Smart contracts from a legal perspective

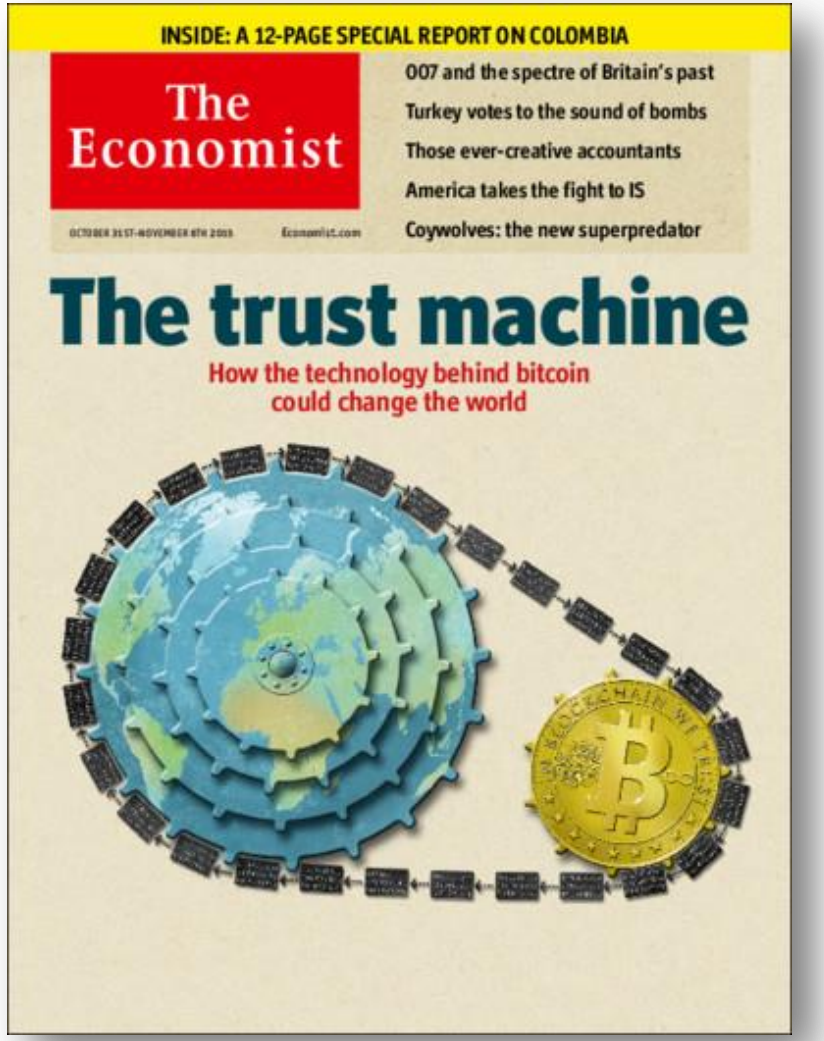
Can Code Be Law?*

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

see: Lawrence Lessig "Code Is Law - On Liberty in Cyberspace", Harvard Magazine, Jan. 1, 2000 (https://harvardmagazine.com/2000/01/code-is-law-html)

DZ BANK
Die Initiativbank

Myth and Marketing

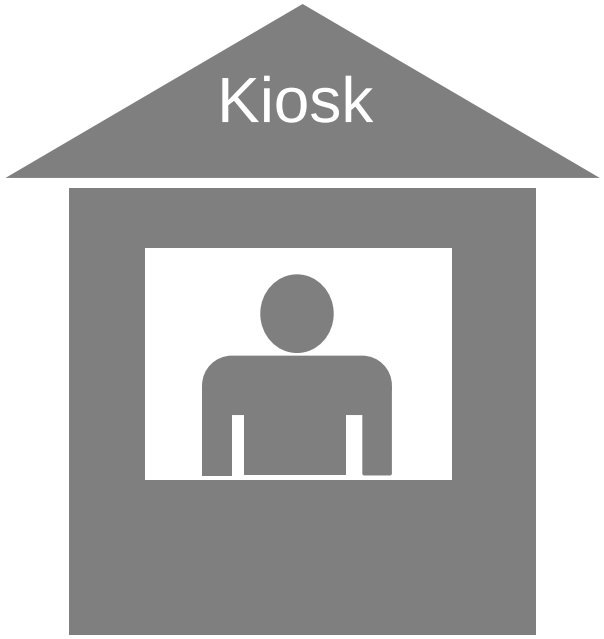


Smart Contracts are said to be:

- "Turing-complete language"
- "custom sophisticated logic"
- "autonomous"
- "automated digital agreements"
- "self-executing contractual states"
- "self-enforcing legal obligations"

DZ BANK
Die Initiativbank

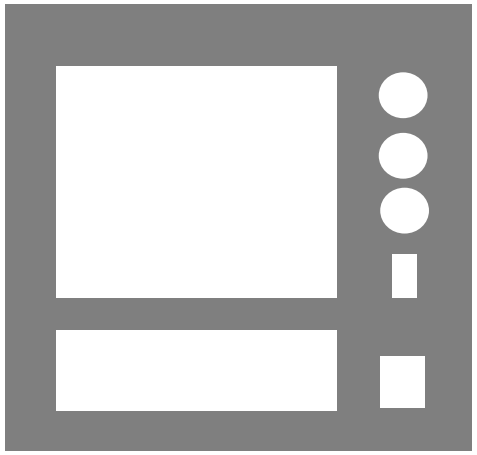
1. Simple contracts and communication of the declaration of will



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.

Vending Machine



Protocol:

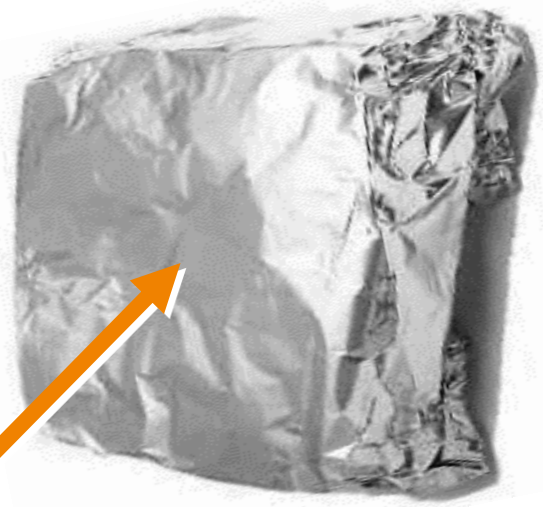
- I press on the “coke” bottom.
- I put the money in the machine.
- Machine dispenses coke automatically & autonomously.

E-Commerce

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 **Solidy** language:

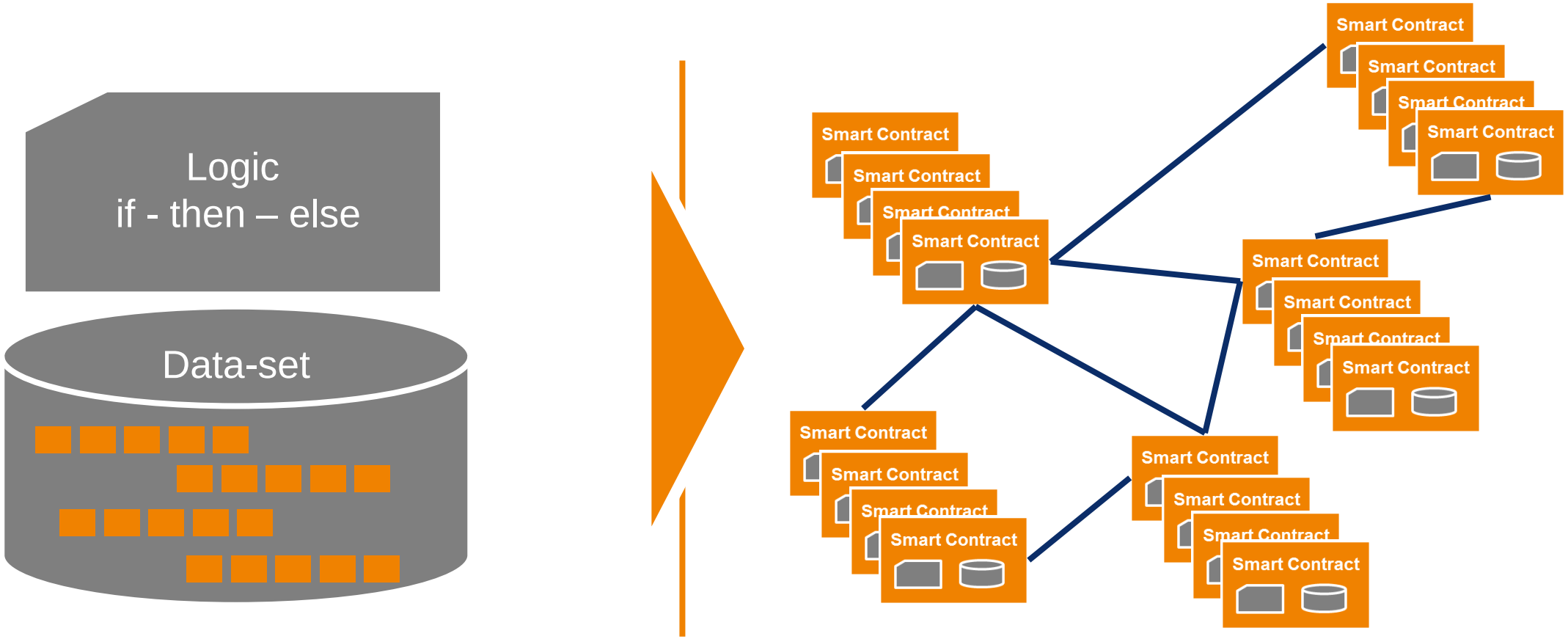
```
pragma solidity ^0.4.11;
contract owned {
    function owned() { owner = msg.sender; }
    address owner;
    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }
}
contract mortal is owned {
    function close() onlyOwner {
        selfdestruct(owner);
    }
}
contract priced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

Ethereum Virtual Machine Byte Code

```
0x6060604052361561004b5760e060020a600035046319e44e32811461008957
d4114610092578063b00606a5146100ad578063ba3ae0ce146100e5578063da9
011f575b6101dc600160a060020a0333166060908152346080527fe1fffcc4923d0
9a8bfc6cda04eb5b0d3c460751c2402c5c5cc9109c90604090a1565b6101de600
6101e860043560016020526000908152604090205460ff1681565b6101e860043
443560643560008481526002602052604081208054829081906001600160a060020a
561038e57610002565b6101fc60043560026020819052600091825260409091
820154928201546003909201546001600160a060020a0391821693929116845565b61
560243560008054600190810180835560001943014018606081815260c0100000
0000000006001600160a060020a038716908102608090815260948790526054832
260208190526040909720805473ffffffffffffffffffffffffffffffffffffffff19168a17815595860
850184905590815260a086905260c08590529192917fd0df5d45cd50ae0aaff901
d1d9722cd6a2ecee1589e7bf64cf837591a1505092915050565b005b606090815
b604080519115158252519081900360200190f35b606093845260809283526 0a
60c05290f35b6040518082600019168152602001915050604051809103 90f35b8
009054906101000a9004600160a060020a0316600160a060020a03166000846
054604051809050600060405180830381858888f193505050509050801561037
694ab2f443abe65d90aba86027f8c9ba2f44f1073bb89390c7ca0bf866a8360000
06101000a9004600160a060020a0316846001016000505485600301600090549
9004600160a060020a0316856040518085600160a060020a0316815260200184
183600160a060020a0316815260200182600160a060020a0316815260200194
60405180910390a1600260005060008960001916815260020019081526020016
0008201600061010 00a815490600160a060020a0302191690556001820160005
600282016000506000905560038201600061010 00a815490600160a060020a03
550505b8093505b505050949350505050565b606088815260ff88166080908152
260c087905260019160e0916020919081861 66161da5a03f1156100025750604
0160a060020a0381168452602092909252822054909250 60ff1615156103ea576
826003016000905490610100 0a9004600160a060020a0316600160a060020a03
56104af57818360030160006101000a815481600160a060020a0302191690830
7fa0cf8a24caec31ed7663626cd6d6ad687b5b0004a7a743af24aabc3665ae24d2
0009054906101000a9004600160a060020a0316846001016000505484604051 8
a060020a0316815260200183815260200182600160a060020a0316815260200 1
060405180910390a1610383565b81600160a060020a0316836003016000905 49
9004600160a060020a0316600160a060020a0316141561022c5761000256
```

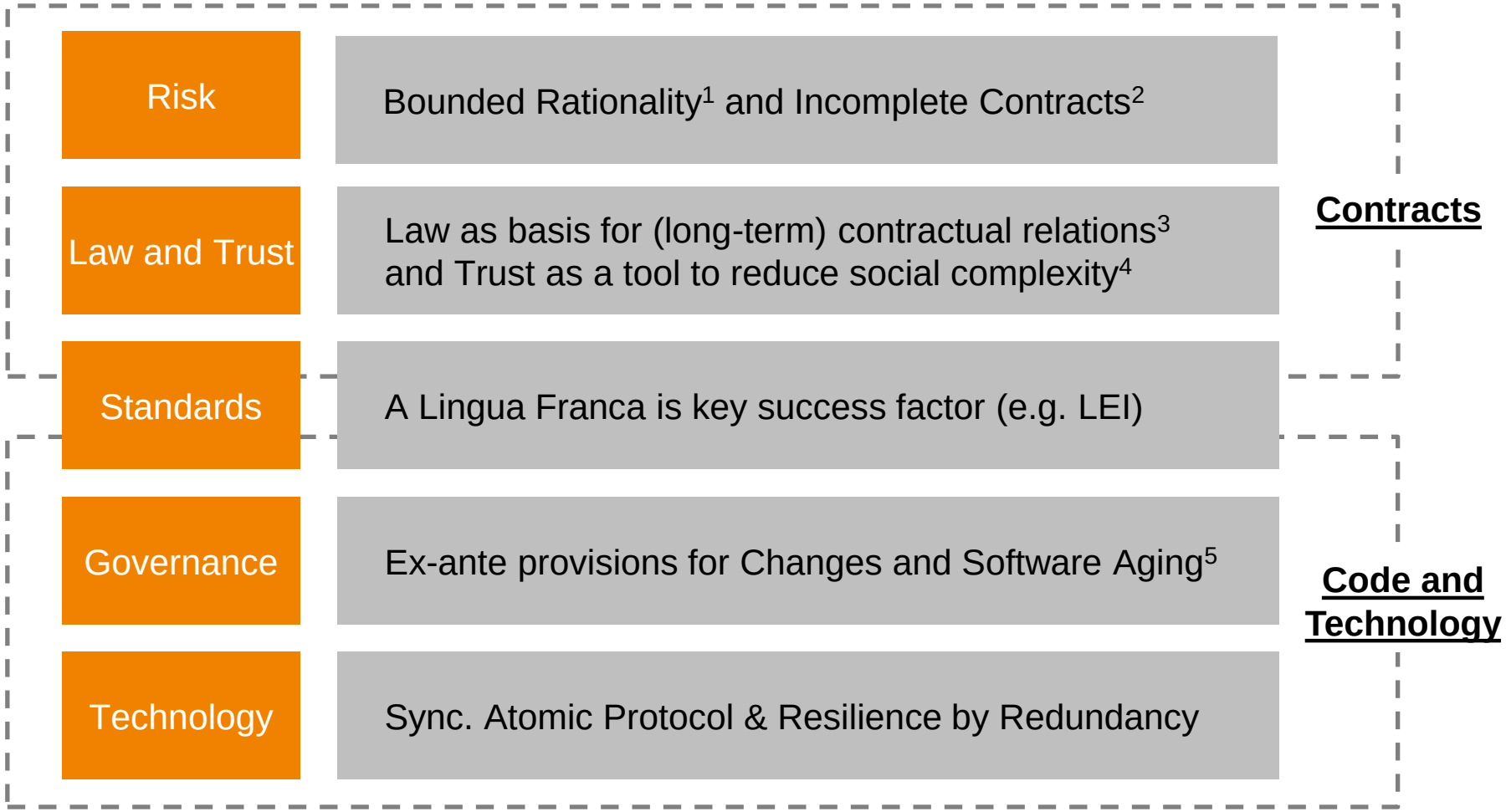
(source: hetherscan.io/address/0x07ee55aa48bb72dcc6e9d78256648910de513

5. Smart Contracts are a change of paradigm in software architecture with distributed code (scripts) with „if – then – else“ and „state machine“



DZ BANK
Die Initiativbank

6. Contracts in the context of a market society



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
3) Lessig, L. (2000). "Code is Law", Harvard Magazine, Vol. 1/2000
4) Luhmann, N. (1968). Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität
5) Parnas, D.L. (1994). Software aging, ICSE '94

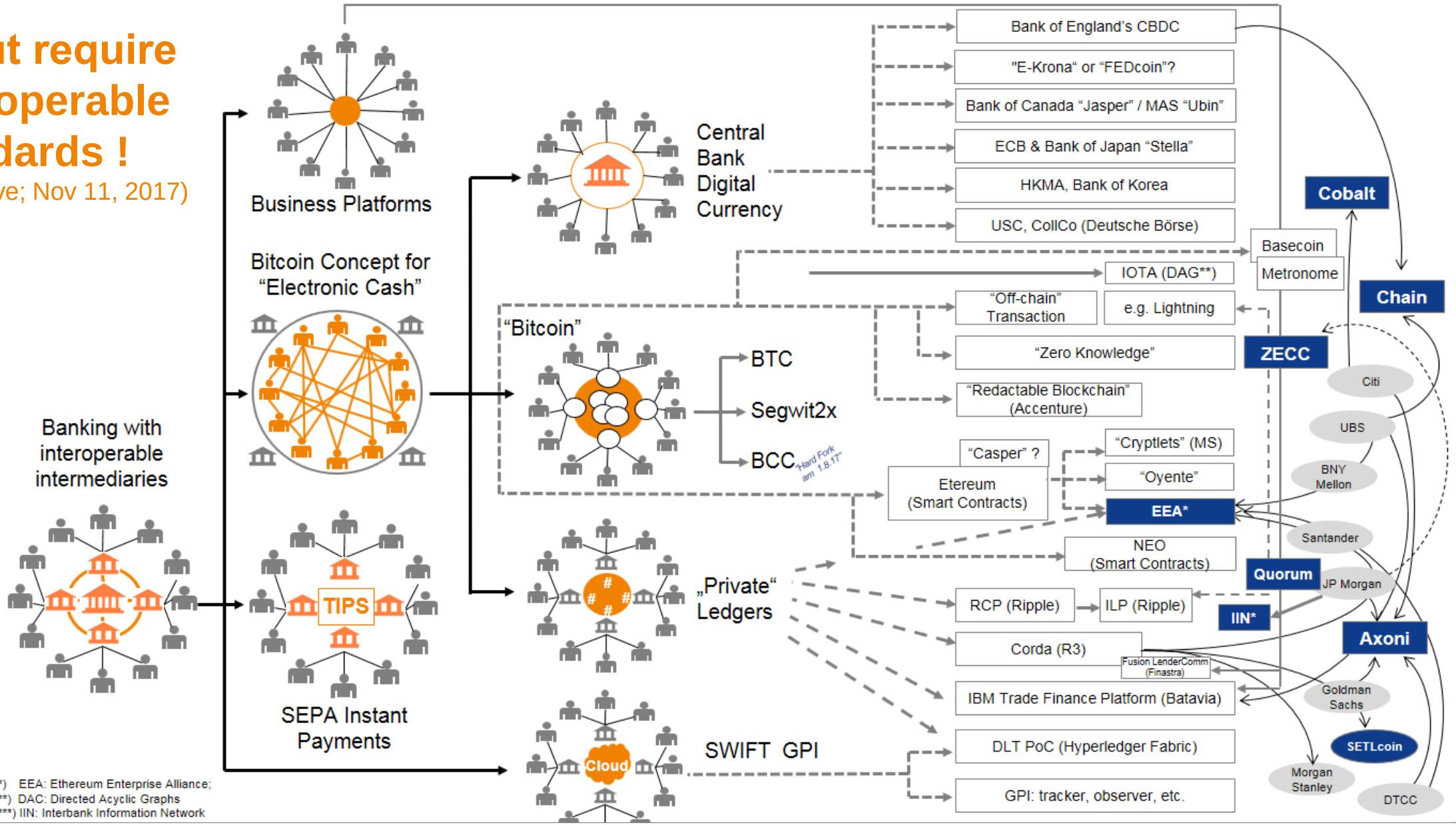
DZ BANK
Die Initiativbank

Conclusion: „smart contracts“ on the blockchain are synchronised scripts with a status concept = “self-reconciling” protocols …

Source: Siemens-Archiv

… but require interoperable standards !

(illustrative; Nov 11, 2017)



*) EEA: Ethereum Enterprise Alliance;
**) DAC: Directed Acyclic Graphs
***) IIN: Interbank Information Network

DZ BANK
Die Initiativbank