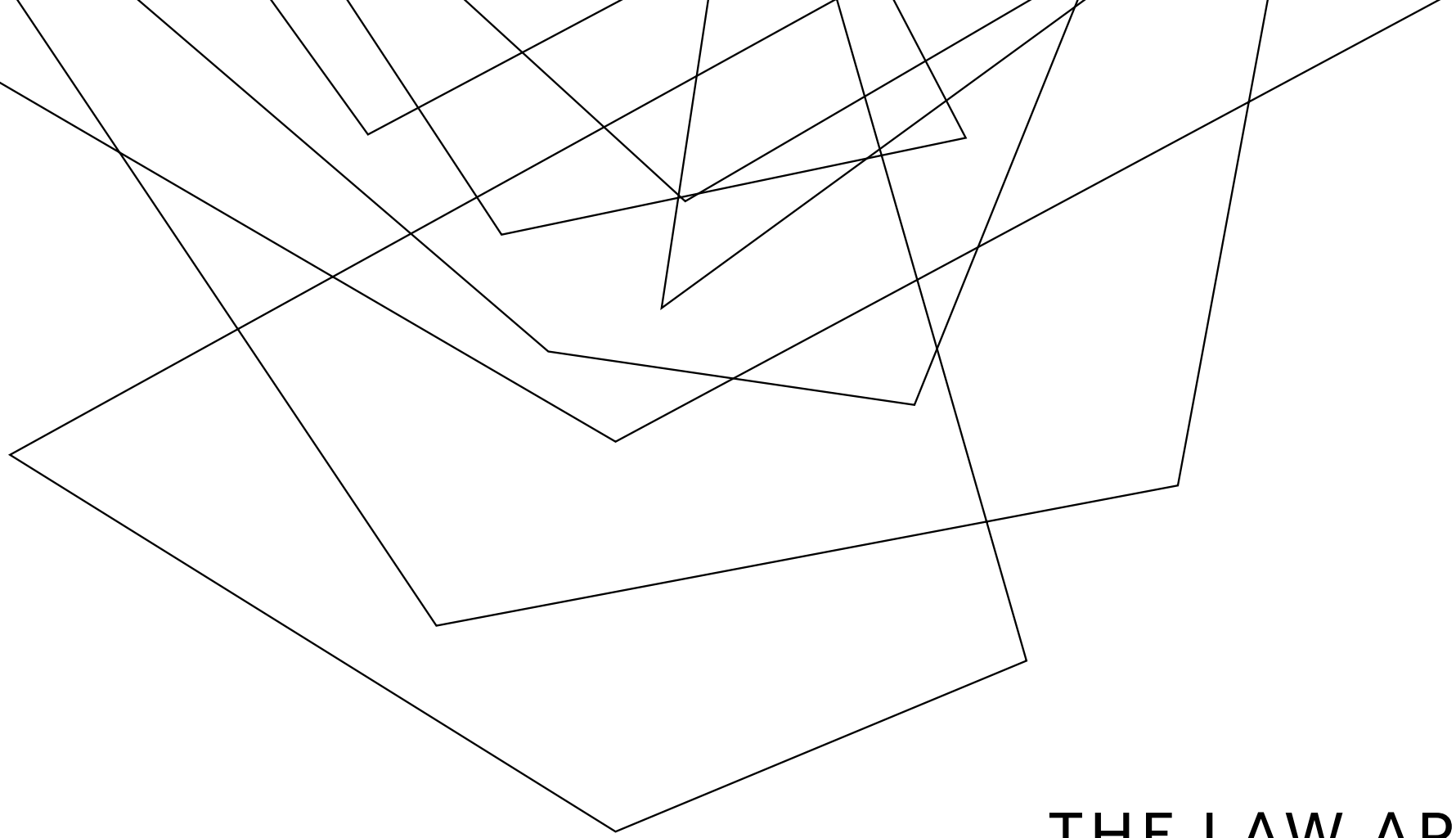


THE LAW APPLICABLE TO STAKING

Digital Assets and Private International Law Conference
April 11-12, 2024, University of Vienna

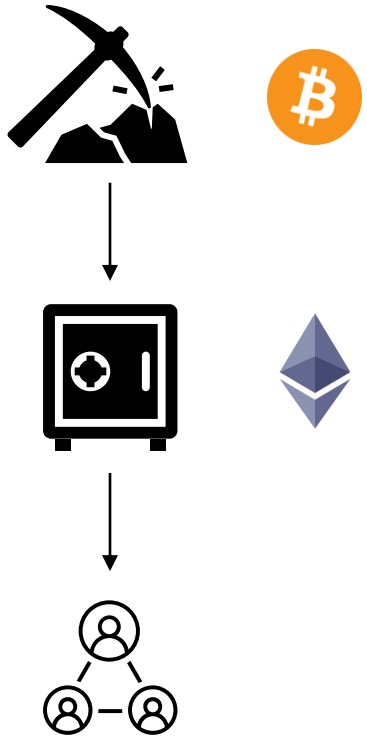
Fabio Andreotti, Bitcoin Suisse AG, Zug, Switzerland

OVERVIEW

- What is staking?
- Relevant relationships
- Applicable law
- Mandatory rules and ordre public
- Conclusions

WHAT IS STAKING?
BACKGROUND

- Proof of work (mining): **computing power**
- Proof of stake (staking): **assets**
- Proof of authority (authority): **identity and reputation**
- Combinations of the different models



WHAT IS STAKING?
DEFINITION

- **Staking**
  - Stakers *lock up* crypto assets *(stake)* in a blockchain protocol to participate in the consensus mechanism of the blockchain (i.e., validation and/or attestation of transactions and blocks)
  - The stake serves to ensure protocol-compliant behavior and thus blockchain security and integrity
  - In exchange for their services, the protocol distributes *staking rewards* to the participants in a programmatic manner

- **No cases of staking** are lock-ups of crypto assets for the purpose of ...
  - ... participation in other governance mechanisms of a blockchain protocol
  - ... DeFi lending (decentralized credit protocols)
  - ... DeFi liquidity providing (decentralized exchange protocols, DEX)

WHAT IS STAKING?
THE DIFFERENT TYPES

Users / customers have ...

Types	Technical infrastructure (validator node)	Power of disposal (“control”)	Digital / crypto assets
Self- / Solo-staking	x	x	x
Non-custodial Staking		x	x
Custodial Staking (incl. Sub-custodial Staking)			x

WHAT IS STAKING?
CRYPTOECONOMICS

Sanctions (*penalties* & *slashing*)

The mechanism serves to ensure the protocol-compliant addition of data to the blockchain

Example Ethereum:

- *Penalties* occur for missed attestations (e.g., downtime), but only affect the staking rewards (“lost profit”)
- *Slashing*, on the other hand, occurs in the event of actual misconduct (e.g., double signing) and therefore also affects the staked crypto assets. In addition, the participant is removed from the network (“forced exit”)

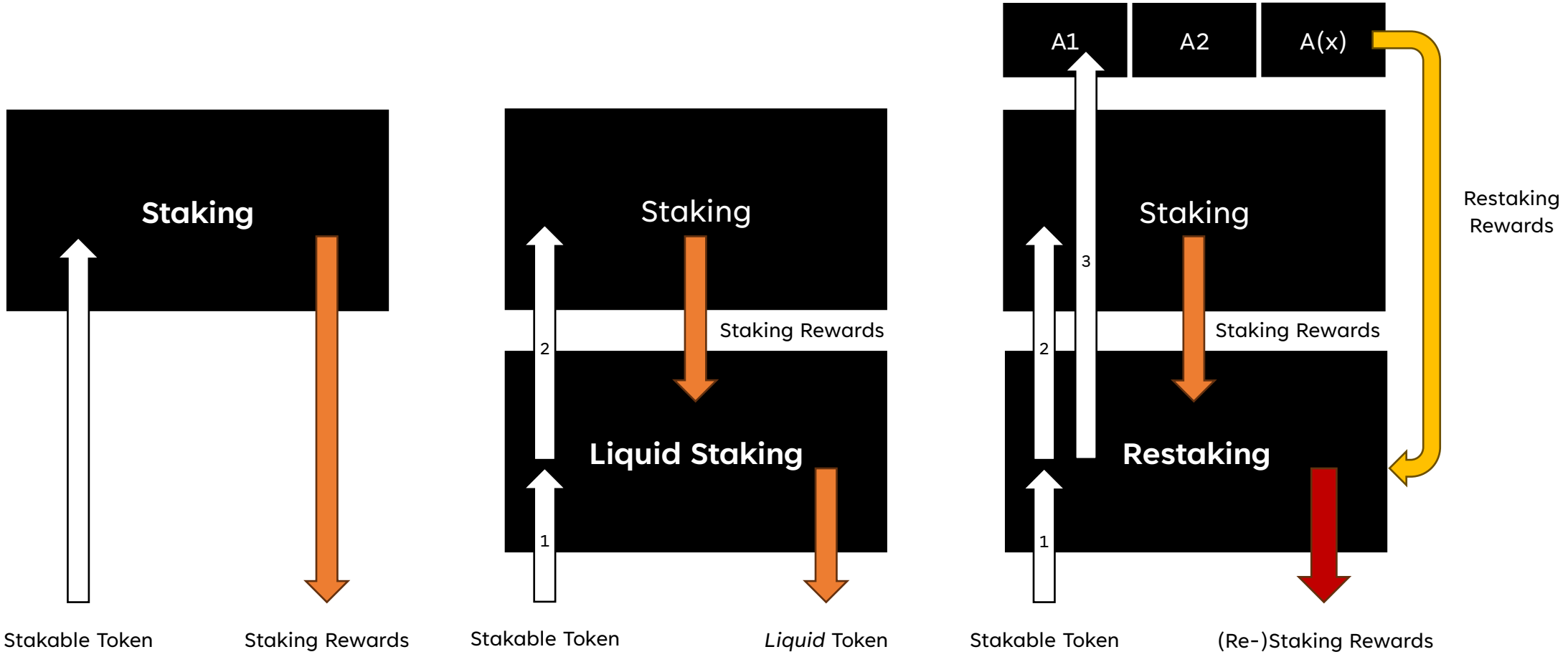
Termination periods (*exit lock*)

The mechanism serves to ensure the possibility of sanctioning violations of the protocol rules during a certain period after the end of staking, as such behavior may only be discovered at a later point in time

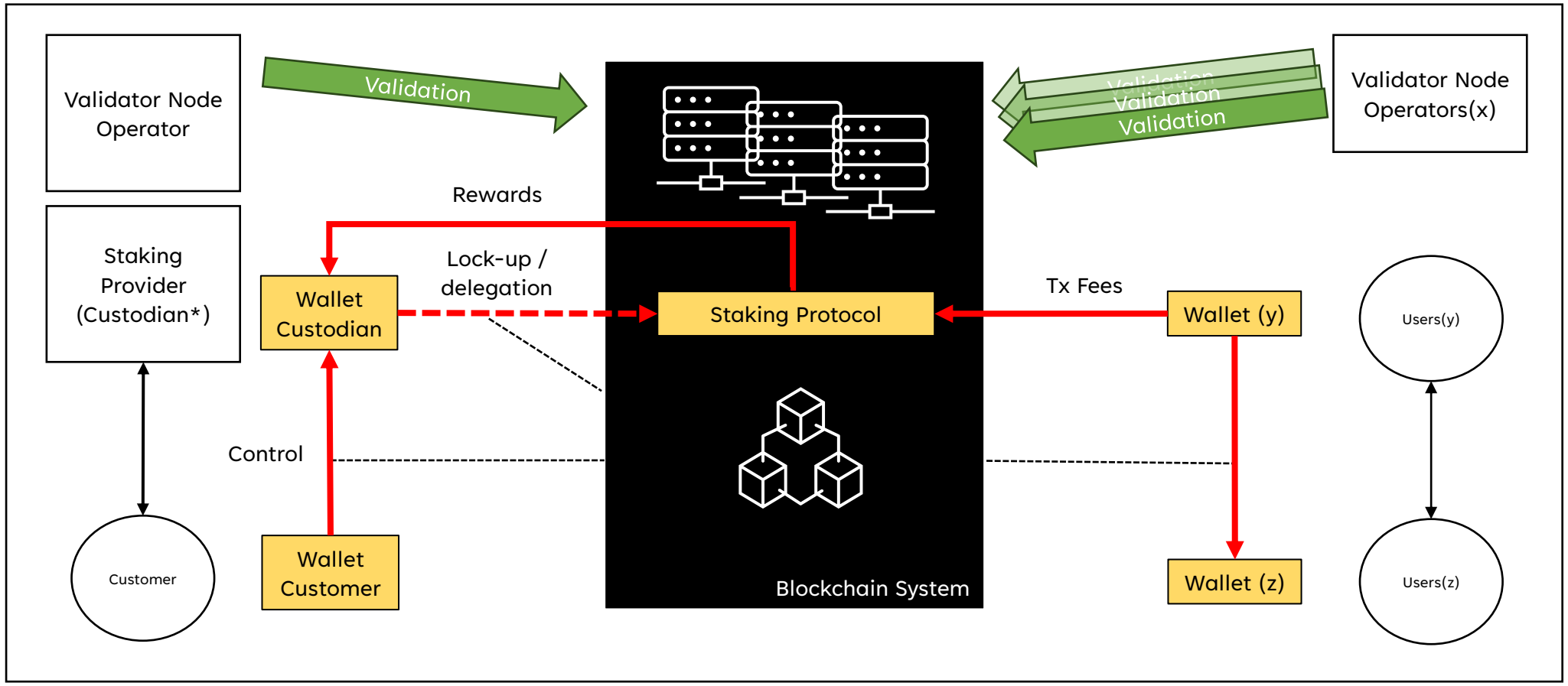
Example Polkadot:

- 28 days

WHAT IS STAKING?
LIQUID STAKING AND RESTAKING



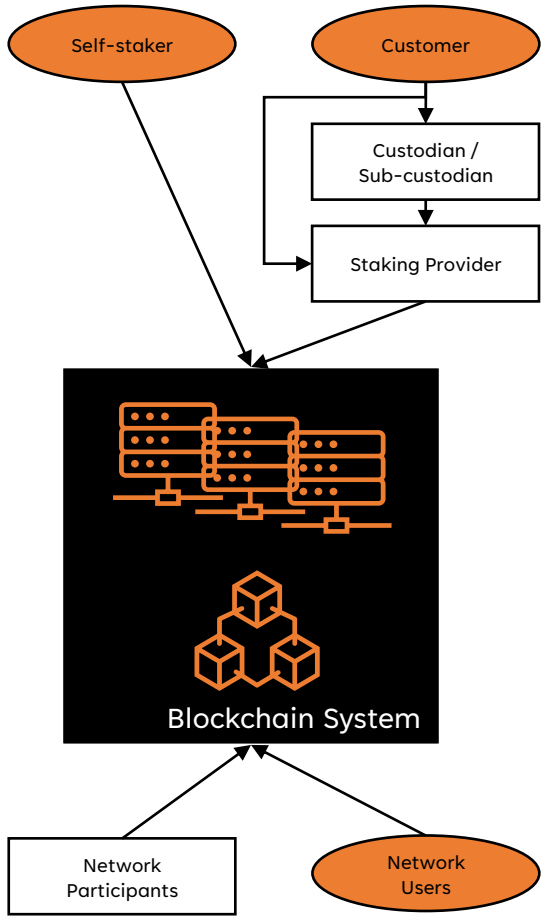
RELEVANT RELATIONSHIPS
LEGAL AND FACTUAL



*Use of sub-custodians relevant in practice

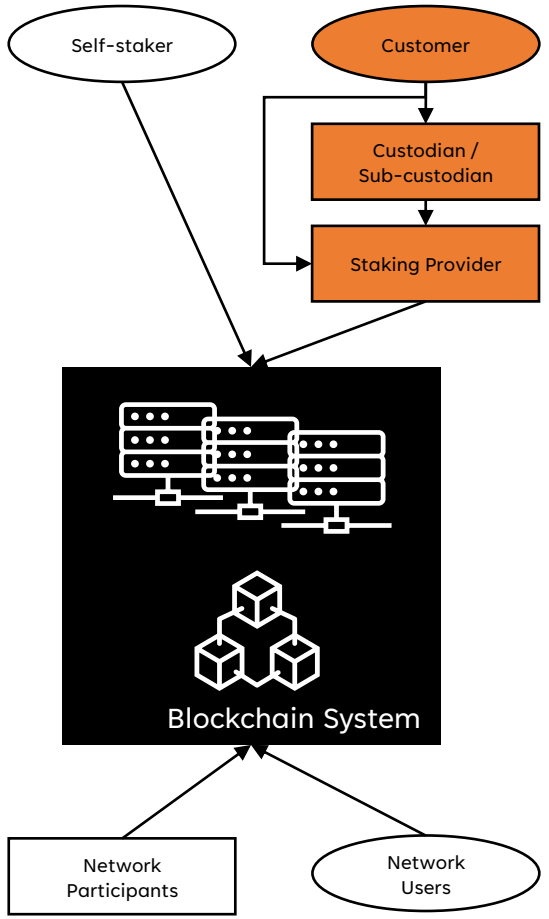
APPLICABLE LAW
"HOLDING" DIGITAL ASSETS

- **Challenges**
  - Permissionless blockchain systems as inherently global phenomena
  - Distributed hard- and software *and* decentralized governance
  - Programmatic software-based rules instead of traditional (legal) relationships
    - Example: Self- / Solo-Staking
  - Resulting in no obvious "closest connection" as per conflict-of-laws rules
    - Example: *SEC vs. Balina,* No. 1-22-cv-00950 (D.W.D. Tex. 2022)
    - Example: *Williams vs. Binance*, No. 22-972 (2nd Circ. 2024)
  - Existence and scope of proprietary and security rights to digital assets
- **Law applicable to "holding" digital assets**
  - *Lex situs* → not a helpful concept in a distributed data environment
  - *Choice of law* → useful in multi-layered setups (cf. intermediated security holdings), but practical challenges remain in bottom-up, polycentric systems



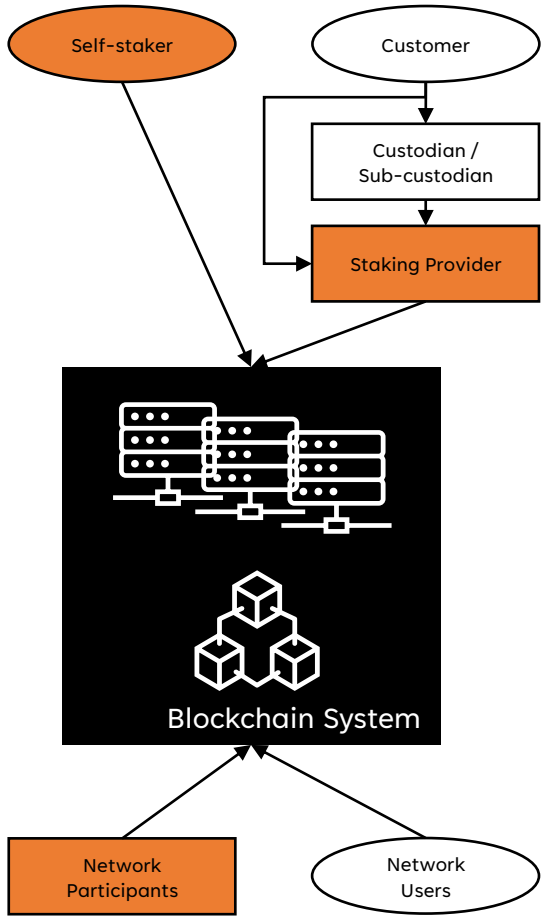
APPLICABLE LAW
STAKING THROUGH AN INTERMEDIARY

- **Background**
  - Custodial staking not only practically, but often also legally "anchored" in the custody agreement (cf. UNIDROIT DAPLP 10(3), 11(1))
    - Example: Under Swiss private law, a custodial staking agreement typically combines elements of a (regular) deposit (bailment), a simple mandate and/or a contract for work
  - Staking relationship (additionally) governed by a *separate* agreement
- **Law applicable to the staking relationship**
  - Custody → the law chosen by the parties (cf. UNIDROIT DAPLP 5(3))
  - Absent a choice of law → the law at the place of establishment of the custodian
  - The *same principles* should apply to the staking relationship
- **Law applicable to staked digital assets in the custodian's insolvency**
  - Applicable substantive domestic law determines whether customers may enjoy (quasi-)proprietary rights to digital assets in a custodian's insolvency
    - Example: Under Swiss civil and insolvency law, customer assets are protected in the event of a custodian's insolvency if custodian has committed to hold them available on individual or pooled blockchain addresses that are assigned to such customers in an internal register (cf. UNIDROIT DAPLP 13(2))



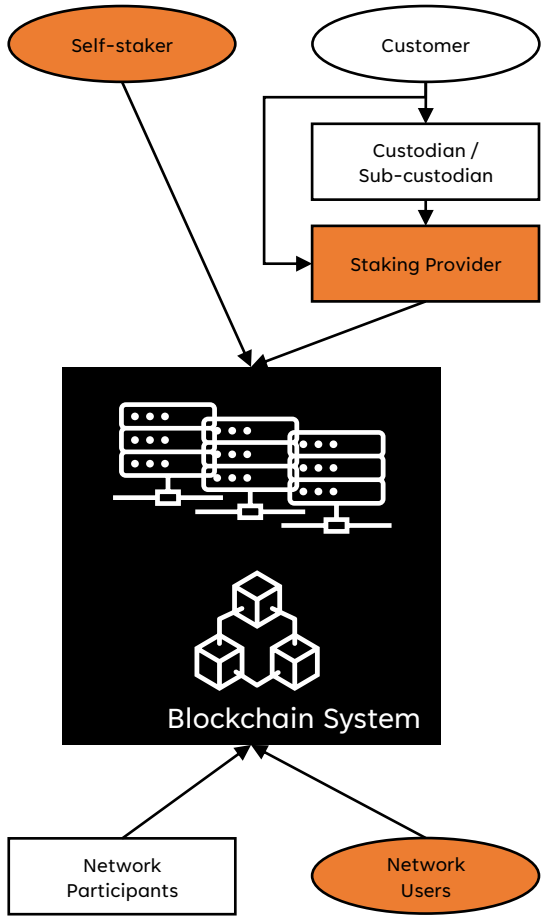
APPLICABLE LAW
PARTICIPATION IN CONSENSUS MECHANISM

- **Background**
  - Similarities between on-chain staking and *pledging / secured* transaction
  - In principle, *control* over digital assets remains with the staking party
    - Example: Ethereum staking requires depositing digital assets into the following smart contract address: 0x00000000219ab540356cBB839Cbe05303d7705Fa
  - Change of control in the event of *slashing*:
    - Control forfeited completely (digital assets are “burnt”)
    - Control transferred to some other address, such as a project’s “treasury”
  - Receipt of *staking rewards* generally programmatic according to the protocol rules
- **Law applicable to consensus participation**
  - Typically, *no contractual relationship* between network participants (despite reliance on the same or similar software protocols for consensus participation)
    - On the contrary, the programmatic rules and the *adversarial* character imply a non-contractual state
  - *Non-contractual* liability (tort) possible in the event of conduct contrary to the protocol rules



APPLICABLE LAW
PARTICIPATION IN BLOCK PRODUCTION

- **Background**
  - Stakers as *suppliers,* network users as "*consumers*" of block space
  - Staking rewards may consist of transaction fees paid by network users
    - Example: Ethereum execution layer rewards
  - Absent special interactions (off-chain communication channels, etc.), parties do not interact with each other *at all*, but are solely mediated by programmatic software-based rules
- **Law applicable to block production**
  - Typically, *no contractual relationship* between participants and users (despite "service character" of block production and fee payment)
  - If at all, party autonomy (choice-of-law rules) would make sense;
    - However, existing protocol software almost never provides for such choice
    - And lack of will to commit to such a choice (programmatic rules!)
  - *Non-contractual* liability (tort) possible in the event of conduct contrary to the protocol rules



MANDATORY RULES AND ORDRE PUBLIC

- **Background**
  - Regulatory law increasingly concerned with staking relationships, in particular to address potential customer protection issues
    - Example: FINMA Guidance 08/2023 “Staking”
  - Regulatory law may limit the conflict-of-laws options of the parties involved, including their choice of law
- **Examples from practice**
  - MAS custody requirements for digital payment token service provider including the restriction to stake on behalf of *retail* customers (April 2024)
  - Qualified custodian rules:
    - MiCAR provisions regarding the minimum content of custody agreements, the limitation of liability, and the segregation of crypto-assets in the event of insolvency (art. 75)
    - SEC proposal regarding safeguarding advisory client assets (February 2023)
    - SIX Swiss Exchange requirements for crypto-related ETP issuers (January 2024)
  - U.S. Treasury Department / OFAC, Sanctions against Tornado Cash (August 2022)

CONCLUSIONS

- Staking comes in various types and comprises different legal and factual relationships
- Custodial staking relationships should be treated in accordance with the UNIDROIT Principles on Digital Assets and Private Law proposed for custody agreements
- Existing private (international) law standards may not fully reflect the primarily non-legal relationships between the parties involved in consensus participation and block production
- Staking may also trigger financial market laws that may supersede certain aspects of the principles of private international law

HELPFUL RESOURCES

- UNIDROIT Principles on Digital Assets and Private Law, Rome 2023 (esp. Principles 5, 10, 11, 13)
- Lehmann Matthias/Held Amy/Krysa Felix/Prévost Emeric/Schinerl Fabian, Staking Your Crypto: What are the Stakes?, Journal of Business & Technology Law 2023, 53 ff.
- Bonomi Andrea/Lehmann Matthias/Lalani Shaheeza (eds.), Blockchain and Private International Law, Leiden/Boston 2023 (various chapters)
- Swiss Financial Market Supervisory Authority (FINMA), FINMA Guidance 08/2023, Staking, December 20, 2023
- Swiss Exchange Regulation AG, Additional Rules for the Listing of Exchange Traded Products, January 16, 2024
- Monetary Authority of Singapore (MAS), Guidelines on Consumer Protection Measures by Digital Payment Token Service Providers [PS-G03], April 2, 2024
- U.S. Securities and Exchange Commission (SEC) vs. Ian Balina, Complaint, Civil Action No. 1-22-cv-00950, September 19, 2022
- U.S. States Court of Appeals for the Second Circuit, Williams et al. vs. Binance et al., No. 22-972, March 8, 2024
- U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, August 8, 2022
- U.S. Securities and Exchange Commission (SEC), Proposed Rule, Safeguarding Advisory Client Assets, February 15, 2023
- Swiss Blockchain Federation (SBF), Zirkular 01/2023, Staking, April 3, 2024 (available in German only)
- Andreotti Fabio/Zimmermann Stephan/Prantl Florian, Custodial Staking. Eine Einordnung in das Schweizer Finanzmarktrecht, GesKR 2023, 333 ff. (available on request in German only)

THANK YOU

Fabio Andreotti

Deputy General Counsel, Bitcoin Suisse AG, Zug, Schweiz

fabio.andreotti@bitcoinsuisse.com