Smart contracts from a legal perspective

Can Code Be Law?*

Frankfurt, 12. Dec. 2017,
Dr. Udo Milkau, Chief Digital Officer, Transaction Banking, DZ BANK

Myth and Marketing

Smart Contracts are said to be:

- “Turing-complete language”
- “custom sophisticated logic”
- “autonomous”
- “automated digital agreements”
- “self-executing contractual states”
- “self-enforcing legal obligations”
1. Simple contracts and communication of the declaration of will

**Protocol:**
- I point to a coke.
- Merchant put it on the counter.
- I put the money on the counter.
- Both take it (“DvP”).
- I get a bill.

**Protocol:**
- I press on the “coke” bottom.
- I put the money in the machine.
- Machine dispenses coke automatically & autonomously.

**Protocol:**
- I click on the “coke” icon.
- I accept terms and conditions.
- I press “buy” and select a payment method (e.g. SDD).
- The SEPA Direct Debit (SDD) is automatically & autonomously.
- Coke will be delivered (later).
2. Contracts and communication with a “Wrapper“

Exchange of offer and declaration of will between contractual parties.

*) see e.g. BGH 16.10.2012 X ZR 37/12: Offer and declaration of will in electronic communication does not result from presumed processing, but in such a way for the human party as he/she has to understand the declaration bona fide und according to ordinary usage.
3. Steps to a complex contract and intension of a contract

Freedom of contract

- Existing legal framework (superior legislation e.g. GDPR in European Union)
- Selection of applicable law (from Delaware via Zug to China; but also medieval “merchant law”)
- Selection of form (if not required by law)
- Selection of language (from English via Swahili to XML/ISO2022)
- Offer and declaration of will in the chosen form/language with identification of parties (e.g. eIDAS)
- **[active legal effect, depending on applicable law]**

→ Sense of contracts: disputes to be resolved ➔ examination, evaluation and interpretation by court*

  based on the *ex-ante* selected framework (in contrast to an *ex-post* “hard fork” by “community”)

→ Possibility for an “*ex tunc*” ruling that a contract was invalid from the outset

*) or by arbitration or medieval merchant courts
4. Smart contracts behind the "Wrapper"

Party A will pay Party B 1.- € on Jan 1, 2018.

**Mark-up language:**
```
<contract>
  <obligor> Party A </obligor>
  <obligation> will pay </obligation>
  <oblige> Party B </oblige>
  <amount> 1.- € </amount>
  <date> Jan 1, 2018 </date>
</contract>
```

**Script in Solidity language:**
```
pragma solidity ^0.4.11;
contract owned {
  function owned() { owner = msg.sender; }
  address owner;
  modifier onlyOwner {
    require(msg.sender==owner);
    _;
  }
  function close() onlyOwner {
    selfdestruct(owner);
  }
  modifier costs(uint price) {
    if (msg.value>=price) { _;
    }
  }
}
contract mortal is owned {
  function close() onlyOwner {
    selfdestruct(owner);
  }
}
```

**Ethereum Virtual Machine Byte Code**
```
0x60604052361561004b576060005260600090815260009058601560506090638182070035
```

(source: etherscan.io/address/0x07ee55aa48bb72dcc6e9d78256648910de513)

**Ethereum**
```
0x60604052361561004b576060005260600090815260009058601560506090638182070035
```

(source: etherscan.io/address/0x07ee55aa48bb72dcc6e9d78256648910de513)
5. Smart Contracts are a change of paradigm in software architecture with distributed code (scripts) with „if – then – else“ and „state machine“
6. Contracts in the context of a market society

- **Risk**: Bounded Rationality\(^1\) and Incomplete Contracts\(^2\)
- **Law and Trust**: Law as basis for (long-term) contractual relations\(^3\) and Trust as a tool to reduce social complexity\(^4\)
- **Standards**: A Lingua Franca is key success factor (e.g. LEI)
- **Governance**: Ex-ante provisions for Changes and Software Aging\(^5\)
- **Technology**: Sync. Atomic Protocol & Resilience by Redundancy

---

1. Grossman and Hart (1986), Hart and Moore (1990), and Hart (1995); but also: Gödel’s incompleteness theorems (1931/1951)
2. Interpretation of Contracts: see e.g. Prenn v Simmonds [1971] 1 W.L.R. 1381; Incomplete Contacts: O.E. Williamson’s work
Conclusion: „smart contracts“ on the blockchain are synchronised scripts with a status concept = “self-reconciling” protocols ...
… but require interoperable standards!
(illustrative; Nov 11, 2017)