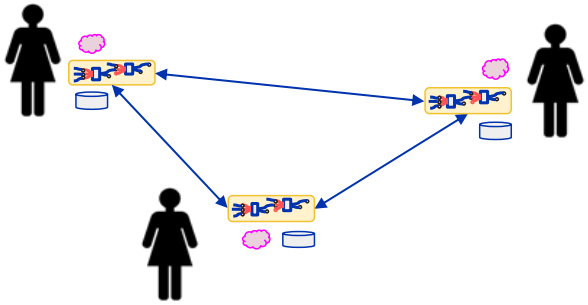
Decentralised applications on blockchain

Blockchain

A blockchain is a Distributed Ledger

... supporting digital assets such as

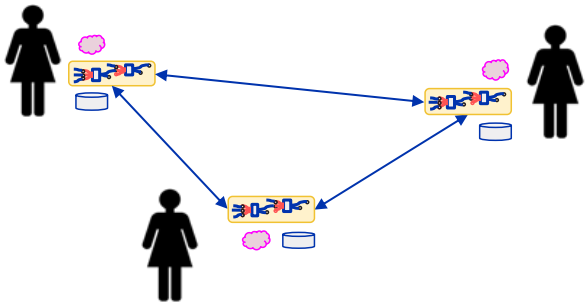
... Bitcoin, Ethereum and Cardano.



Decentralised Applications (DApps) on Blockchain

A DApp is an application running on top of a blockchain ...

... where the key part that manipulates digital assets is an on-chain ***smart contract*** or program.



Blockchain in practice

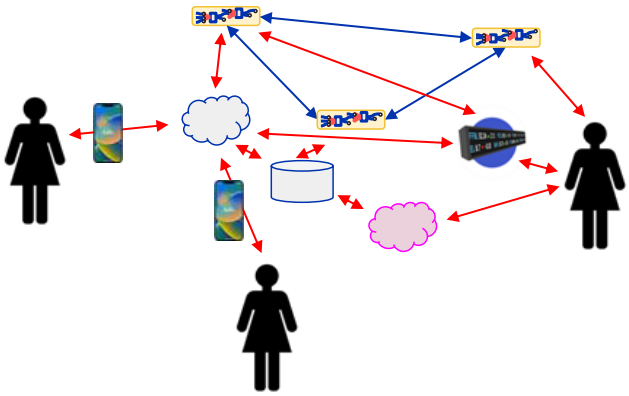
More complicated than the original Bitcoin vision:

... services

... "light clients"

... oracles,

all interacting with smart contracts i.e. programs running on blockchain.



Two questions

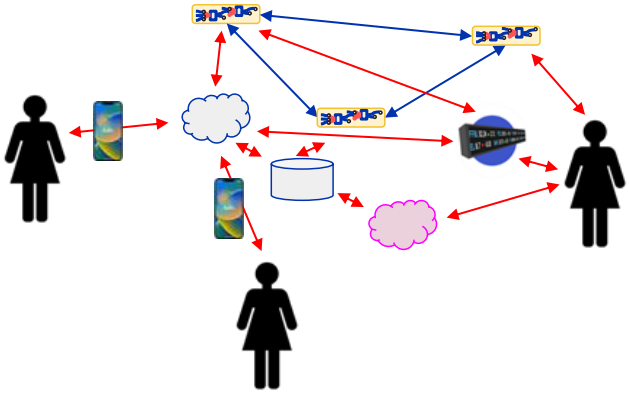
The return of trust – two questions

Identity

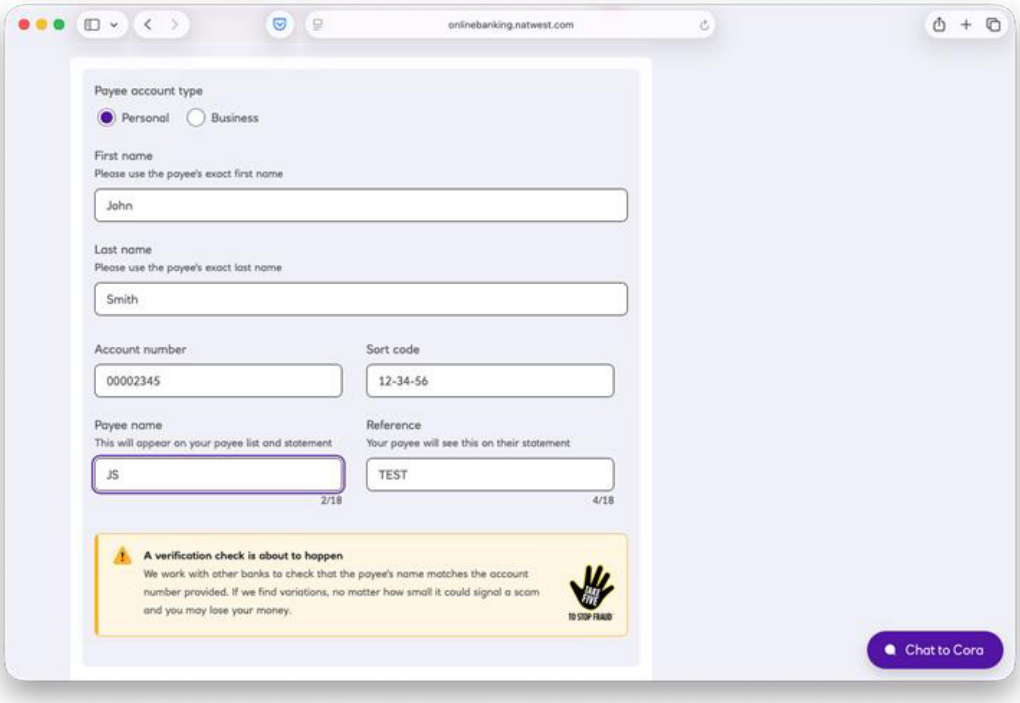
Who am I talking to?

Verification

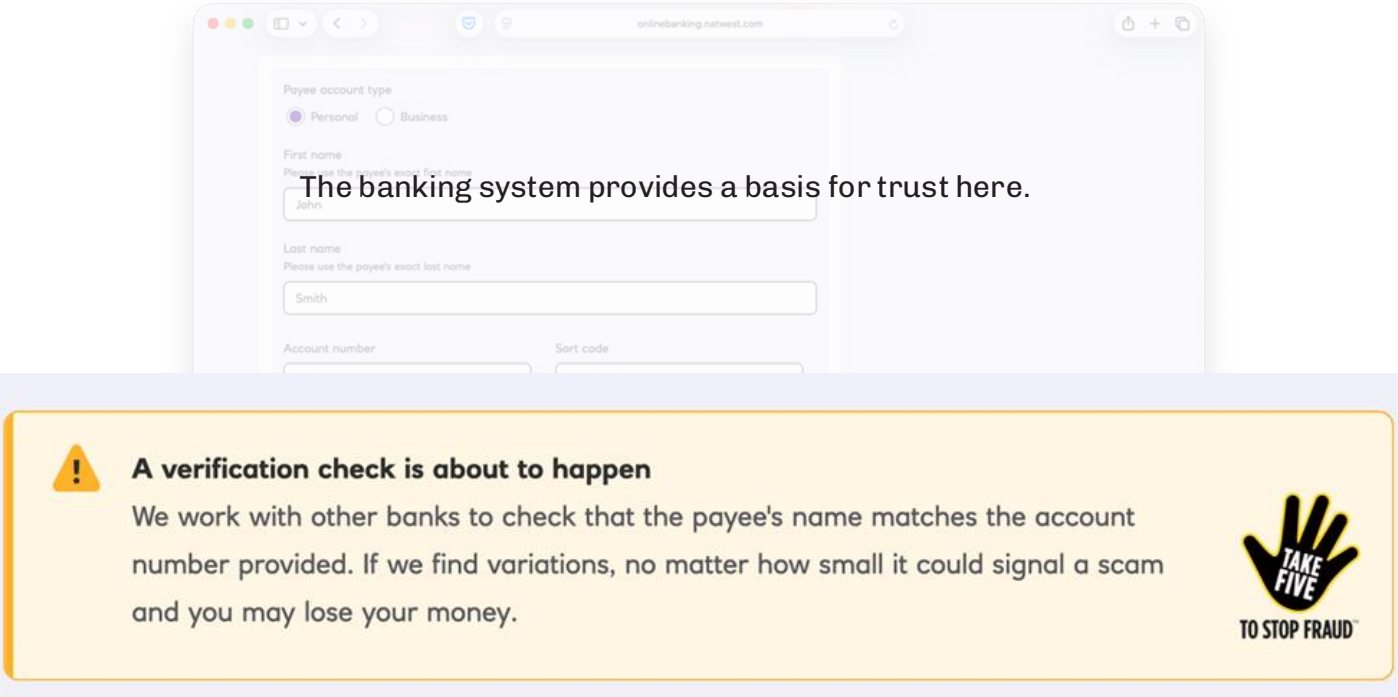
What am I interacting with?

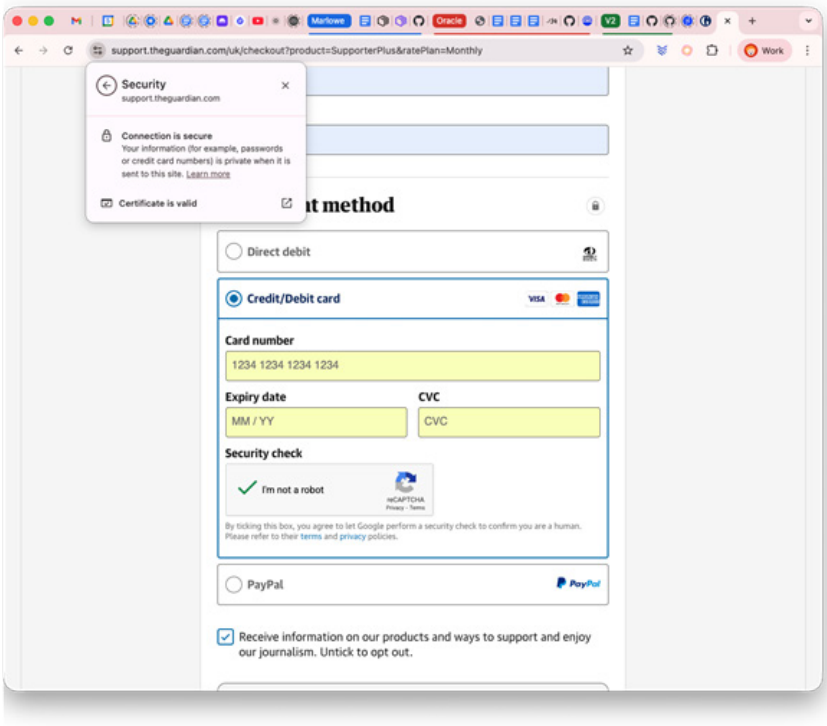


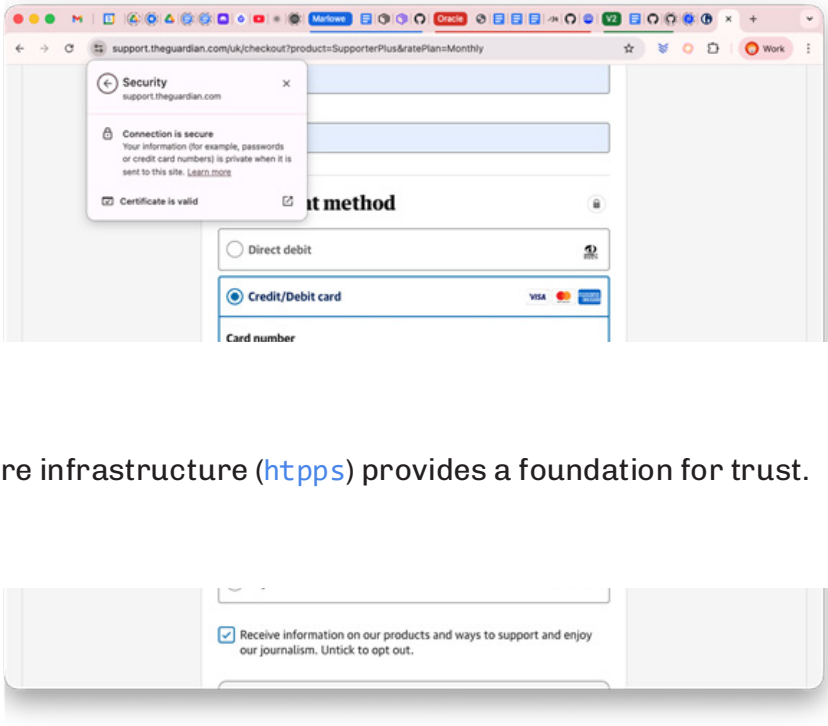
Identity



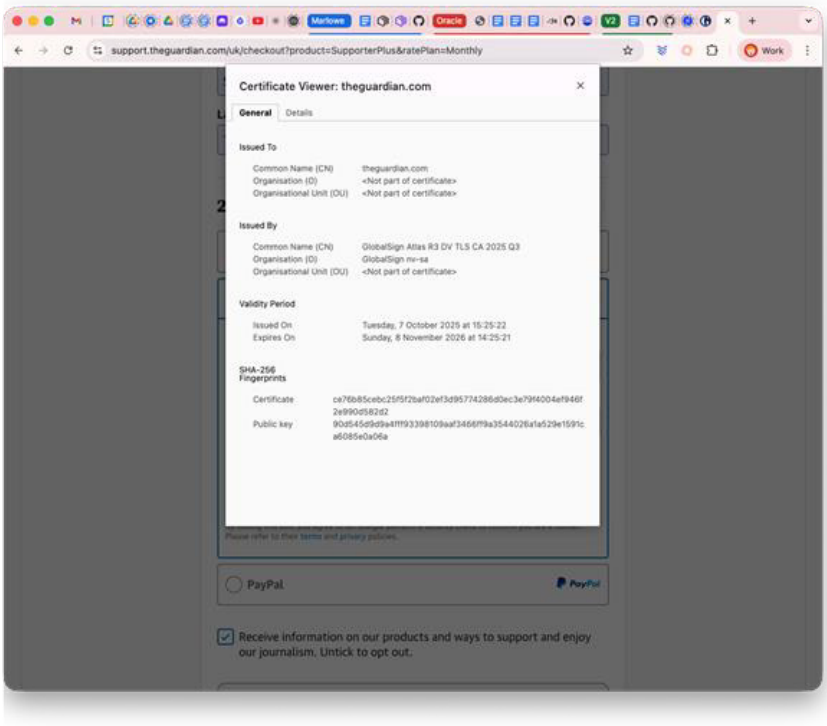
The banking system provides a basis for trust here.

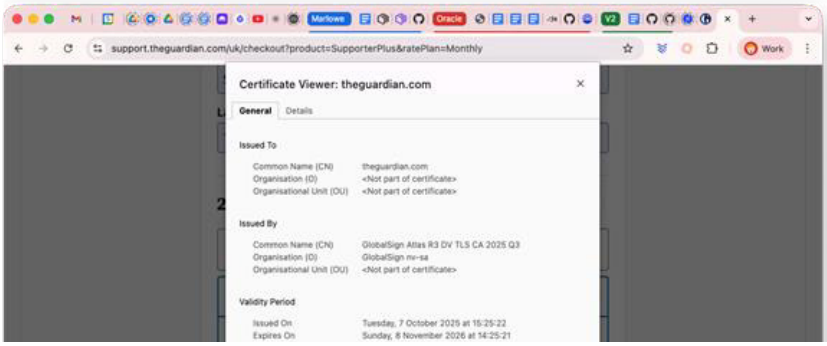




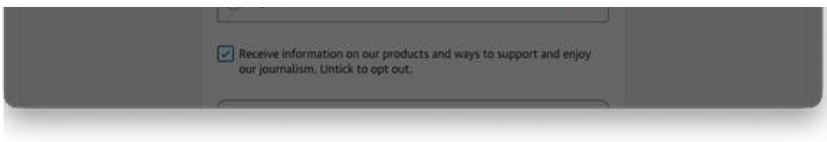


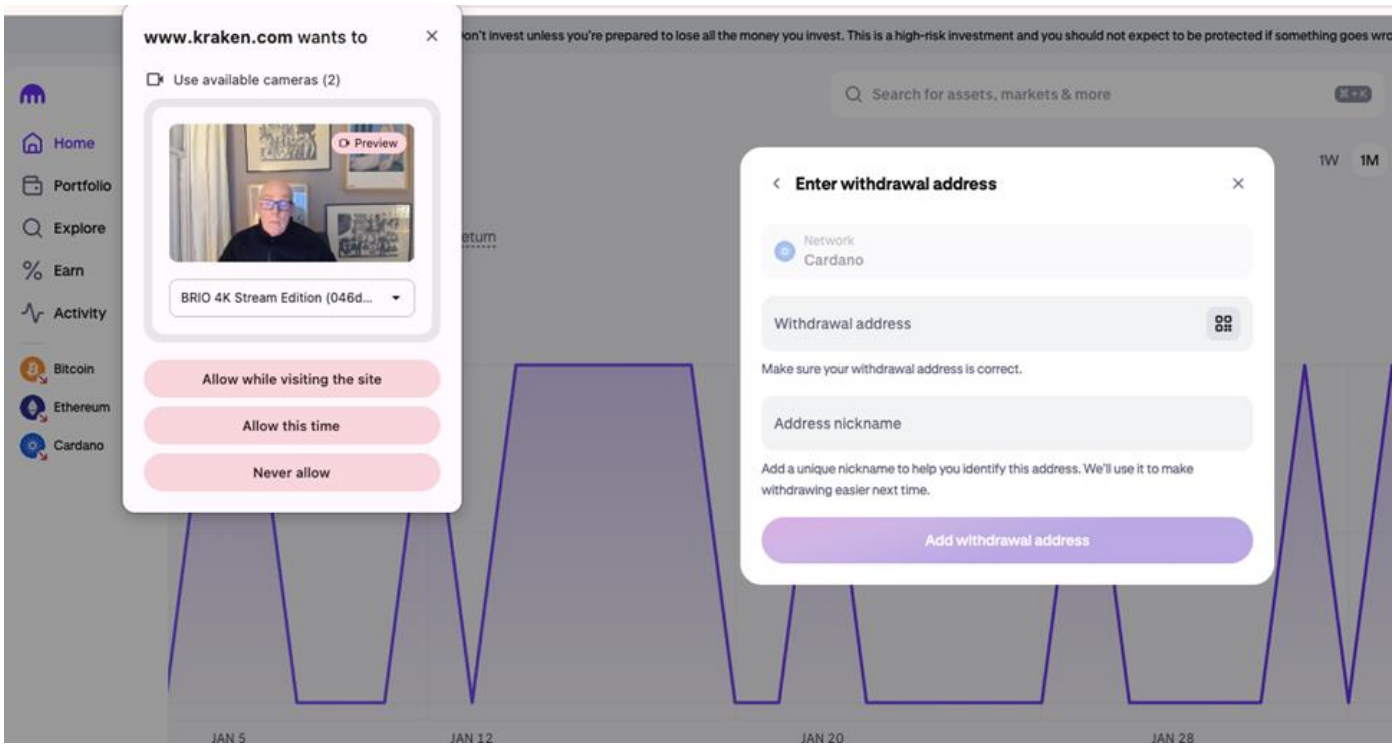
Secure infrastructure (`htpps`) provides a foundation for trust.

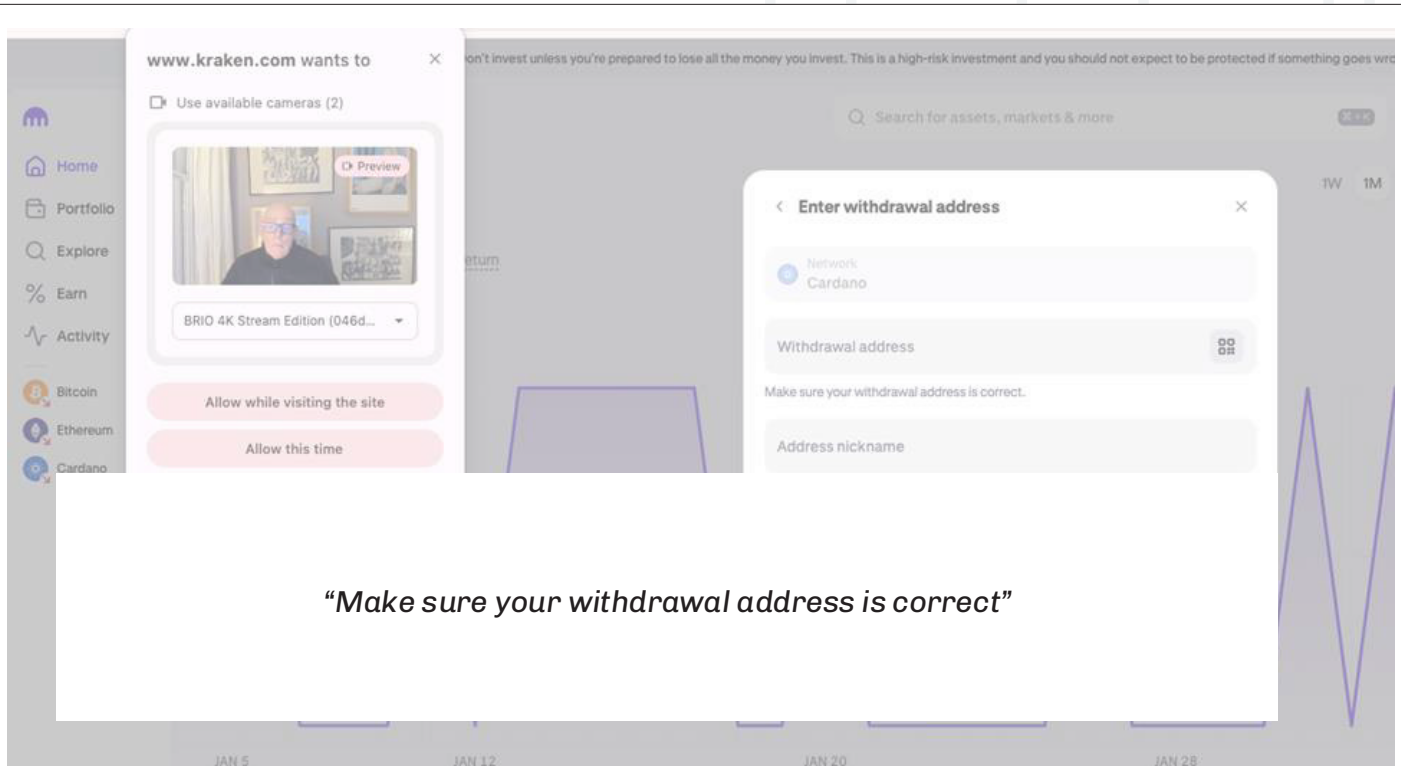




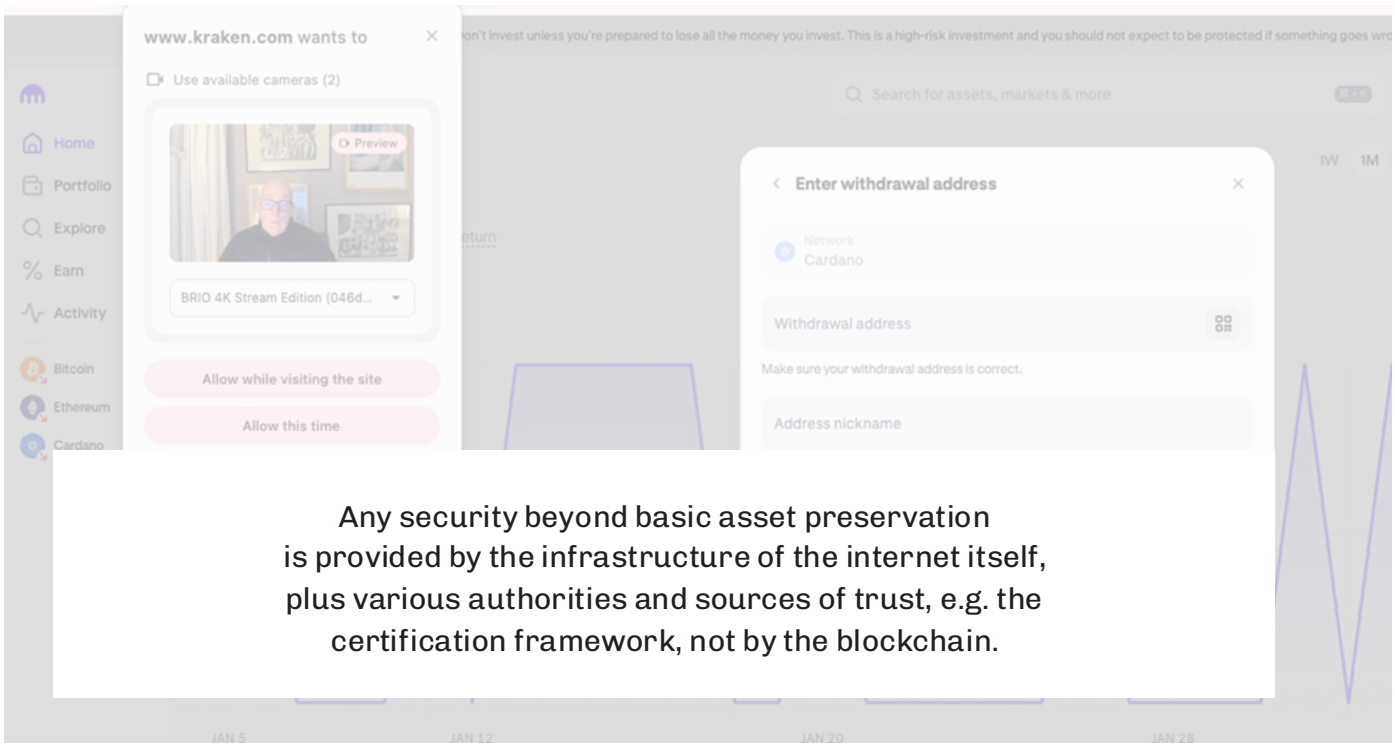
Certification provides a trust framework for internet domains.



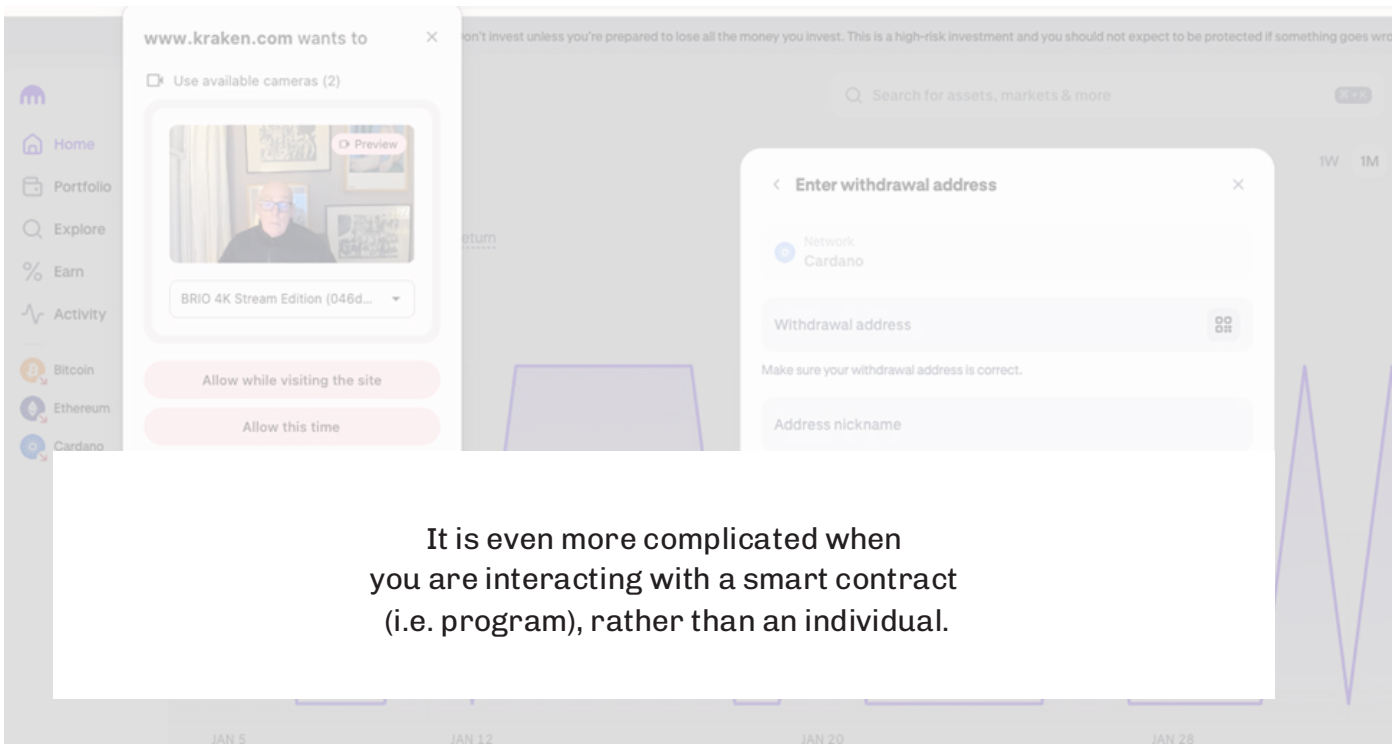




"Make sure your withdrawal address is correct"

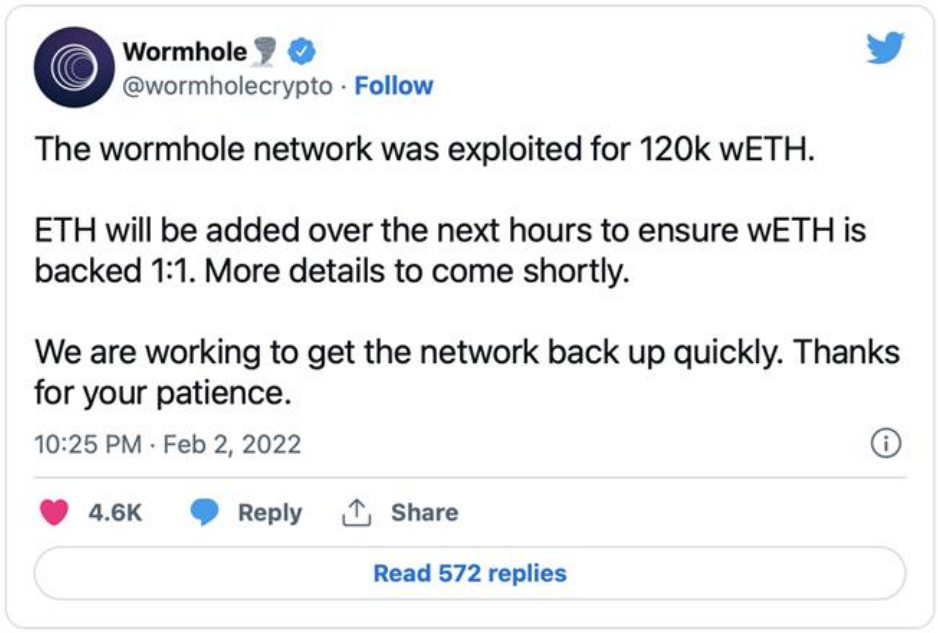


Any security beyond basic asset preservation is provided by the infrastructure of the internet itself, plus various authorities and sources of trust, e.g. the certification framework, not by the blockchain.



It is even more complicated when you are interacting with a smart contract (i.e. program), rather than an individual.

Problem #2: what does this do?


Wormhole
@wormholecrypto · Follow
The wormhole network was exploited for 120k wETH.
ETH will be added over the next hours to ensure wETH is backed 1:1. More details to come shortly.
We are working to get the network back up quickly. Thanks for your patience.
10:25 PM · Feb 2, 2022
4.6K
Reply
Share
Read 572 replies

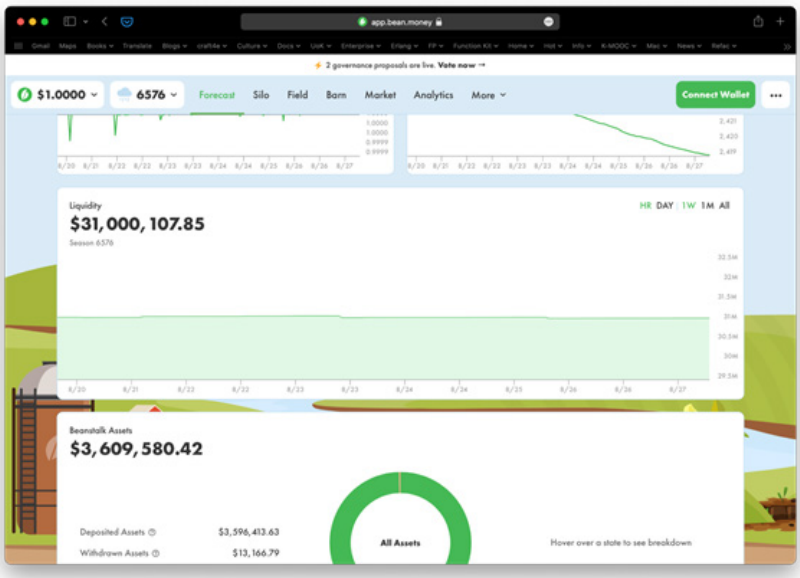

Algo Stablecoin Protocol Beanstalk Relaunches Following $180M Hack
Beanstalk is hoping its revamped launch will help buoy issues pertaining to its security and trust following a major hack in April.
SOURCE: SHUTTERSTOCK AND BEANSTALK

Top exploits in 2022

Exploit	Date	Value (USD)	Blockchain
Ronin network	March 2022	$620M	Ethereum
Wormhole	Feb 2022	$326M	Solana
Beanstalk	April 2022	$182M	Ethereum
Harmony Protocol	June 2022	$98M	Harmony/Ethereum
Rari Capital	May 2022	$80M	Ethereum

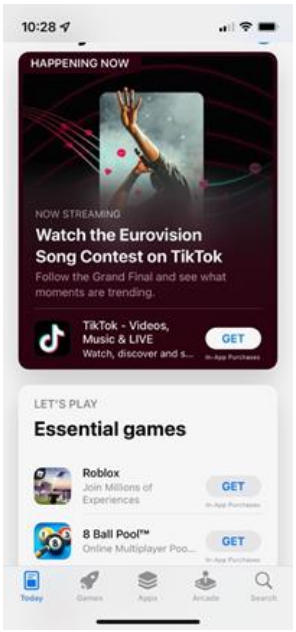
The challenge: assurance

Where is the difficulty?



What a DApp is not

It is *not* code that you download and run.



It's not a web page or a download

Program code ...

... "on-chain" and "off-chain"

... distributed

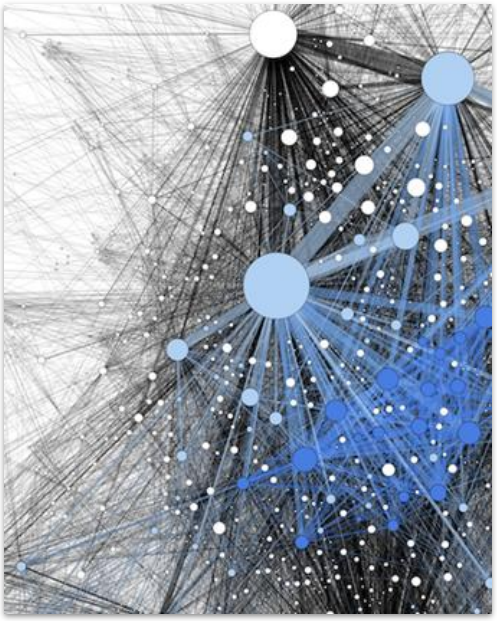
... decentralized

... consensus

... externalities

... crypto-economics

... socially-engineered structure.

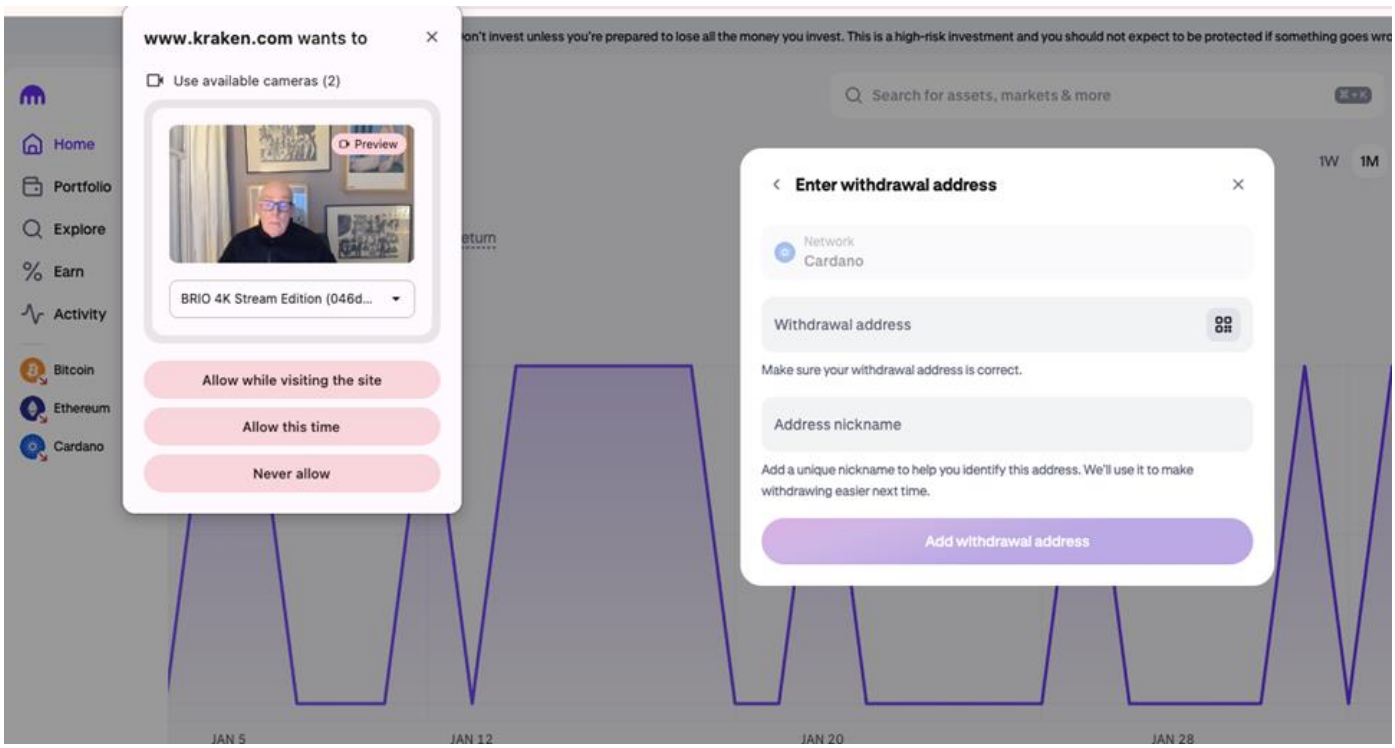


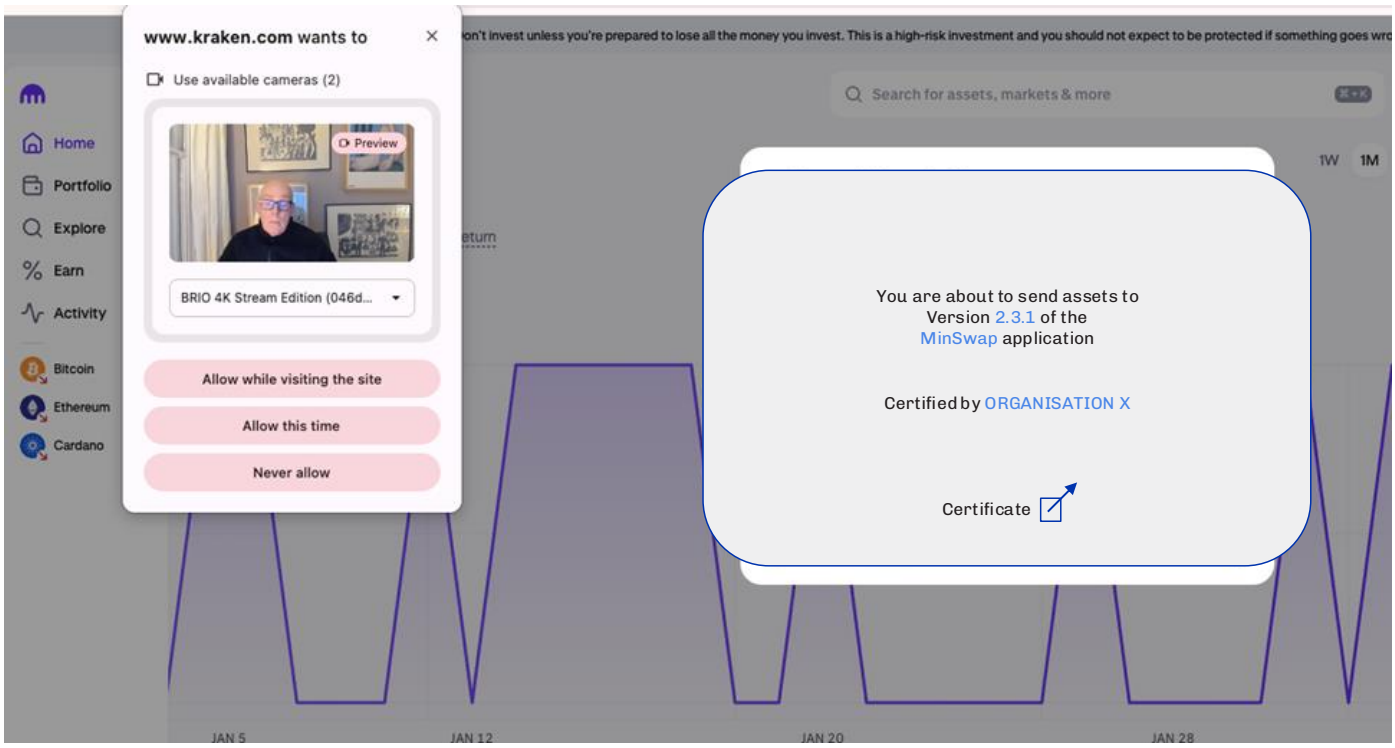
The challenge: provide assurance for DApp users

We need a DApp to perform as needed ...

... and to be secure against accidental errors and malicious attacks.

Multiple scopes: on- and off-chain code, complete DApp, wallets, services, and the social and economic context.





Standards are emerging

Enterprise Ethereum Alliance EthTrust Certification

*"This document defines the requirements for EEA EthTrust Certification, a set of certifications that a smart contract has been reviewed and **found not to have a defined set of security vulnerabilities**."*

https://entethalliance.org/specs/ethtrust-sl/

Version 3, March 2025.

Enterprise Ethereum Alliance EthTrust Certification

*"This document defines the requirements for EEA EthTrust Certification, a set of certifications that a smart contract has been reviewed and **found not to have a defined set of security vulnerabilities**."*

https://entethalliance.org/specs/ethtrust-sl/

Version 3, March 2025.

Examples include:

- Flaws in programming language itself
- Manipulating values from "oracles"
- Blockchain weaknesses: front-running etc.

Audit in practice

Feedback from smart contract auditors

“We always find something … we still haven't had a completely clean review”

Close correlation between the client team ethos and code quality

Crucial role of software tools

Feedback from smart contract auditors

"We always find something ... we still haven't had a completely clean review"

Close correlation between the client team ethos and code quality

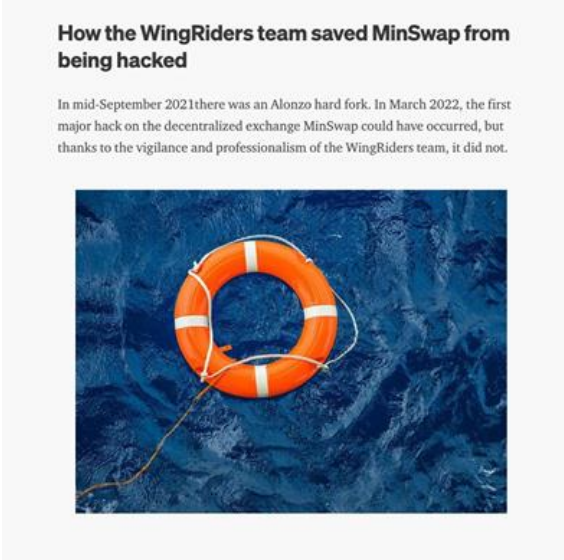
Crucial role of software tools

Need to pay particular attention to minting and burning of tokens

Potential disconnects between teams building on- and off-chain code

Optimisation is prevalent, but can introduce vulnerabilities

The community to the rescue


How the WingRiders team saved MinSwap from being hacked

In mid-September 2021there was an Alonzo hard fork. In March 2022, the first major hack on the decentralized exchange MinSwap could have occurred, but thanks to the vigilance and professionalism of the WingRiders team, it did not.

> *That's how the MinSwap bug was found! Their code was open source, it was not because of an Audit.*
>
> - Abhidoop

In conclusion

Conclusions

The libertarian principles that underlie blockchains do not render irrelevant the traditional issues of identity and trust.

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Conclusions

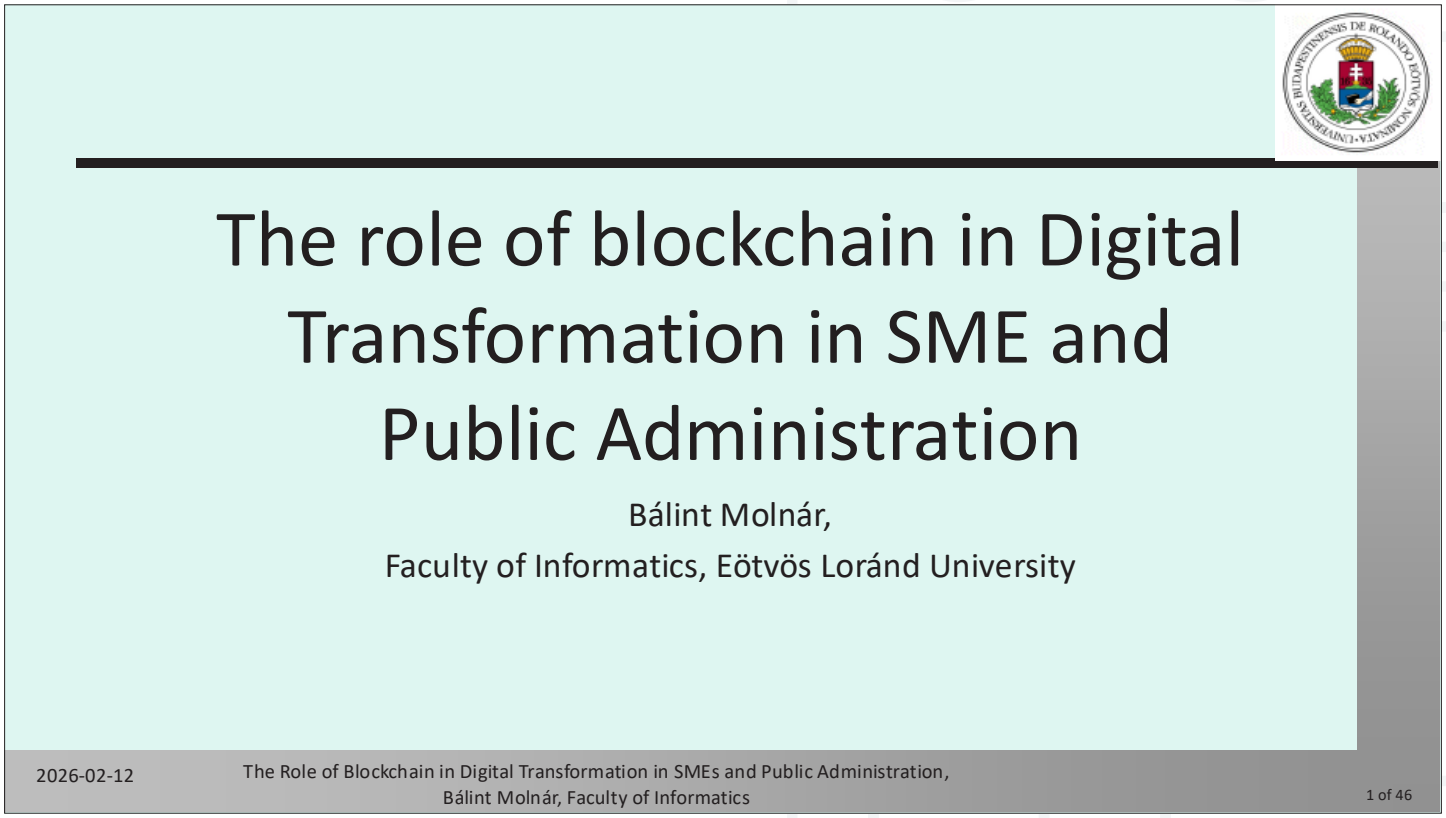
The libertarian principles that underlie blockchains do not render irrelevant the traditional issues of identity and trust.

In a fast-moving, technically challenging field, software solutions “play catch up”, and legal approaches lag further behind.

Questions?

The role of blockchain in Digital Transformation in SME and Public Administration

Bálint Molnár
Professor ELTE Faculty of Informatics



PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Digital Transformation & Blockchain

Blockchain is often discussed as a financial technology.

In reality, it is becoming a new institutional infrastructure for trust in digital economies.

The key question is not whether blockchain is legal or illegal, but where it creates real technological value for *SMEs* and *public administration* under existing legal constraints.

Digital transformation has solved many problems of efficiency, but not the fundamental problem of trust between organizations.

Blockchain introduces a new model: trust embedded in infrastructure rather than guaranteed solely by institutions.

This shift has profound implications for SMEs, public administration, and the legal frameworks that govern them.

Digital Transformation Context

Digital transformation drivers

- Automation and efficiency
- Trust and transparency
- Data-driven decision making
- Cross-organizational collaboration
- Secure digital services

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Digital Transformation Context

Challenges

- Fragmented systems
- Trust between actors
- Data integrity
- Compliance and regulation

Key question:

Can blockchain become a foundational trust infrastructure?

Why Blockchain Now?

Key enabling factors

- Distributed trust models
- Cryptographic security
- Smart contracts and automation
- Tokenization and digital assets
- Growing interoperability ecosystems

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Why Blockchain Now?

Strategic relevance

- Trusted data sharing
- Process automation
- Multi-stakeholder collaboration

Blockchain as Infrastructure for Trust

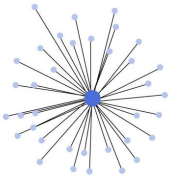
Blockchain enables **trust without central intermediaries**.

Core technological features

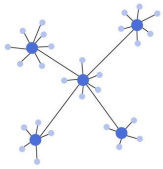
- Distributed ledger
- Immutability
- Consensus mechanisms
- Cryptographic verification
- Transparency with controlled access

Impact:
Reduction of reconciliation, verification, and dispute resolution costs.

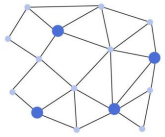
PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra



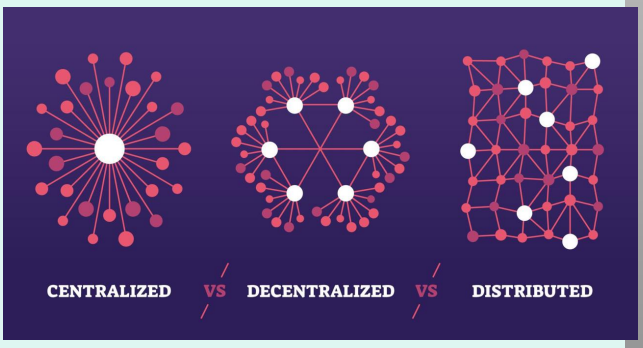
Centralized



Decentralized



Distributed



Types of Blockchain

- Public blockchain
- Private/permissioned blockchain
- Consortium blockchain

Most relevant for SMEs and public administration: consortium and permissioned

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Blockchain in SME Digital Transformation

Challenges:
- Limited resources
- Trust barriers
- Administrative burden

Blockchain offers:
- Trusted transactions
- Process automation
- Reduced overhead

SME Use Cases

- Supply chain traceability
- Smart contracts and automated payments
- Digital identity and credentials
- Tokenization and new financing models

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Italy – Blockchain for Supply Chain & SMEs

Sector: Made in Italy products

Use cases

- Fashion traceability
- Food supply chain
- Anti-counterfeiting

SME benefits

- Brand protection
- Trust certificationExport credibility
- Transparency for consumers

Supported by Italian Ministry of Economic Development.

Germany – Energy & SME Blockchain

Projects

- Energy trading platforms
- SME energy cooperatives
- Smart grid blockchain pilots

Benefits

- Automated billing
- Peer-to-peer energy trading
- Transparency
- SME participation in energy markets

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Benefits for SMEs

Operational:
- Lower transaction costs
- Faster settlements
- Reduced fraud

Strategic:
- Market access
- Increased credibility
- Innovation opportunities

Public Administration Transformation

Challenges:
- Fragmented databases
- Bureaucratic processes
- Limited interoperability

Opportunities:
- Trusted public records
- Transparency
- Automation

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Public Administration Use Cases

- Digital identity
- Land and company registries
- Public procurement transparency
- Secure document management

European Blockchain Services Infrastructure (EBSI)

Applications

- Digital diplomas
- Self-sovereign identity
- Trusted document exchange
- SME financing support

Impact

- Cross-border verification without intermediaries
- Increased administrative trust
- Reduced fraud
- EU digital single market integration

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Estonia – Blockchain in Public Administration

Technology: KSI Blockchain
Use since: ~2012

Applications

- Health records integrity
- Judicial system
- Government regisrtries
- National data infrastructure

Impact

- Tamper-proof government data
- High citizen trust
- Efficient digital state
- Reduced administrative overhead

Estonia is often cited as **global benchmark**.

Spain – Public Procurement Transparency

City-level pilots

Zaragoza

Catalonia

Blockchain use

- Tender tracking
- Contract transparency
- Anti-corruption tools

Impact

- Public trust
- Auditability
- Reduced manipulation risk

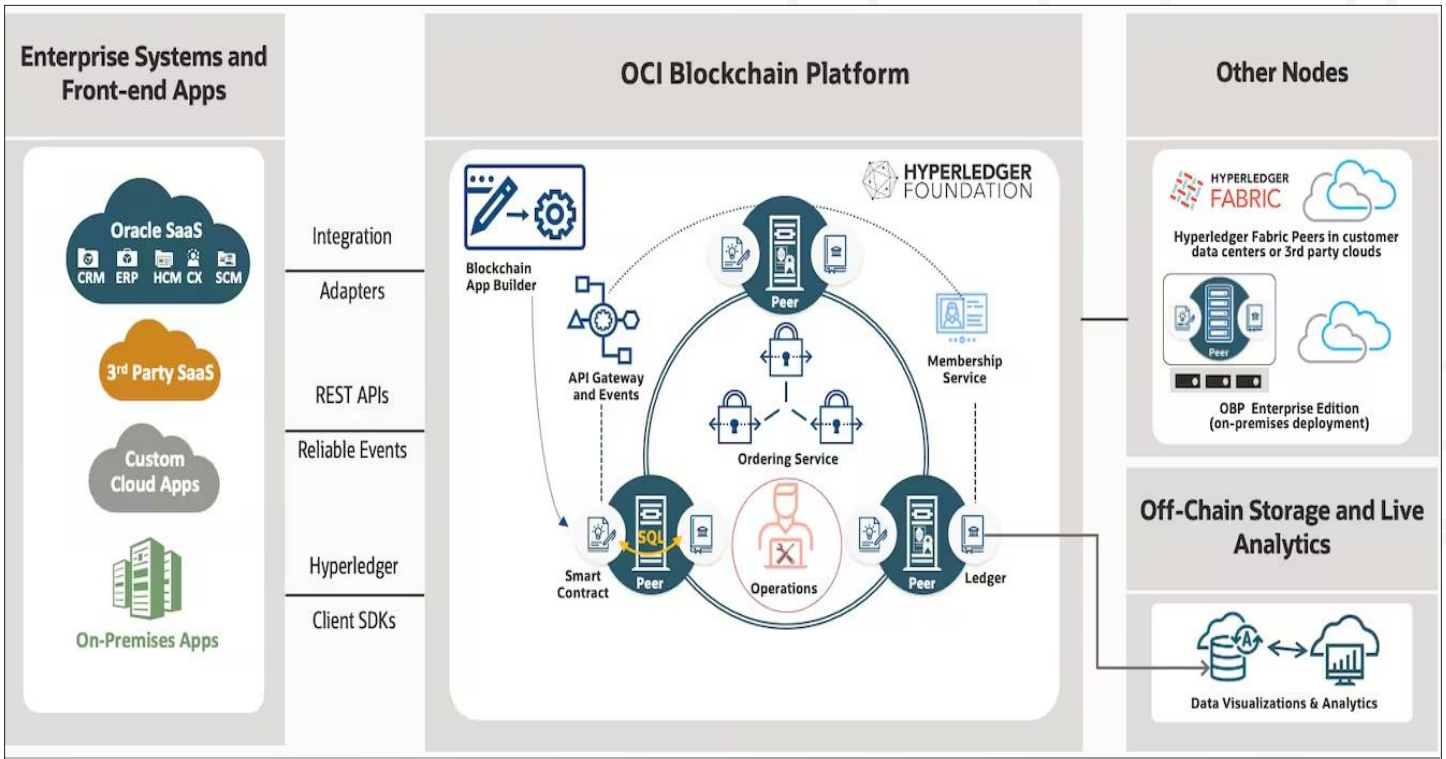
PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Interoperability & Integration

Blockchain integrates with:

- ERP systems
- Government platforms
- Legacy systems
- Cloud infrastructure

Blockchain as trust layer



PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Smart Contracts

Enable:

- Automated compliance checks
- Conditional payments
- Licensing and permits
- Grant distribution

Hotly debated notion in legal terms

Justinian Law:

The master cannot make a contract to deaf and mute servant (libertus)

Smart Contracts

A contract can be defined not by intention alone but by **valid participation in a formal execution protocol**.

Legal effect depends on successful execution of a predefined formal system.

A **human-executed smart contract**, enforced by formal language rules.

Blockchain smart contracts are: Machine-executed stipulations, enforced by code (program code).

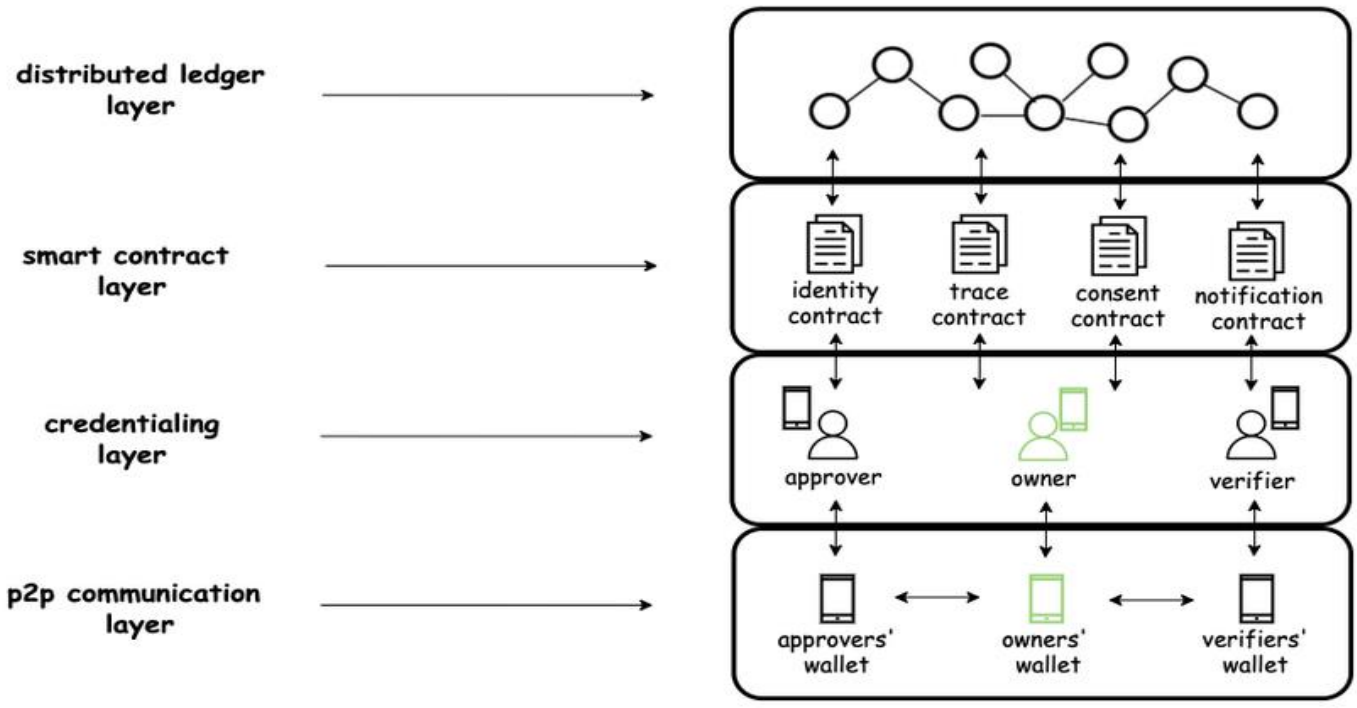
PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Technology Architecture

1. User applications
2. API layer
3. Blockchain layer
4. Off-chain storage
5. Identity & access management

Blockchain System Architecture (Hybrid Model)

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra



Data Management

On-chain:
- Hashes
- Proofs
- Transactions

Off-chain:
- Documents
- Personal data
- Large datasets

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Legal & Regulatory Awareness

- Data protection requirements
- Digital identity regulations
- Smart contract enforceability
- Electronic signature standards

Governance Issues

- Node operation
- Validation rights
- Data ownership
- Standards definition
- Dispute resolution

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Blockchain Governance Model

Consortium Governance Board

Node Operators (Public agencies, SMEs)

Regulatory & Compliance Layer

Users & Citizens

30 of 46

Blockchain Infrastructure Operated by Consortium or Ecosystem

Consortium / Virtual Organization
Governance & Infrastructure Control

Master Nodes (Full Ledger + Consensus)
Operated by: corporations / public institutions

SME Node Partial Ledger	SME Node Partial Ledger	Self-employed Node Partial Ledger	Partner Node Partial Ledger

31 of 46

SME Participation Model in Blockchain Infrastructure

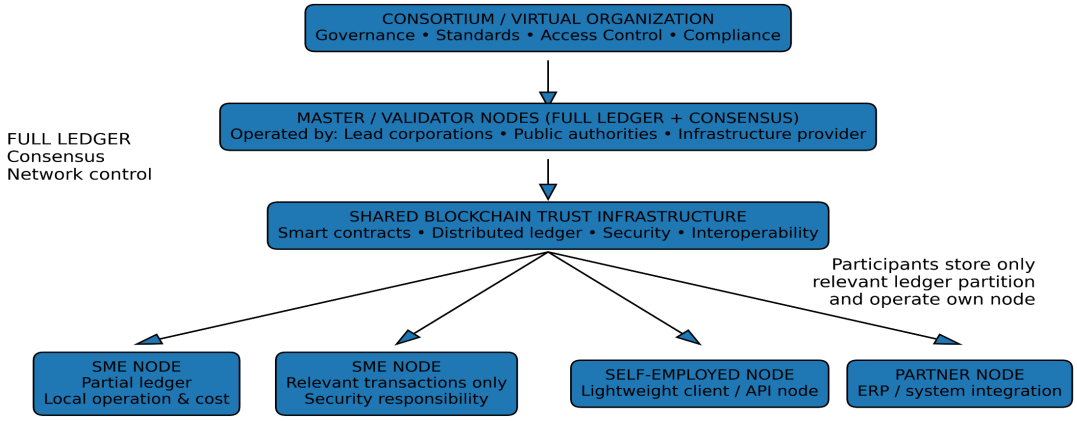
Infrastructure Governance
Consortium or Lead Organization

Blockchain Infrastructure
Full nodes, consensus, security

Run participant node	Ensure security	Store ledger partition	Cover node cost

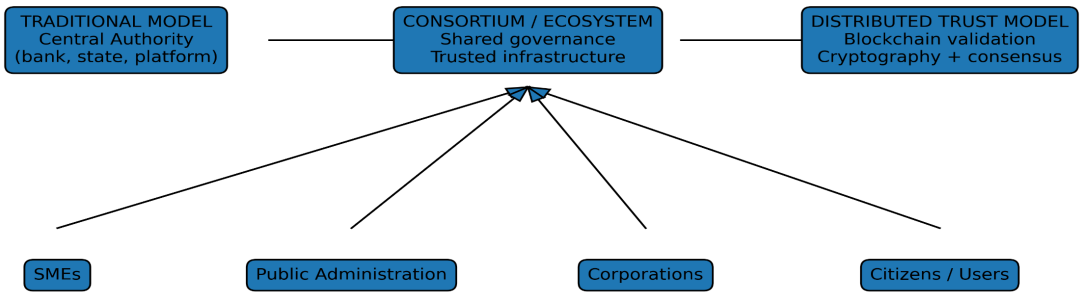
32 of 46

Consortium-Operated Blockchain Infrastructure for SMEs and Public Administration



KEY MESSAGE FOR SMEs & PUBLIC SECTOR:
Blockchain infrastructure is typically operated by a consortium or lead organization.
Participants join the ecosystem, run lighter nodes, store only relevant data,
and are responsible for operation and cost of their node while benefiting from shared trusted infrastructure.

Shift of Trust in Blockchain-Based Digital Infrastructure



Key insight: Trust shifts from single central authority → to consortium governance → to distributed technological trust based on cryptography, consensus and shared infrastructure. Law and governance remain essential but are embedded into the architecture.

Risks and Limitations

Technical:

- Scalability
- Interoperability

Organizational:

- Resistance to change
- Lack of expertise

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Adoption Barriers

- Knowledge gaps
- Unclear ROI
- Regulatory uncertainty
- Integration complexity

Success Factors

- Clear use case
- Multi-stakeholder collaboration
- Legal-by-design
- Strong governance
- Gradual implementation

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

SME & Public Administration Blockchain Ecosystem

Public Administration

Blockchain Trust Infrastructure

SMEs & Industry

Citizens / Users

38 of 46

Roadmap for SMEs

1. Identify trust problems
2. Evaluate suitability
3. Pilot project
4. Join consortium
5. Integrate systems
6. Scale

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Roadmap for Public Administration

1. Identify high-trust processes
2. Regulatory sandbox
3. Pilot projects
4. Standardization
5. Integration

When Should Blockchain NOT Be Used?

- Single organization controls all data → Use traditional database
- No multi-party trust problem → Blockchain adds no value
- High speed / real-time system required → Blockchain may be too slow
- Sensitive personal data must be deletable → Immutability conflict
- No ecosystem or consortium exists → Governance missing
- Costs exceed expected benefits → ROI not justified

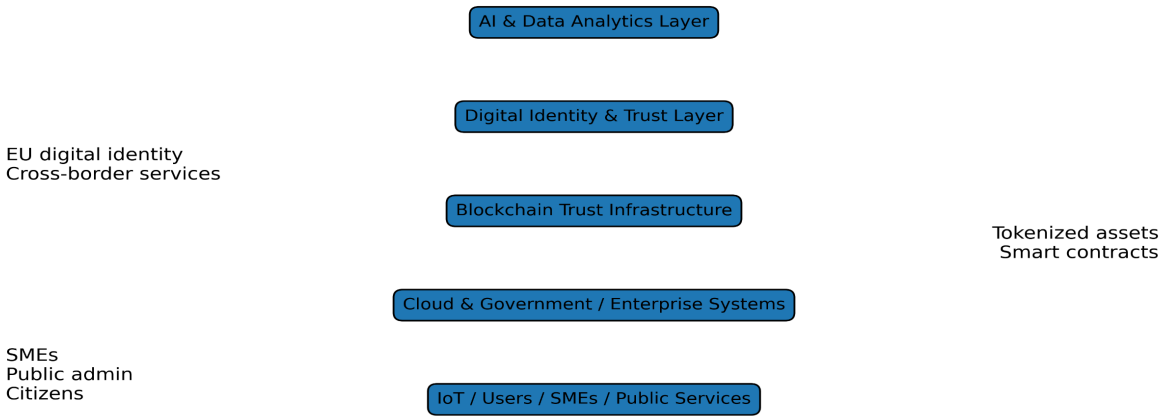
Scientific rule: Use blockchain only where multiple actors need shared trust, tamper-resistant records and coordinated governance.

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Future Outlook

- AI + blockchain
- Digital identity ecosystems
- Tokenized economy
- Cross-border services
- EBSI initiatives

Future Digital Infrastructure Architecture (2025–2035)



Blockchain becomes invisible trust infrastructure connecting AI, digital identity, public administration and SME ecosystems across borders.

Strategic Implications

Blockchain as trust infrastructure

Impact:

- Institutional trust
- Automated governance
- New digital ecosystems

Conclusion

Blockchain supports digital transformation of SMEs and public administration.

Requires:

- Proper use cases
- Integration
- Legal awareness
- Interdisciplinary cooperation

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

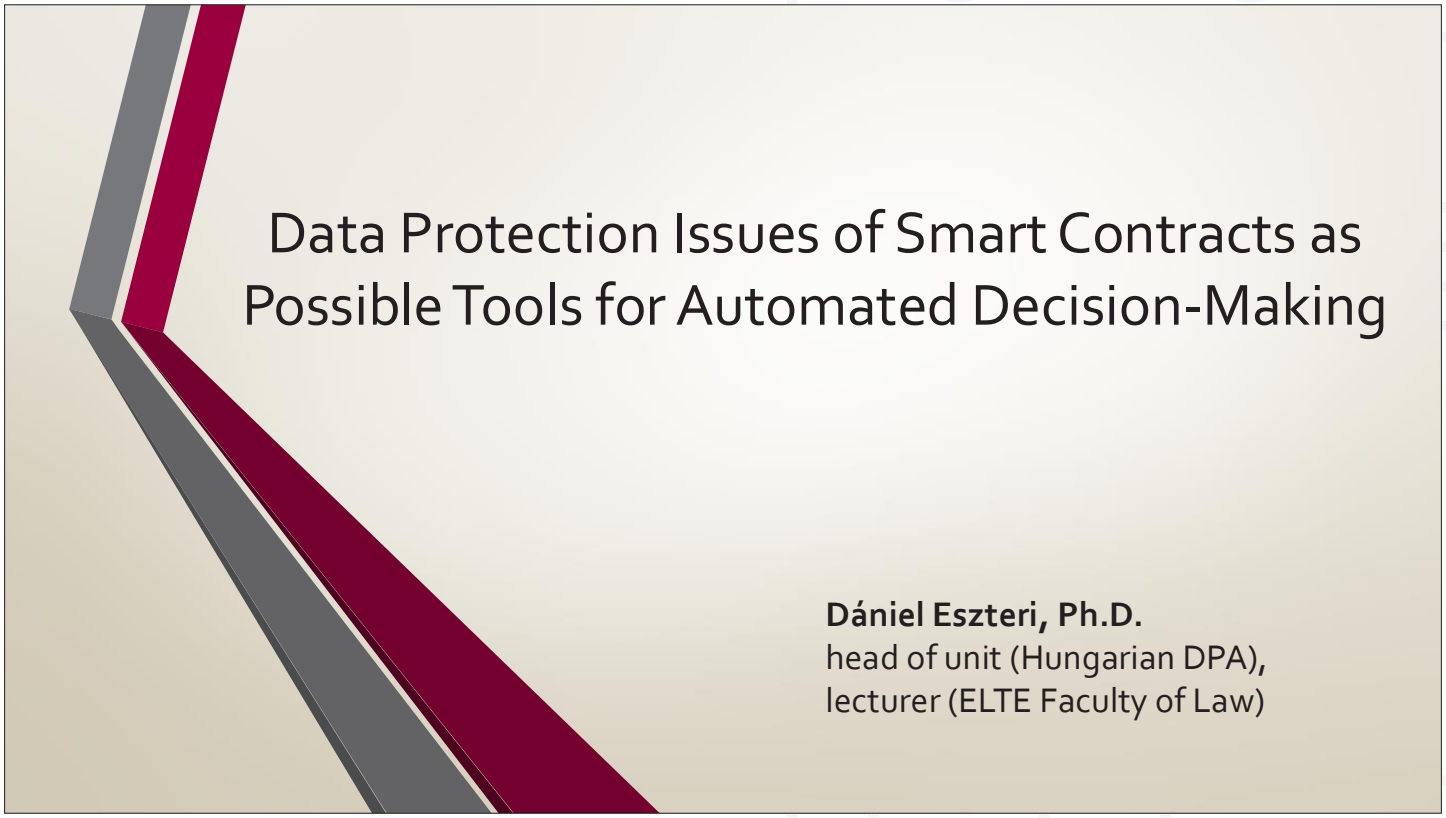
Thank You

Questions & Discussion

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

The Data Protection Issues of Smart Contracts as Possible Tools for Automated Decision-Making

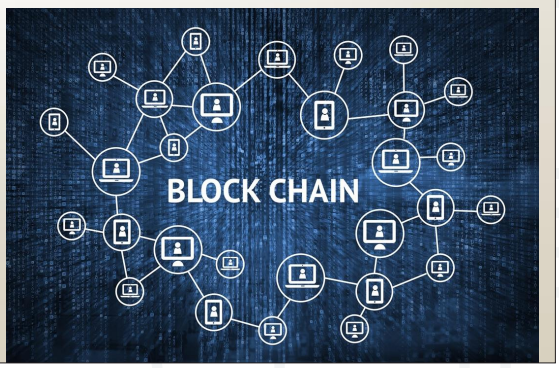
Dániel Eszteri
Head of Unit, Hungarian National Authority for Data Protection and Freedom of Information, Data Breach Notification and Forensic Analysis Unit



PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Blockchain: a data processing technology

- Blockchain is one of the representatives of so-called "distributed ledger technologies" (DLTs).
- A transactional database that is distributed over a network of multiple computers.
- No central controlling entity or server: algorhitmic self-checking verifies data.
- Individual computers = "nodes"
- Data and transactions are linked by groups ("blocks") in chronological order to form a chain of blocks.



Smart contract: automated contract based on blockchain

- The smart contract is automatically implemented if the predetermined conditions are met. [Nick Szabo, 1996.]
- The performance, security and unbreakability of the contract are ensured by the computer network in which the parties prepared it.
- The nodes authenticate the process, the conditions (e.g. deadlines) and the data to be processed in connection with it (e.g. identity of the parties, bank account number, amounts).
- Blockchain: smart contract platform
- Self-executing automated applications embedded into blockchain

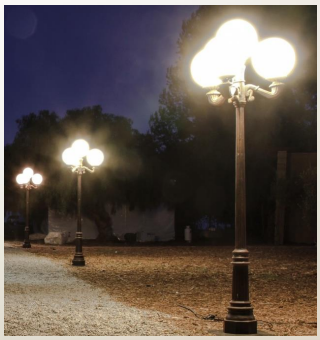
Deterministic and non-deterministic smart contracts

- Deterministic smart contract: a predefined digital contract that obtains all the necessary information from the database of the blockchain itself for which it was developed.
- Non-deterministic smart contract: This requires information that appears outside the blockchain, independent of it. The user must entrust an *"oracle"* (third party) that has the information necessary for completion.

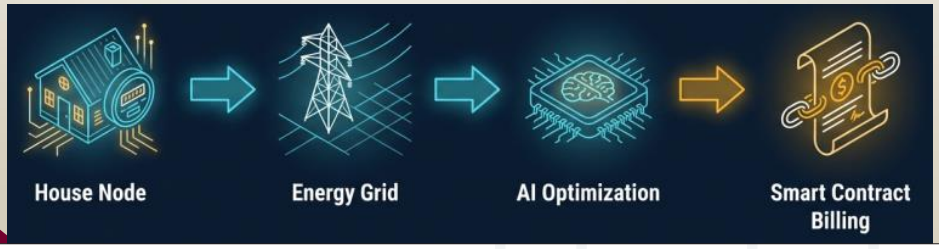
- The data transmitted by oracles can be interpretable information or unquestionable facts.
- The information to be interpreted comes into play when a smart contract needs information that needs to be considered. E.g. the fact is not clear and different experts are needed to decide the case (e.g. determining the amount of insurance in the event of damage).
- Unquestionable facts do not require a separate interpretation, as they are clear and unambiguous for all parties (e.g. the value of the outside temperature).

Examples of a blockchain-based system in a smart city

- E.g.: Optimizing the performance and operation of street lamps [Sandner et. al., 2020]:
- The network of lights makes up the blockchain, and each lamp has its own identity (block) on the network. Lamps store data on their usage, performance and downtime.
- The maintainer can take advantage of this data and optimize the maintenance of the network: e.g. an algorithm recommends more regular maintenance of the lamps that are used more frequently, etc.



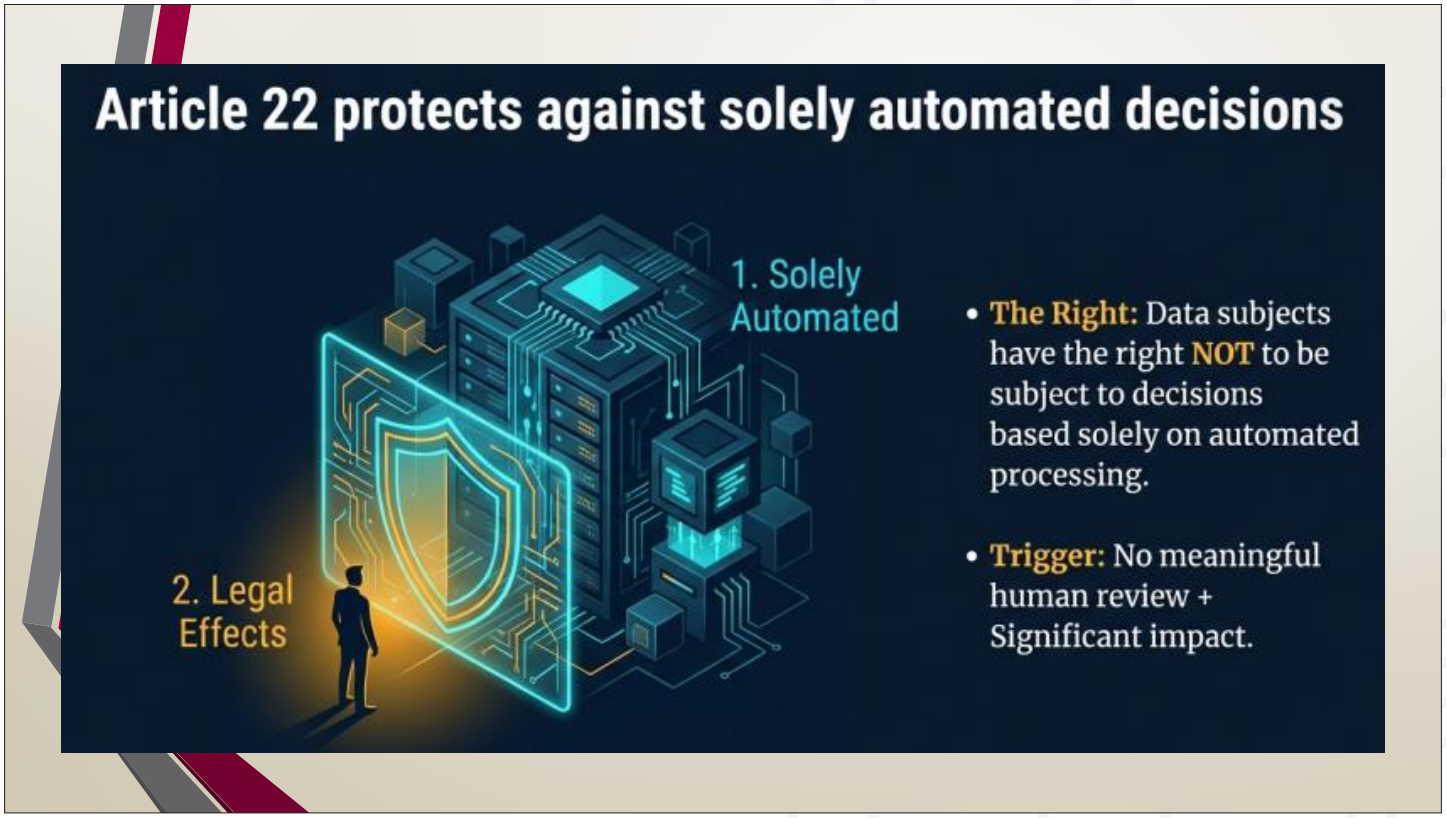
- This example can also be easily applied to a system based on personal data: Operation of "smart meters" by utility providers [WP29 07/2013]
- Individual households: blocks of the network.
- Blocks: Data on water, gas, electricity consumption, etc.
- These are sent in real time by the network to the service providers.
- AI and machine learning technologies can analyse household consumption data: identify consumption patterns to optimise energy distribution between consumers.
- Individual providers can also share identified data processing patterns with each other to synchronize their services for better service distribution.

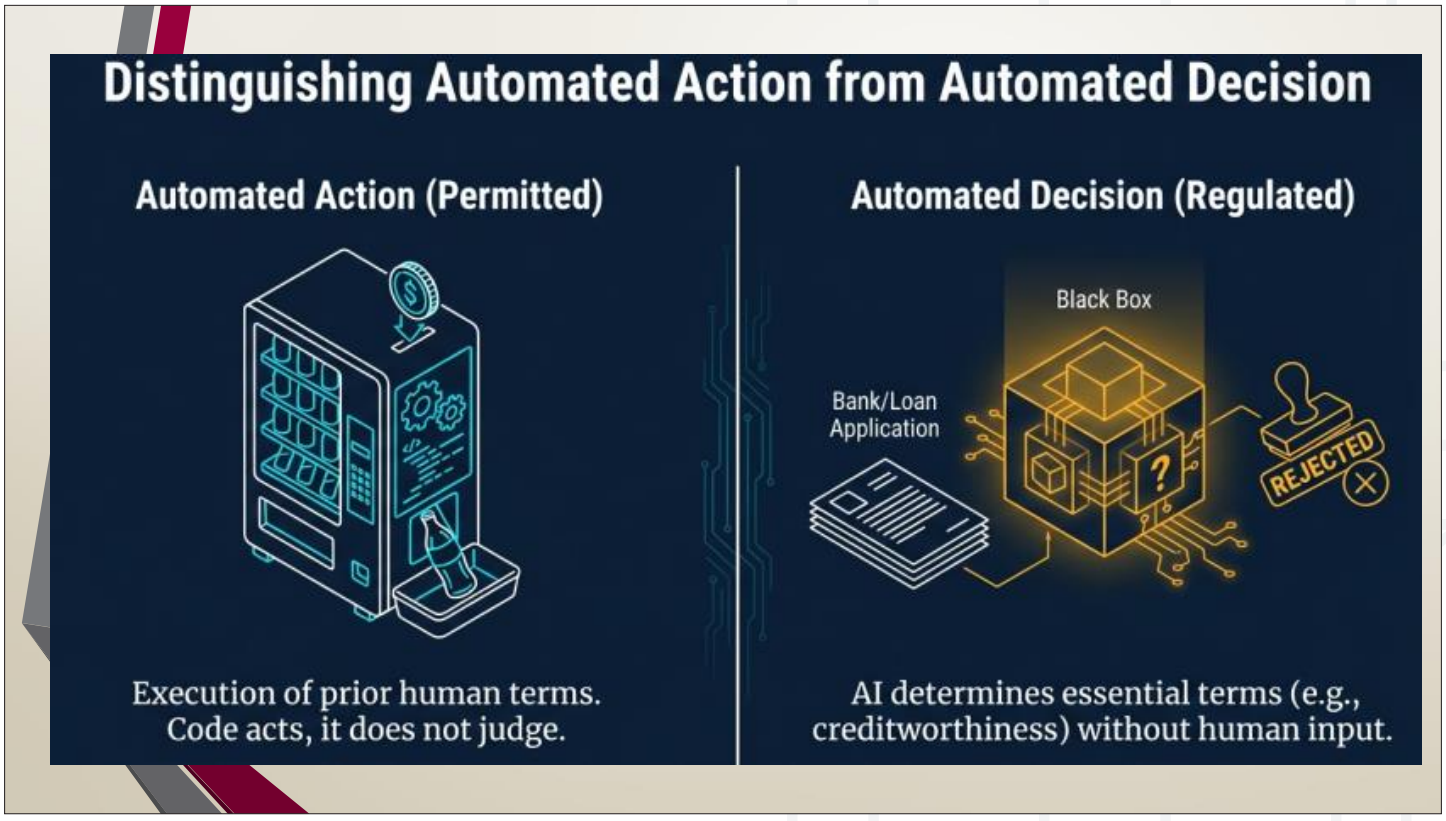


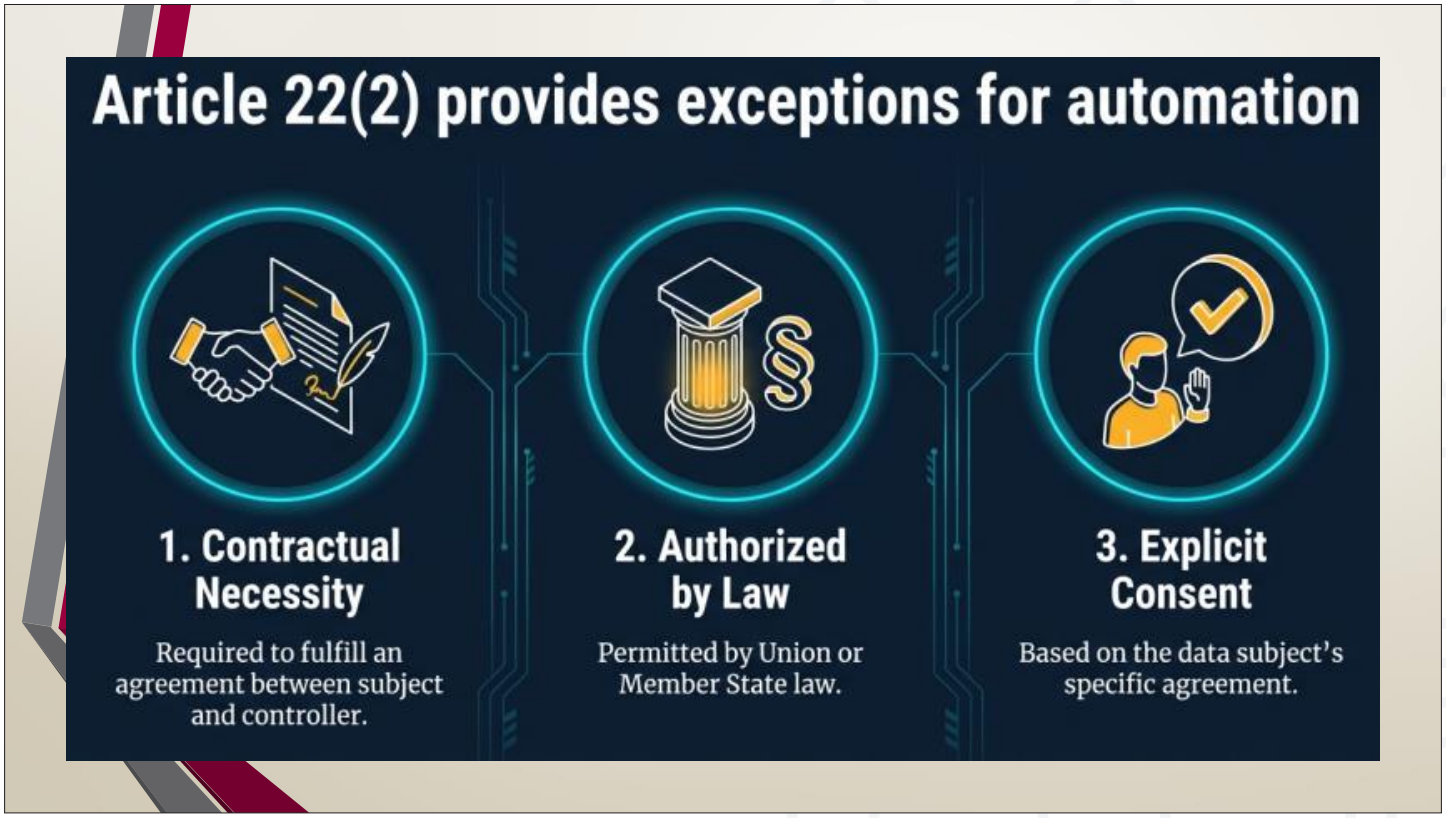
- The history of consumption data is also recorded in the blocks (households) and can be traced historically → This can make the system more transparent and help to further develop the AI and machine learning techniques used to make the smart grid and smart metering system work better.
- Smart contract apps can process billing and service data from households. For example, a smart contract app can track consumers' unique consumption data and issue "smart bills," or even automatically initiate financial transactions to users' bank accounts or crypto wallets.
- If it is necessary to collect data from third parties in order to carry out contractual transactions, then oracles can also be created in the system. E.g. to take into account discounts for certain users.

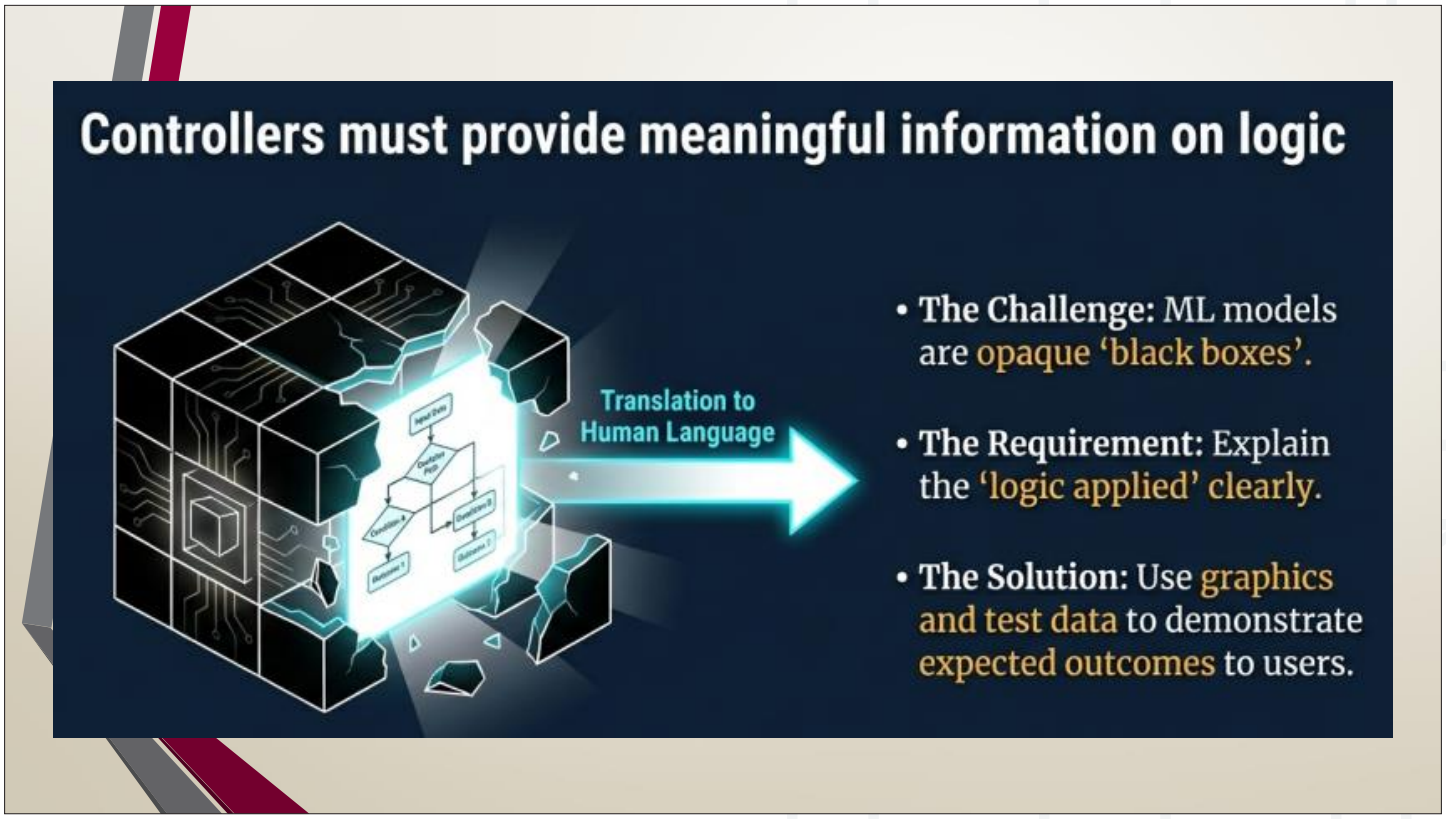
Applicability of the GDPR

- Node operators are considered data controllers for the purposes of adding data and commanding transactional operations [CNIL 2018, NAIH 2017, EDPB 2025]
- Cryptographic authentication of transactions ordered by others → Data processing [CNIL 2018, EDPB 2025]
- Design smart contract applications → Data processing


Article 22 protects against solely automated decisions
1. Solely Automated
2. Legal Effects
• The Right: Data subjects have the right NOT to be subject to decisions based solely on automated processing.
• Trigger: No meaningful human review + Significant impact.

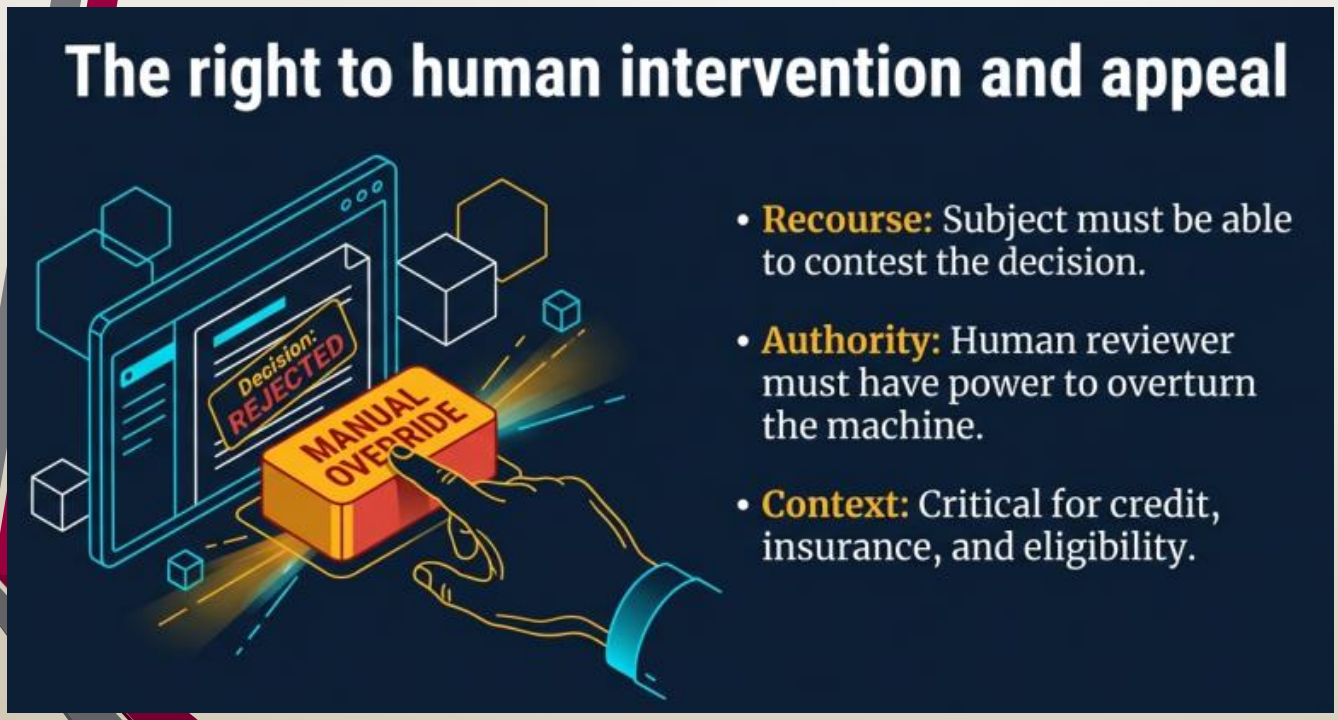

Distinguishing Automated Action from Automated Decision
Automated Action (Permitted)
Execution of prior human terms. Code acts, it does not judge.
Automated Decision (Regulated)
Black Box
Bank/Loan Application
REJECTED
AI determines essential terms (e.g., creditworthiness) without human input.





PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

The right to human intervention and appeal

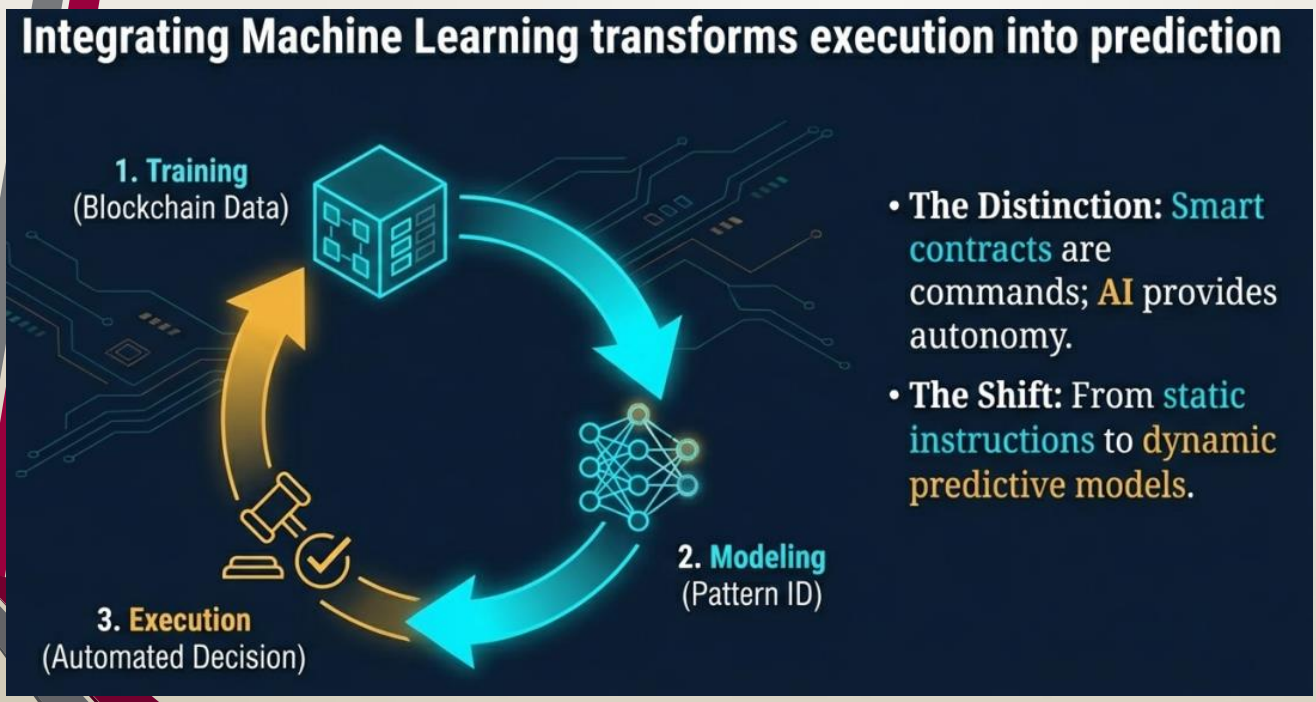


- **Recourse:** Subject must be able to contest the decision.
- **Authority:** Human reviewer must have power to overturn the machine.
- **Context:** Critical for credit, insurance, and eligibility.

Automation on the blockchain and the relationship with GDPR

- Synergy of blockchain, AI, and smart contracts:
- **First approach:** AI analyzes the data stored in the blockchain and tries to look for patterns in it, so the blockchain serves as a source of data (a training database) in the process of machine learning.
- **Second approach:** AI not only analyzes data, but also makes decisions and they are recorded in the blockchain (the blockchain and the Merkle tree).

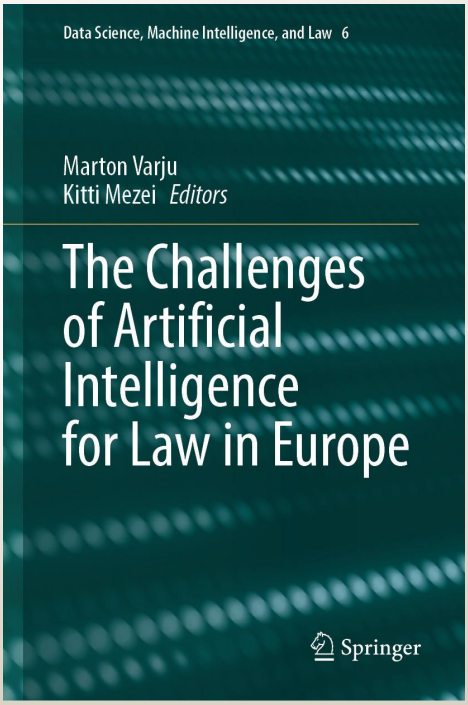
- Automated action =/= Automated decision.
- Smart contracts may not fall under Article 22 of the GDPR, as in many cases they only implement decisions made by humans in advance. Usually deterministic systems.
- At the same time, if the system makes independent decisions, for example in the case of an energy network optimized by machine learning, then Article 22 of the GDPR may already apply.



Conclusions

- **Smart contracts** efficiently automate and secure contractual relationships, typically using blockchain as a highly secure and distributed technical infrastructure.
- **Most smart contracts are not AI systems,** as they usually execute predefined actions and do not make autonomous, data-driven decisions.
- **Combining smart contracts with machine learning** enables complex automated decision-making systems that may significantly affect users' and consumers' rights.
- **Data protection compliance becomes critical** in such systems, and the applicability of **Article 22 GDPR** must be assessed, with transparency and explainability as key requirements.

Dániel Eszteri: The Data Protection Issues of Smart Contracts as Possible Tools for Automated Decision-Making. In: *The Challanges of Artificial Intelligence for Law in Europe* (eds.: Kitti Mezei, Márton Varju), Springer 2025



PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

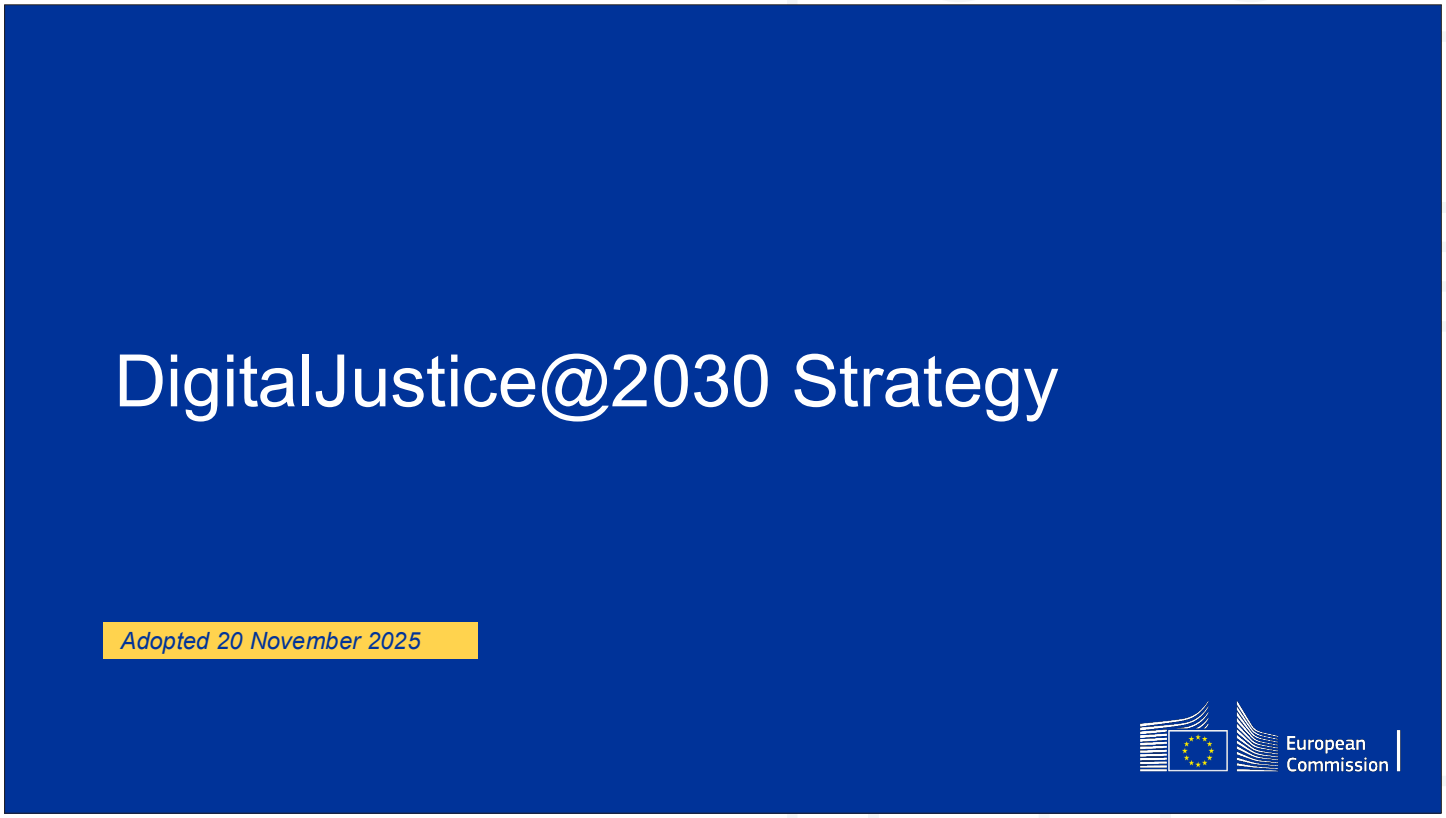
Thank you for your attention!

eszteri.daniel@naih.hu

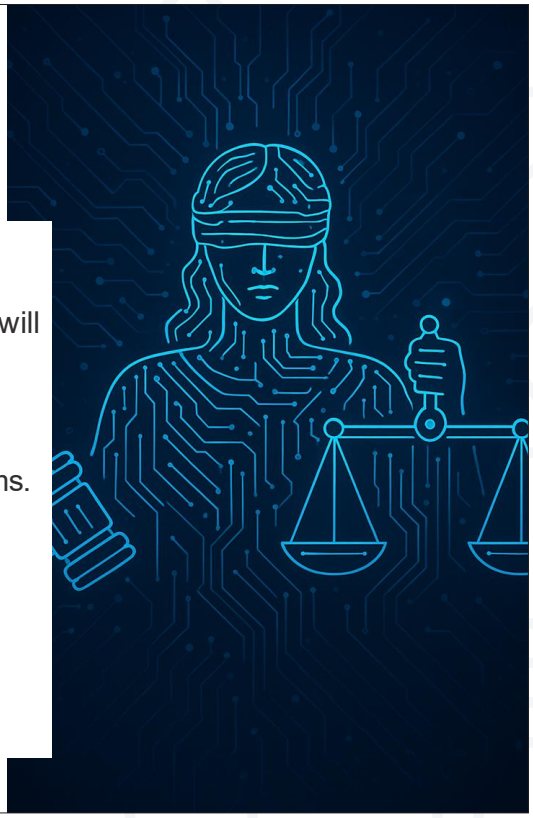
Digitalisation and the Deployment of AI, with a Particular Focus on the Digital Justice 2030

Strategy

László Csaba Ormai
Policy Officer, European Commission, DG Just, Digital transition and Judicial Training Unit



DigitalJustice@2030



- The EU's competitiveness will increasingly depend on the digitalisation of all sectors, which will drive investment.
- Digitalisation and the deployment of artificial intelligence (AI) will be essential to public authorities to deliver high-quality public services at reduced cost - also in the field of justice.

Objective: accelerate the digitalisation of national justice systems.

This should bring:

- Efficiency gains and cost savings.
- Effective justice - a pre-condition for growth.
- Resilient justice.

2

Workstreams

- Mapping and monitoring
- IT toolbox
- AI in justice
- Videoconferencing
- European Legal Data Space
- Full digitalisation of cross-border proceedings
- Funding

Mapping and monitoring

Challenge:

- Some Member States are progressing well with digitalisation while others are less advanced.
- It may be challenging for Member States to obtain useful information on tools and experiences from other member States, to facilitate the digitalisation of their own national justice systems.
- Same or similar IT tools and data standards could be used in the Member States to prevent re-inventing the wheel and save costs.

4

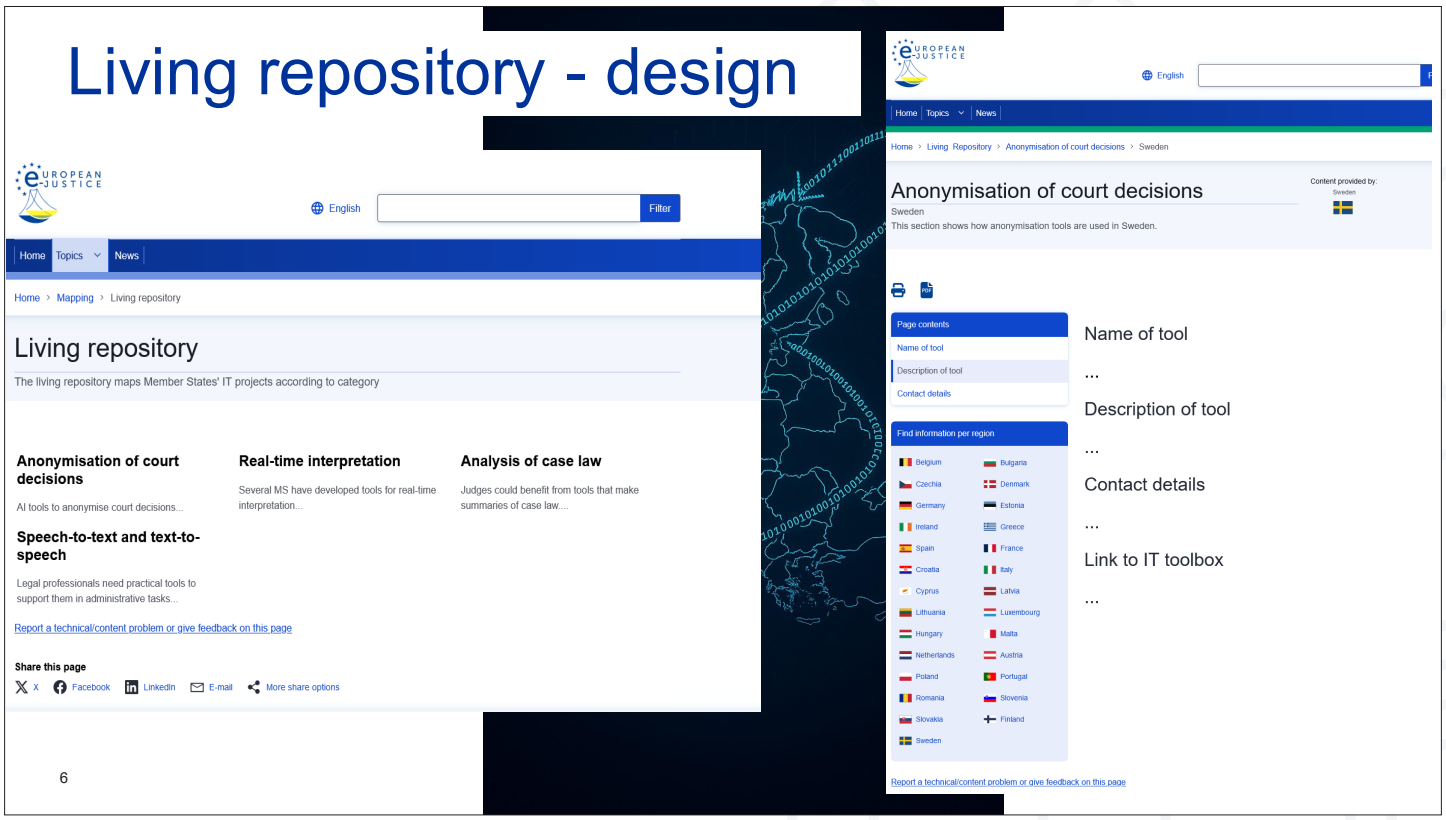
Mapping and monitoring

Solution:

- The Commission, together with the Member States, will create a knowledge base on digitalisation projects and tools used in the Member States
- This work will build on the work already carried out by the previous ES and PL Presidencies and the Council
- Based on this mapping exercise, a 'living repository', hosted on the E-Justice Portal, will be created to facilitate an effective, permanent mechanism for collecting information and exchanging best practices on digitalisation of justice.

5

Living repository - design



Name of tool

...

Description of tool

...

Contact details

...

Link to IT toolbox

...

Mapping and living repository - actions

- **Action 1:** The Commission will create a living repository of digital tools, in particular AI, used in justice across the EU, available on the European e-Justice Portal by the end of 2026.
- **Action 2:** The Commission will facilitate exchange of best practices among Member States on digital tools, in particular AI, used in justice.

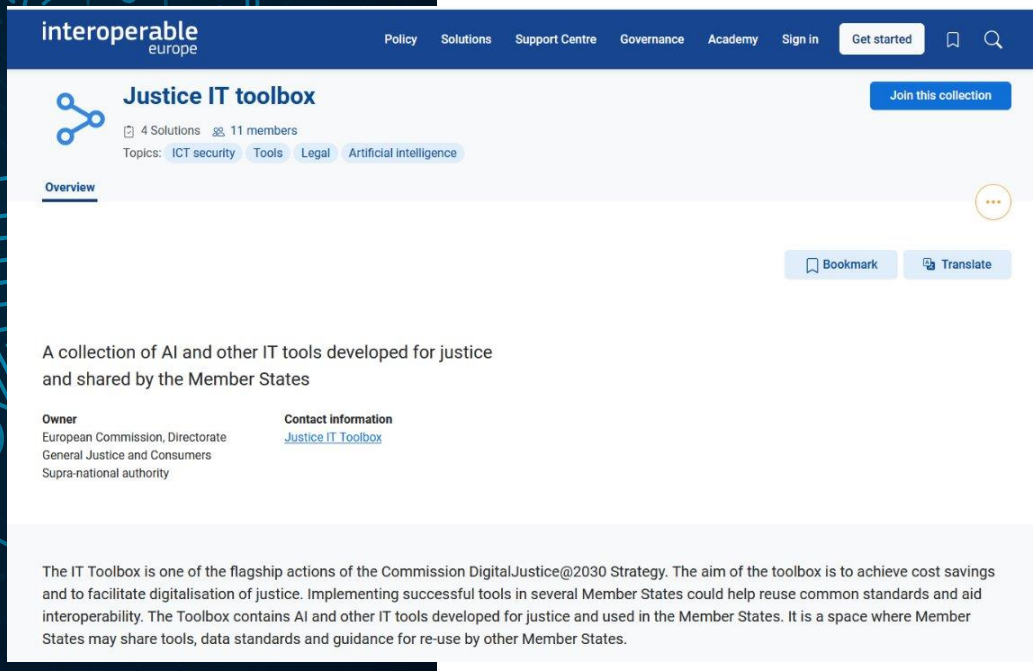
IT toolbox for justice

- Similar problems in the national justice administrations to be addressed by digitalisation.
- Digitalisation brings efficiency gains but it is costly.
- Sharing of IT tools between Member States could reduce costs.
- Reuse of tools promotes interoperability and common standards.

Solution:

- Toolbox on the **Interoperable Europe Portal**
- Linked to the Public Sector Tech Watch
- There will be a general link on the main page of the toolbox to the e-Justice Portal, and vice versa. In addition, for every tool that is available in the toolbox, a link will be placed on the e-Justice Portal leading to the toolbox (and vice versa).

IT toolbox for justice - design



PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

IT toolbox vs Living repository and actions

- The living repository will host not only IT tools but also best practices, description of project and links to their factsheets
- The IT toolbox would be hosted by the Interoperable Europe Portal, while the living repository would be hosted by the e-Justice Portal
- The Interoperable Portal would have no restrictions on access to its content, whereas the Living Repository is supposed to have some kind of access limitations to courts, legal professionals
- The IT toolbox would contain links only to open-source software, whereas the living repository would contain links to open-source software and proprietary tools as well

- **Action 1:** The Commission will create the IT toolbox by the end of 2026 and promote its use.

AI in justice

- **AI Act:** legislative framework - rules for high-risk AI.
- The AI Act requirements take care of fundamental rights concerns.
- Commission will adopt guidelines – input from DG JUST on justice sector.
- Member States still need to decide:
  whether & how to use AI in justice.
- Possibly justice-specific guidance on where to use AI in justice and how in the most efficient way.

11

AI in justice - actions

Action 1: The Commission will elaborate on the use of high-risk AI systems in justice notably by defining relevant guidelines under the AI with input from the justice community.

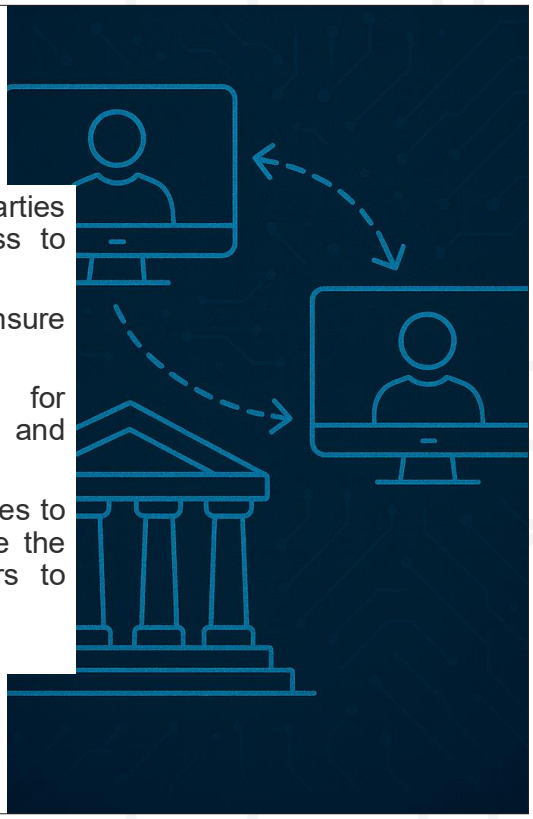
Action 2: The Commission will identify together with the Member States, and other relevant stakeholders areas where the EU can support them in their uptake of AI in justice, possibly with dedicated guidelines about whether, for what purpose, and how they could use AI tools.

12

Videoconferencing

- Videoconferencing facilitates the participation of parties located in different Member States, improving access to justice and reducing costs.
- There are certain practical challenges to be tackled to ensure that remote hearings via videoconference go smoothly.
- Voluntary common technical requirements for videoconferencing could help to overcome problems and improve the quality of videoconferencing.
- Providing an IT solution that would enable Member States to use their own videoconferencing tools could help solve the interoperability issue, which currently creates barriers to cross-border videoconferencing.

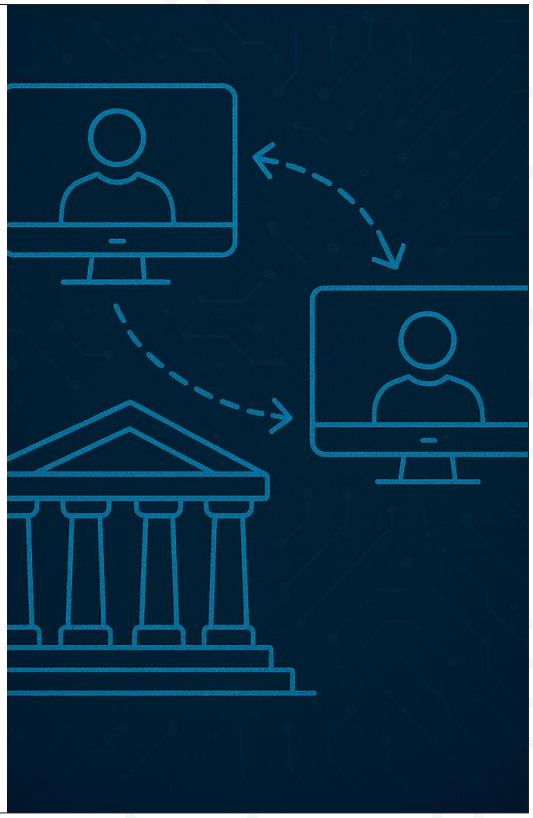
13



Videoconferencing - actions

- **Action 1:** The Commission will recommend voluntary, common EU-wide technical requirements for videoconferencing by the end of 2027.
- **Action 2:** The Commission will study the feasibility and assess the costs and benefits of different options to overcome interoperability issues for cross-border videoconferencing in judicial proceedings by the end of 2027.

14



European Legal Data Space

- Legal and judicial data is a treasure of information

We aim to achieve:

- Every justice practitioner can access the relevant law and case law of another Member State, when applying foreign law in cross-border proceedings.
- Legal and judicial data are available in machine readable format for LegalTech companies to develop and train AI applications for the use in justice.

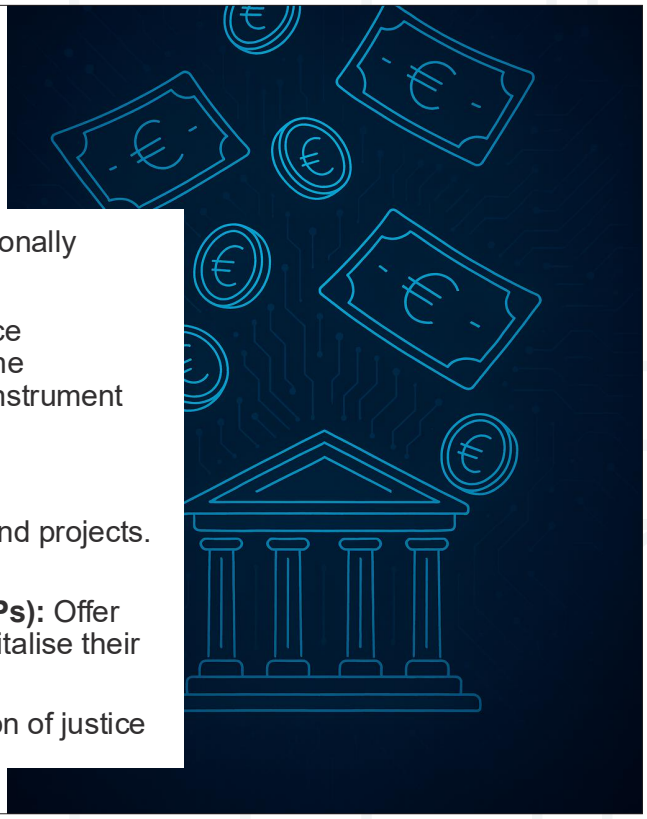
How?

- Support Member States to fully roll-out ELI and ECLI
- Adding legal and judicial data to the list of high-value data sets

Full digitalisation of cross-border proceedings

- Full digitalisation of civil and commercial court proceedings from launching a court case to the judgment = cost and time savings for businesses and citizens.
- Most cross-border procedures are not fully digital.
- The Commission will analyse the costs and benefits of closing the remaining gaps to achieve fully digital cross-border proceedings.
- To be discussed after the European Electronic Access Point becomes operational in 2028.

EU Funding is key



Almost all actions require significant investments, nationally and/or at EU level.

Under the **current MFF:** e-justice call under the Justice Programme, with a priority on the implementation of the Digitalisation Regulation, and the Technical Support Instrument (TSI).

Under the **proposed new MFF** (still to be adopted):

- **Justice Programme:** funds EU-level IT systems and projects. Proposed tripling of the budget.
- **National and Regional Partnership Plans (NRPPs):** Offer Member States access to significant funding to digitalise their national justice systems.
- Important for Member States to include digitalisation of justice in their NRPPs.

TUTELA: CONSUMERS AND LAW

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

The new Consumer Credit Directive and its implementation in Italy

Elena Bargelli
Professor of Private Law, University of Pisa

Implementation of the Consumer Credit Directive in Italy

Elena Bargelli
Professor of Private Law
University of Pisa

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Legislative decree 31 December 2025, no 212 implementing CCD3 and amending Banking Act (Testo Unico Bancario - **TUB**)

CCD2 and CCD3 have been implemented in the Banking Act (TU 385/93)

CCD3 – implementation without substantial changes

→Full harmonisation→MSs not allowed to maintain or introduce national provisions diverging from those laid down in this Directive.

Room is left to MSs for remedies and penalties applicable to infringements of the national provisions adopted pursuant to the CCD3

Remedies→ Such restriction should only apply where there are provisions harmonised in this Directive. **Where no such harmonised provisions exist, Member States should remain free to maintain or introduce national legislation** (ex., provisions on joint and several liability of the supplier of goods or the provider of services and the creditor, on the cancellation of a contract for the sale of goods or supply of services where the consumer exercises his or her right of withdrawal from the credit agreement)

Penalties→ Member States shall lay down the rules on penalties applicable to **infringements of the national provisions adopted pursuant to this Directive** and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive

Overview of the main obligations imposed on the creditor
1. CCD3 requires increased, more detailed information – what if they are not given?

Advertising and marketing of credit agreements (Arts. 7, 8)

General and pre-contractual information (Arts. 9-11) - The Bank of Italy specifies the content, drafting criteria,and methods of making general information available

Adequate explanations as a result of the extensive case law regarding credit agreements indexed to foreign currencies (Art. 12)

1.1. Information to be included in the credit agreement

- If the consumer has not received the contractual terms and conditions and the information in accordance with Articles 20 and 21, **the withdrawal period starts from the day on which the consumer receives the contractual terms and conditions and the information in accordance with Articles 20 and 21 – What about failing to deliver a copy of the contract to the consumer?**
- It shall in any event expire 12 months and 14 days after the conclusion of the credit agreement.
- This shall not apply if the consumer has not been informed about his or her right of withdrawal in accordance with Article 21(1), first subparagraph, point (p)

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Is the postponement of the withdrawal right the only «penalty»?

- According to Article 125-ter, consumers must repay the loan and pay any accrued interest up to the point of withdrawal.
- Does this rule also apply if the information is not provided in accordance with Articles 20 and 21?
- The Banking Act does not clarify this issue.
- Advocate General Hogan (Opinion in joined cases C-33/20, C-155/20, and C-187/20) emphasizes that Member States are allowed to provide that "the absence of certain mandatory information in the credit agreement may result in the loss of interest on the debt."

2. CCD3 requires a thorough assessment of the consumer's creditworthiness – what if it does not happen?

- Assessment of the creditworthiness of the consumer (Art. 18): Member States shall ensure that **the creditor only makes the credit available to the consumer where the result of the creditworthiness assessment indicates that the obligations resulting from the credit agreement are likely to be met** in the manner required under that agreement, taking into account relevant factors as referred to in paragraph 14→ if the bank refuses credit, it must provide reasoning and supporting documentation.

2.1. Consumers' rights in case of creditworthiness assessment involving the use of automated processing of personal data – what if the consumer's right is infringed?

- Right to request and obtain from the creditor human intervention, consisting of the right to:
- Request and obtain from the creditor a clear and comprehensible explanation of the assessment of creditworthiness (in line with Art. 86, Regulation 2024/1689 *AI Act*),
- Express the consumer's own point of view to the creditor; and
- Request a review of the assessment of the creditworthiness and the decision on the granting of the credit by the creditor

Failure to provide information and inadequate creditworthiness assessment- Administrative penalties (art. 44 CCD3, Art. 144 TUB)

An administrative fine ranging from €30,000 to 10 per cent of revenue shall apply in case of infringement of the following provisions:

Articles 123, **123-bis**,117 para. 1, 2 e 4, 118, 119, 120, 120-*quater*, 122 -*bis*, para. 2, 124 para 1,124 para. 2, **124-*bis*, 125,** para. 1 –***quinquies,*** 125, para. 2, 3 e 4, 125-*bis*, para. 1, 2, 3, 3-*bis*, 3-*ter* e 4, **125 -*septies*,** para **2,** 125-*octies*, subs. 2, **2 -*bis*** e 3, 125-*decies,* **125 -*undecies* , 125 -*terdecies*,** para. **2**

What about private law «penalties»? Lack of certain essential information→Nullity - But what about its lack of transparency?

If the contract **does not contain** certain essential information, namely the type of contract, the parties to the contract, the total amount of the loan, and the conditions for disbursement and repayment, it is void (Art. 125-*bis*, para 8 TUB)→in line with ECJ 9 November 2016, causa C-42/15, Home Credit Slovakia

See also Art. 117 TUB – lack of written form

In this case, the consumer cannot be required to repay more than the sums used and has the right to pay the amount due in installments, with the same frequency as provided for in the contract or, failing that, in thirty-six monthly installments (Article 125-*bis*, para 9 TUB).

Lack of assessment of creditworthiness – right to damages or nullty?

- ECJ 11 January 2024 C-755/22 Nárokuj s.r.o. V EC Financial Services, a.s
- Right to damages? Trib. Padova, 23 July 2024, Trib. Trani 19 september 2024, no 1326, Trib Spoleto 6 July 2023, no 529
- ABF Neaples 13 July 2023
- Nullity?

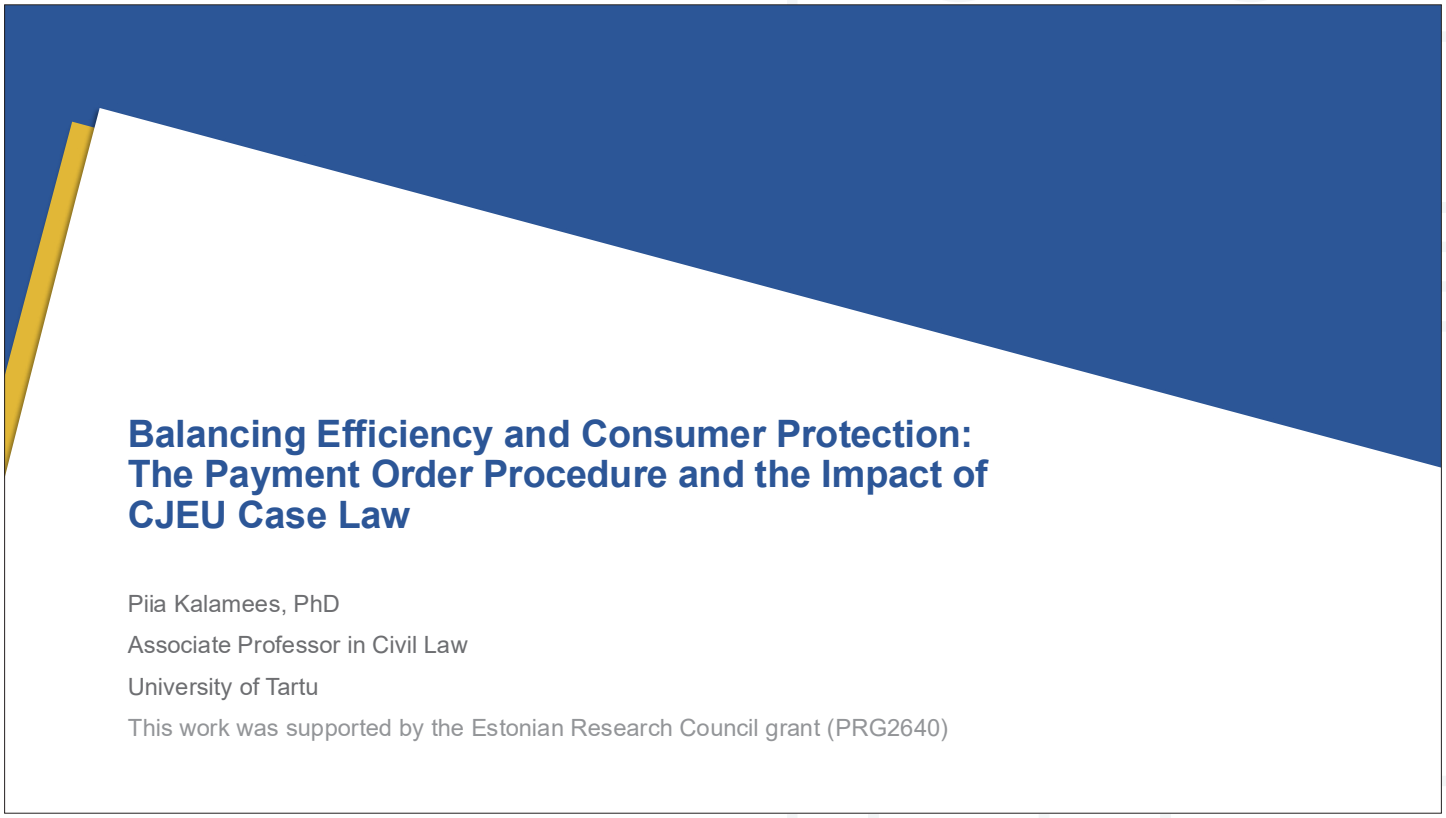
Final remarks

- The implementation of CCD3 confirms that the Italian legal system prioritises public over private enforcement of CCD3 infringements.
- The Italian legislator did not take the opportunity presented by the implementation of the CCD3 to improve private enforcement, address current gaps, or clarify some pressing open questions.
- Notably, despite the growing significance of creditworthiness assessments, the available remedies for consumers in the event of a breach remain unclear.

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Balancing Efficiency and Consumer Protection: The Payment Order Procedure and the Impact of CJEU Case Law

Piia Kalamees
Associate Professor, University of Tartu, Faculty of Social Sciences, School of Law



PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Indicators of extensive use in consumer claims

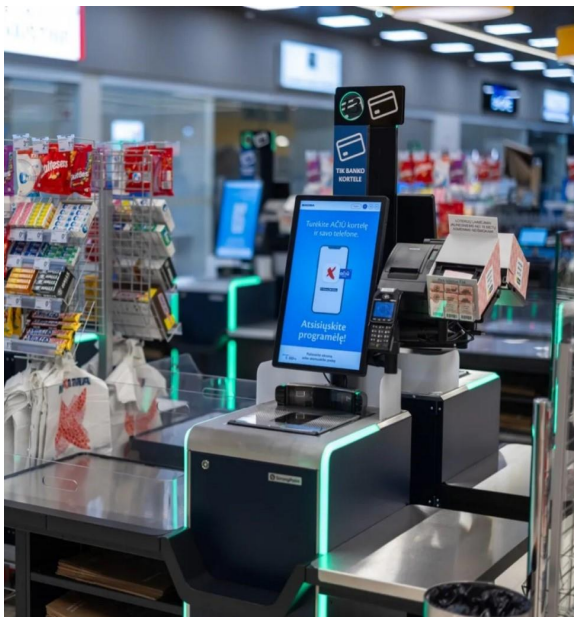
- High volume
- Mass consumer contract litigation
- Repeat-player creditor vs passive consumer
- Structural risk of unfair terms going unchecked

How the payment order procedure works?

Simplified application → **Formal** review → **Payment order** issued → **Enforcable** unless the consumer objects

Why the order for payment procedure is attractive?

- Reduced court workload
- Faster debt recovery
- Lower costs
- Reduced strategic non-payment



General rule: *ex officio* review

***Ex officio* review as an obligation of the court**

- **where legal and factual elements available** (C-243/08 Pannon)
  - in giving the default judgment (C-495/19 Kancelaria Medius)
  - in order for payment procedure (C-618/10 Banco Español de Crédito)
- while examining the **creditworthiness assessment** (C-679/18 OPR –Finance)

Ex officio review in order for payment procedure

Elements of fact and law available to the court

- the court must be allowed to assess unfair terms *ex officio* where it has necessary legal and factual elements available to it (C-618/10 Banco Español de Crédito SA)
- court allowed *ex officio control*, court official's decision does not suffice (C-49/14 Finanmadrid)

Ex officio review in order for payment procedure

Elements of fact and law not available to the court

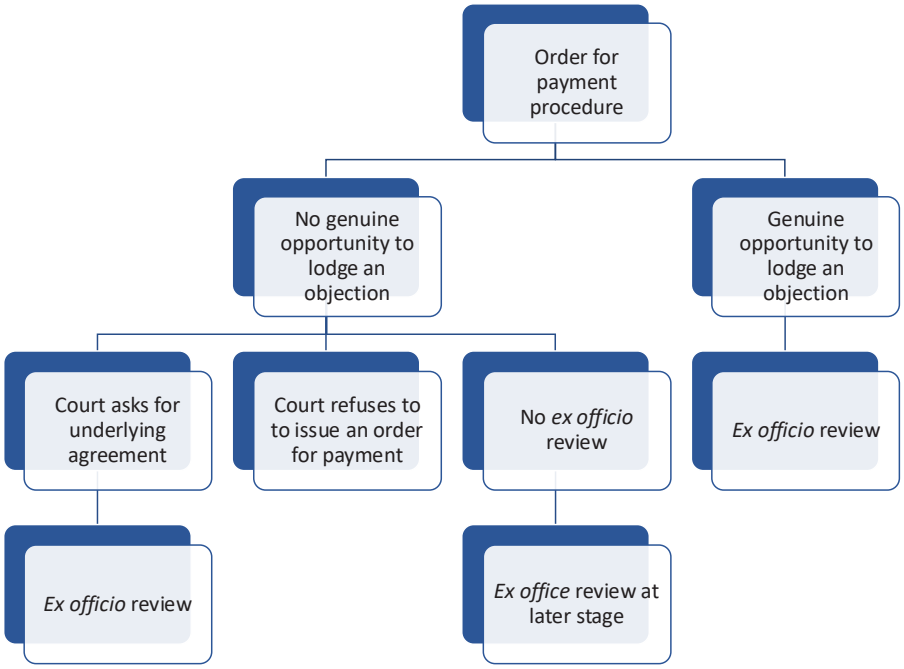
- **No obligation, if** lodging an objection is realistic and accessible (C-176/17 Profi Credit Polska, C-632/17 PKO Bank Polski, C-448/17 EOS Slovensko; C-531/22 Getin Noble Bank)
- Significant risk if the consumer needs to:
  - lodge an objection in 14 or 15 days
  - explain whether the order is disputed in whole or in part
  - explain inadmissibility
  - present facts and evidence
  - pay ¾ of the court fee when lodging an objection

Ex *officio* review in order for payment procedure

Court's obligation to assess the possible unfairness without consumer lodging an objection?

C-419/18 and 483/18 Profi Credit Polska: default judgment, national court had serious doubts regarding unfair nature of standard terms

C-453/18 and C-494/18 Bondora: European order for payment procedure, the court is allowed to request additional information related to the contract



Res judicata: the tension

- The principle of *res judicata* is of significant importance to ensure stability of law and proper administration of justice (C-421/14 Banco Primus; C-40/08 Asturcom Telecomunicaciones).

- EU law does not require a national court to disregard the principle of *res judicata*, even if doing so would allow for the remedy of a breach of the provisions of the UCTD. However, principles of equivalence and effectiveness need to be respected (C-154/15, C-307/15 and C-308/15 Gutiérrez Naranjo et al).

Res judicata: the tension

- **Reopening of proceedings**. Review of standard terms must be possible by reopening the proceedings or in enforcement proceedings or a separate subsequent procedure (C-582/21 Profi Credit Polska).

- **Enforcement proceedings**. The court in enforcement proceedings must be able, including for the first time, to assess the validity of standard terms (C-693/19 and C-831/19 SVP Projekt 1503 Srl; C-724/22 Investcapital; C-531/22 Getin Noble Bank).

- **Bankruptcy proceedings.** The court can assess the fairness of standard terms in case of the binding nature of the list of claims (*res judicata*) (C-582/23 Wiszkier).

Conclusion:
Conditional efficiency

1. The CJEU case law does **not require** that the court needs to examine the possible unfairness of standard terms or the creditworthiness assessment *ex officio* in every order for payment procedure case.
2. It **suffices** if the court can assess these matters after the consumer has lodged an objection.
3. Lodging an objection **must not be excessively burdensome** for the consumer or deter the consumer from lodging an objection.
4. The jurisdiction with regard to order for payment procedure can be conferred to **court officials**.

In case of no sufficient opportunity for *ex officio* control in order for payment proceedings, such a check needs to be performed at a **later proceeding**.

Scored by Design: AI-Driven Social Scoring in Consumer Law Contexts

Martin Hamřik
Assistant Professor, Civil Law Department Law Faculty, Univerzita Komenského v Bratislave

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

It was one of those pictures which are so contrived that the eyes follow you about when you move. BIG BROTHER IS WATCHING YOU, the caption beneath it ran.

ORWELL, G. 1984.
London: Secker & Warburg, 1949

In medias res

Prohibited AI systems (practices) – Article 5 AI Act

- ❑subliminal, deceptive, or manipulative techniquesexploitation of vulnerabilities
- ❑social scoring
- ❑predictive criminal risk profiling
- ❑untargeted facial image scraping
- ❑emotion recognition (workplaces and schools)
- ❑biometric categorization
- ❑real-time remote biometric identification for law enforcement

Hypothesis

AI driven social scoring within B2C relationships is prohibited under Art. 5 (1) c Act on Artificial Intelligence.

Reasons behind Art. 5 (1) c) Artificial Intelligence Act

The following AI practices shall be prohibited: ....

c) the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

- (i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;
- (ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity

Slovak E-kasa Ruling

"automated assessment based on blanket data collection interferes with the right to "informational self-determination," regardless of consequences."

Constitutional Court of the Slovak Republic
(PL. ÚS 25/2019)

Forbidden AI Social Scoring Test (B2C)

1. Deployment
Used in a specific relationship (B2C)

↓

2. Evaluation
Classifies consumer over a period of time

↓

3. Result
Leads to detrimental or unfavorable treatment

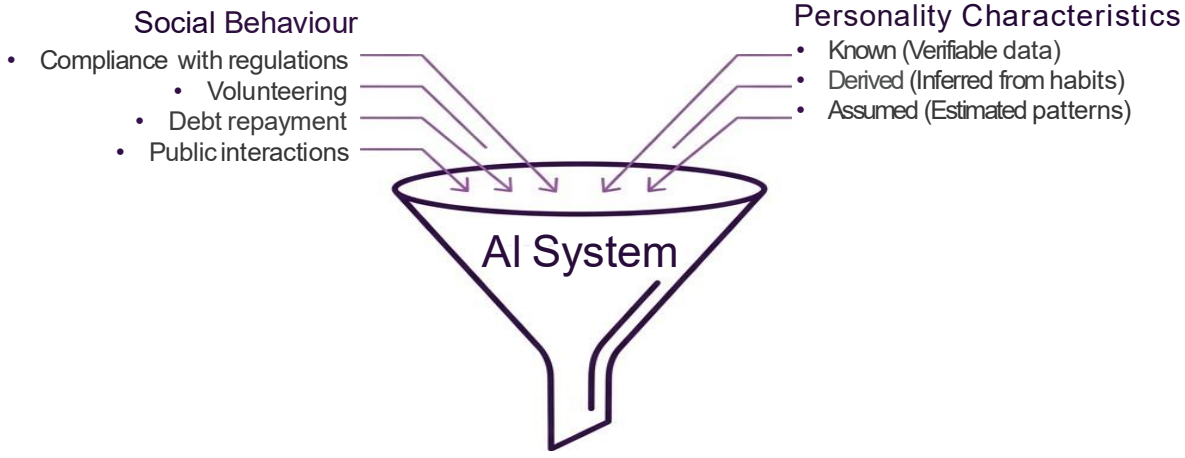
↓

4. The Trigger (Crucial)
Occurs in an unrelated context OR is unjustified/disproportionate to the behavior.

1. Deployment of AI system in a B2C relationship

- placing on the market
- putting into service
- use of AI systems

2A. Data collection & Evaluation or classification of consumer



Social score of consumer

2B. Evaluation over period of time

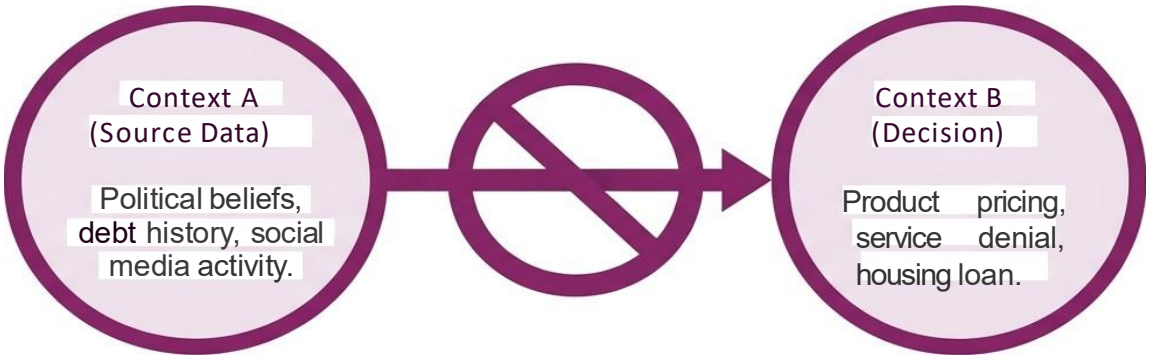
At the time of the decision
- not one-off evaluation
- not a single criterion identified

3. Result

the social score assigned to a consumer by an AI system is the reason for the trader's inappropriate harmful or unfavourable treatment of the consumer

4A. Trigger – (Un)related context

- *is carried out in a social context unrelated to the contexts in which the data for the social score was originally generated or collected*



4B. Trigger – (Dis)proportionality

- *it is unjustified or disproportionate to the social behaviour of a natural person or its seriousness*

Behavior: Return of goods (14-day right)

Penalty: Refusal to sell or Price Hike

Permitted scoring?

- **Creditworthiness**
  Assessing ability to repay a loan (required by law).
- **Insurance**
  Health assessments for life insurance (sector-specific regulation).
- **Fraud Prevention**
  AML (Anti—Money Laundering) checks.
- **Platform Safety**
  Identifying users who violate terms of service (e.g., hate speech).

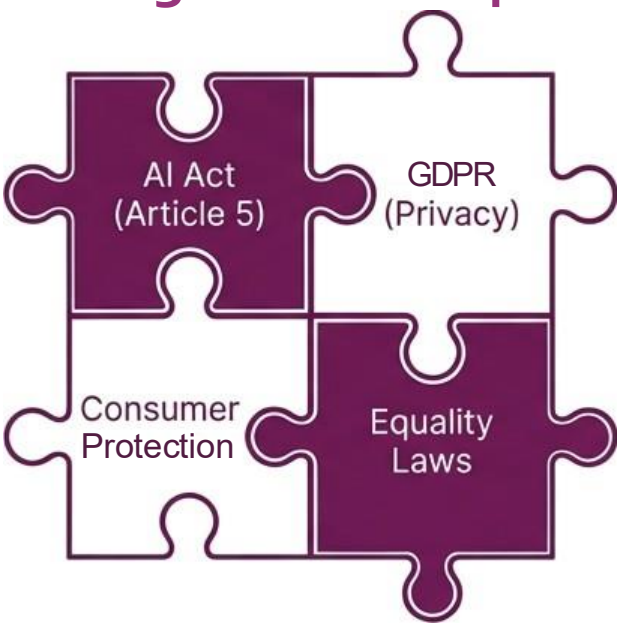
Is positive social scoring permitted?

The Trap: A reward for one group can imply a punishment for another.

Legal Boundary: Positive scoring becomes illegal if it constitutes:

- Unfair Commercial Practice (Misleading pricing)
- Discrimination (Violating the Consumer Protection Act)

Social Scoring in B2C Compliance



Conclusion

AI driven social scoring within B2C relationships is
NOT
prohibited under Art. 5 (1) c Act on Artificial Intelligence,

if conditions are met:

- context-limited
- purpose-bound
- proportionate
- does not cause unjustified or cross-domain harm

Thank you for your attention!

Back to the Future – How Would Roman Law Respond to the Technological Legal Challenges of Today's Car Manufacturing?

Péter Báldy
Vice Director of Institute for Postgraduate Legal Studies, ELTE Law

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

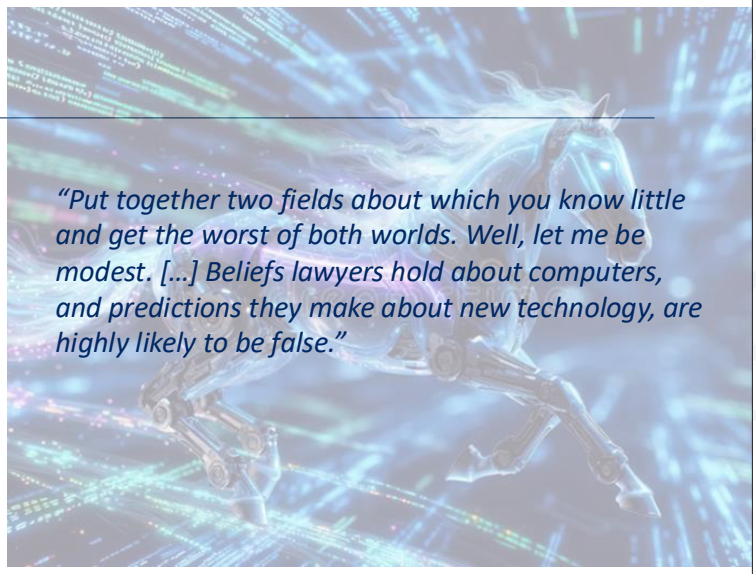
Law of what?

Law of the Horse

Frank H. Easterbrook (1996)

Legal aspects of blockchain and digital assets — issues of technology and law

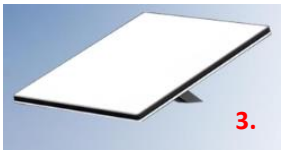
Law of
- technology?
- blockchain? else?
- AI?

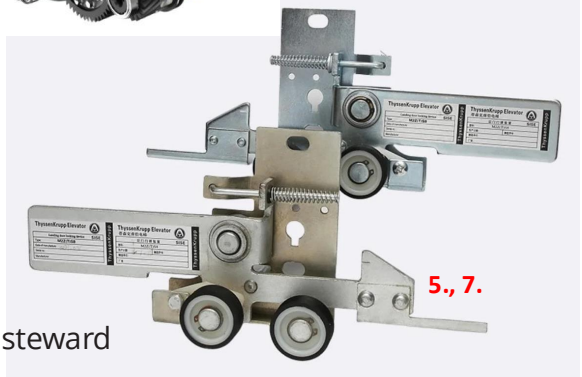


GDPR (15):

" In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used."

CRA obligation – 5(7) outcome





- manufacturers
- suppliers
- importer
- distributor
- open-source software steward

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Responsibility – accountability – liability

Existed in roman law

contratual – delictual

diligence

What has changed?

complexity of legal relationships

interdependency

What has not changed?

the substantive content of the legal relationship

Top 5 legal issues in technology

1. AI regulation and accountability
   - who is liable when AI causes harm
   - how to handle biased or opaque algorithms
   - new legal categories (like "electronic personhood") are needed or if existing liability rules suffice
2. Data protection and privacy
   - Automated decision making and profiling
   - Farewell to consent models
3. Cybersecurity and cybercrime
   - IT creates its own risks
4. Intellectual property in the digital/AI age
   - exploiting AI generated content
   - training AI
5. Digital platforms and contents
   - competition
   - fairness
   - free speach

What has changed? The dimensions.

Ad 1. ???
Ad 2. 'dignitas, bona fama'
Ad 3. 'crimen'
Ad 4. 'honorarium'
Ad 5. 'bona fides'

ELTE EÖTVÖS LORÁND UNIVERSITY
BACK TO THE FUTURE - HOW WOULD ROMAN LAW RESPOND TO THE TECHNOLOGICAL LEGAL CHALLENGES OF TODAY'S CAR MANUFACTURING?

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

Characteristics of AI

AI

- a machine-based
- autonomy
- may exhibit adaptiveness
- for explicit or implicit objectives
- Infers
- generate outputs
- that can influence physical or virtual environments

Servi

- human
- autonomy
- may exhibit adaptiveness
- for explicit or implicit objectives
- Infers
- generate outputs
- that can influence physical or virtual environments

'peculium'
'noxa'

Be agile?

Technology: leans on short time frames, adaptability, and iteration

Legal system:

- iteration is basic feature of law: regulation – application – awareness – re/de regulation
- who to be on short time frame? Legislator? Law enforcement? What is short?
- what to adapt to? Technology? Business? Citizens' expectations?

Rushed regulation = undervalued legal science

What is the most significant novelty of artificial intelligence applications that we are unable to handle?
Where has the complexity of the legal relationship really expanded?
the spread of non-deterministic algorithms

ELTE EÖTVÖS LORÁND UNIVERSITY
BACK TO THE FUTURE - HOW WOULD ROMAN LAW RESPOND TO THE TECHNOLOGICAL LEGAL CHALLENGES OF TODAY'S CAR MANUFACTURING?

Cross-sterilization of ideas

"AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm"

In the era of Zombification and Non-Player Consumer
more detailed regulation or
flexibility in interpreting the moral foundations of law?

"the best way to learn the law applicable to specialized endeavors is to study general rules" Frank H. Easterbrook

Do we need law or recipe (algorithm)?

PROGRAM FINANCED FROM THE NRDI FUND
Mecenatúra

ELTE EÖTVÖS LORÁND UNIVERSITY

Thank you!

Back to the Future – How Would Roman Law Respond to the Technological Legal Challenges of Today's Car Manufacturing?

Báldy Péter | ELTE Faculty of Law, Institute for Postgraduate Legal Studies

LEGAL ASPECTS OF BLOCKCHAIN AND DIGITAL ASSETS — ISSUES OF TECHNOLOGY AND LAW
12 February 2026 | ELTE Faculty of Law