UNECE Chain Project

Legal Interoperability Working Group

9 July 2020

Legal Interoperability

Managing cross-border issues

Legal interoperability is about the options and barriers foreseen when working together requires operations that cross borders (from a legal point of view) and thus become subject to different legal frameworks.

Our working group looked at potential legal issues that would arise regarding:

- Determining Applicable Laws
- Tamper evidence, resistance, and immutability
- Privacy
- Legal governance
- Digital Signatures
- Smart Contracts
- Multi-chain transactions

We also looked at how UNECE can play a role in addressing these issues.

Applicable Laws

Where is the blockchain located?

Determining the applicable law is the first challenge

- General laws like GDPR don’t take into account the decentralized nature of blockchains
- Conflict of laws in different jurisdictions is not always settled
- This means legal uncertainty

Many types of law can apply to blockchains

- Laws that affect Code (communication laws, IP rights, encryption)
- Laws that affect Governance (arbitration, antitrust, liability)
- Laws that affect Use Cases (financial regulation, AML, privacy, consumer protection)

There may be different connecting factors determining the respective applicable law by jurisdiction. E.g. some local laws may only apply to residents.

Choice of law and arbitration clauses may help but some laws such as GDPR cannot be waived.

Would a different law apply to a Public blockchain than a private permissioned one? What if they interoperate?

Tamper evidence, resistance, immutability

Hope you're making some good points.

Immutability is a key feature of DLTs

Legally some data may need to be modifiable

- Storing the information off-chain and only storing a hash to prove the information on-chain.
- A private chain that is connected as a side chain to a public main chain. If needed, the data can be deleted and a new corrected side chain created. This may reduce trust in the system.
- A specialized architecture that provides the possibility to delete entries under specific conditions. For example, by automatically deleting all records after 10 years. Technologies like chameleon hashes can be used for that purpose.

When working cross-border these different solutions may have different legal implications.

Privacy and Self-Sovereign Identity

More secure than centralized identity systems?

Self-sovereign Identity and Decentralized Identity may add a layer of security and control compared to centralized systems.

What are the specific risks and are there legal implications?

- Risk of encryption failing over time
- Risk of a private key becoming compromised
- Is SSI on a DLT equivalent to encrypting personal data with an unchangeable password?

Legal implications of on-chain governance

Every chain has off-chain governance

The most basic blockchain governance is the hard fork.

Blockchains including Bitcoin and Ethereum usually have off-chain governance to decide development and improvements. Others, including EOS integrate governance into their protocol.

- These arbitration-like governance mechanisms might not always comply with the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards
- Arbitration agreements might not be recognized in all jurisdictions

Aligning the legal governance with the technical from early days is an important first step for DLTs operating cross-border to avoid conflicts before they happen

Digital Signatures

Can we relate keys to persons?

Blockchains work with digital signatures employing a combination of public and private keys.

It is possible to attribute public keys to natural persons or legal entities by means of, for example, a Certificate Authority.

- There may be challenges related to personal information and GDPR
- A certificate and key are usually stored on devices. If the security of these keys become compromised, would this leave a signature or agreement open to legal challenges?
- What if there are multiple jurisdictions involved?
- Would digital signatures be vulnerable to advances in quantum computing?

Smart Contracts

Can they represent real contracts?

A smart contract allows for the definition and adoption of rules in order to perform transactions on a blockchain.

These can be designed to represent legal contracts in the real world, adding efficiency and trust to the process

- There exists the possibility of such a contract conflicting with mandatory law.
- Some legal provision of a coded smart contract might not be enforceable off-chain
- Remedies may need to be pre-set on-chain or off-chain

Trust in oracles and data inputs affects legal interoperability.

- Smart contracts can only access data securely on-chain
- If real-world contracts are represented, the data provided by oracles needs to be trusted
- Data collection and trustability must be rigorously defined from the beginning and flexible for changing off-chain situations

Multi-chain transactions

Adding to the complexity

Real-world transactions may involve multiple blockchains to complete

- Financial transactions may involve multiple cryptocurrencies or tokens
- Supply chain traceability may track the components of a product using multiple blockchain systems

In addition to the technical challenges there may be significant legal complexity in a multi-chain environment due to applicable law, differences in how immutability is handled between chains, and so on.

In multi-chain transactions we can have situations where parts of a transaction may be completed and immutable while other parts become blocked or reversed for legal reasons.

Potential contribution of UNECE

Managing cross-border issues

- Supporting the development of vocabularies and definitions for DLT Interoperability such as ISA2 Core Vocabularies.

- Collect understanding and create recommendations for cross border harmonization

- Develop guidelines to help smooth the transition to DLT interoperability

MINESPIDER

Thank you.

Any questions?

Nathan Williams, Founder & CEO

nathan@minespider.com