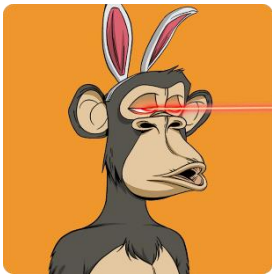
Seminar Law and Computer Science: Distributed Trust in Finance – Topic 5: NFTs

Handout for the presentation of May 13th, 2022

Terms

- Non-fungible tokens: Each is unique and cannot be switched as is.
- Fungible tokens: Each has the exact same value, can easily be switched with another. Example: Coins, Bills
- Semi-fungible tokens: Tokens that switch from being fungible to non-fungible (or vice-versa) during their lifetime. Example: Coupon for free hotdog. Before usage fungible, afterward non-fungible.
- Minting: Create an NFT entry with a transaction.
- Burning: Remove/Destroy an NFT with a transaction.
- IPFS: Inter Planetary File System
- Register Value Right: A special type of security (Wertpapier)

What is an NFT?




```
{"image":"ipfs://QmaPyRUapJjQXzqb3scCX5gycN6dyqFRY5phd64V97upAP",
"attributes":[
{"trait_type":"Background","value":"Orange"},
{"trait_type":"Hat","value":"Bunny Ears"},
{"trait_type":"Fur","value":"Black"},
{"trait_type":"Eyes","value":"Laser Eyes"},
{"trait_type":"Mouth","value":"Phoneme  ooo"}]}
```


How is an NFT created and stored?

Just like with other (fungible) tokens, NFTs are handled by a smart contract. Potential metadata is stored directly in the blockchain, but the assets are usually stored off-chain due to gas fees. The minimal part for an NFT is the ID.

What are the functions of smart contracts for NFTs?

If a standard has been implemented certainly the transfer and allowing others to sell them in the user's name. Additionally, creation (minting), destruction (burning), and further functionality is up to the user.

Are NFTs completely decentralized? Are there "gatekeepers" or centralized entities in the middle?

Depending on how the access to the chain with the contract is handled. Marketplaces have TOS, which if broken allows them to make NFT contracts unavailable. The storage is not completely decentralized in the sense that the asset is guaranteed to be available indefinitely.

Vulnerabilities?

Many pitfalls, most attacks happen through human error.

Register Value Right (Registerwertrecht)

Art. 973d OR

[1] Ein Registerwertrecht ist ein Recht, das gemäss einer Vereinbarung der Parteien:

1. in einem Wertrechteregister gemäss Absatz 2 eingetragen ist; und
2. nur über dieses Wertrechteregister geltend gemacht und auf andere übertragen werden kann.

[2] Das Wertrechteregister muss die folgenden Anforderungen erfüllen:

1. Es vermittelt den Gläubigern, nicht aber dem Schuldner, mittels technischer Verfahren die Verfügungsmacht über ihre Rechte.
2. Seine Integrität ist geschützt, indem es durch angemessene technische und organisatorische Massnahmen, wie die gemeinsame Verwaltung durch mehrere voneinander unabhängige Beteiligte, gegen unbefugte Veränderungen geschützt ist.
3. Der Inhalt der Rechte, die Funktionsweise des Registers und die Registrierungsvereinbarung sind im Register oder in damit verknüpften Begleitdaten festgehalten.
4. Die Gläubiger können die sie betreffenden Informationen und Registereinträge einsehen sowie die Integrität des sie betreffenden Registerinhalts ohne Zutun Dritter überprüfen.

[3] Der Schuldner hat sicherzustellen, dass das Wertrechteregister dessen Zweck entsprechend organisiert ist. Insbesondere ist sicherzustellen, dass das Register jederzeit gemäss Registrierungsvereinbarung funktioniert.

Case study

Person A creates an NFT of the monkey nature and sells it to Person B via an auction. Person C screenshots the monkey as shown on the website of the auction house and mints a new NFT with the image file and sells for a huge sum to person D.