LegalTech #9

tomasz.**korwin-gajkowski**@p2p.systems

P2P.SYSTEMS

Agenda

1. Blockchain fundamentals
2. Blockchain vs DLT
3. Consensus algorithms
4. Blockchain vs DB
5. What are Smart Contracts and their limitations
6. Public vs private Blockchain
7. Blockchain and physical world

Blockchain fundamentals

“The blockchain is an ***incorruptible digital ledger of economic transactions*** *that can be programmed to record* ***not just financial transactions*** *but virtually everything of value.”*

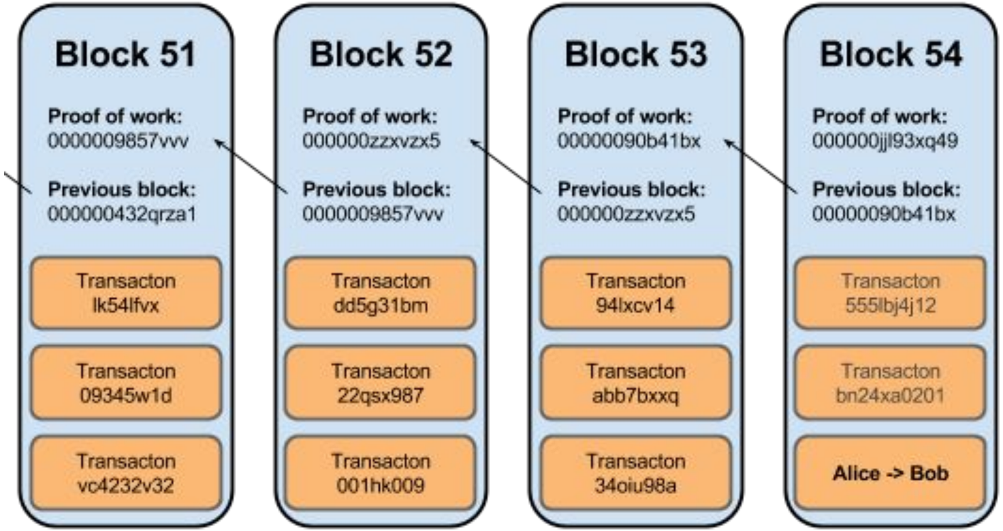
Don & Alex Tapscott

“Blockchains are ***politically decentralized*** *(no one controls them) and* ***architecturally decentralized*** *(no infrastructural central point of failure) but they are* ***logically centralized*** *(there is one commonly agreed state and the system behaves like a single computer)”*

Vitalik Buterin

Block - set of transactions

Blockchain - cryptographically linked blocks



Block 51

Proof of work:
0000009857vvv

Previous block:
000000432qrza1

Transacton
lk54lfvx

Transacton
09345w1d

Transacton
vc4232v32

Block 52

Proof of work:
000000zzxvzx5

Previous block:
0000009857vvv

Transacton
dd5g31bm

Transacton
22qsx987

Transacton
001hk009

Block 53

Proof of work:
00000090b41bx

Previous block:
000000zzxvzx5

Transacton
94lxcv14

Transacton
abb7bxxq

Transacton
34oiu98a

Block 54

Proof of work:
000000jjl93xq49

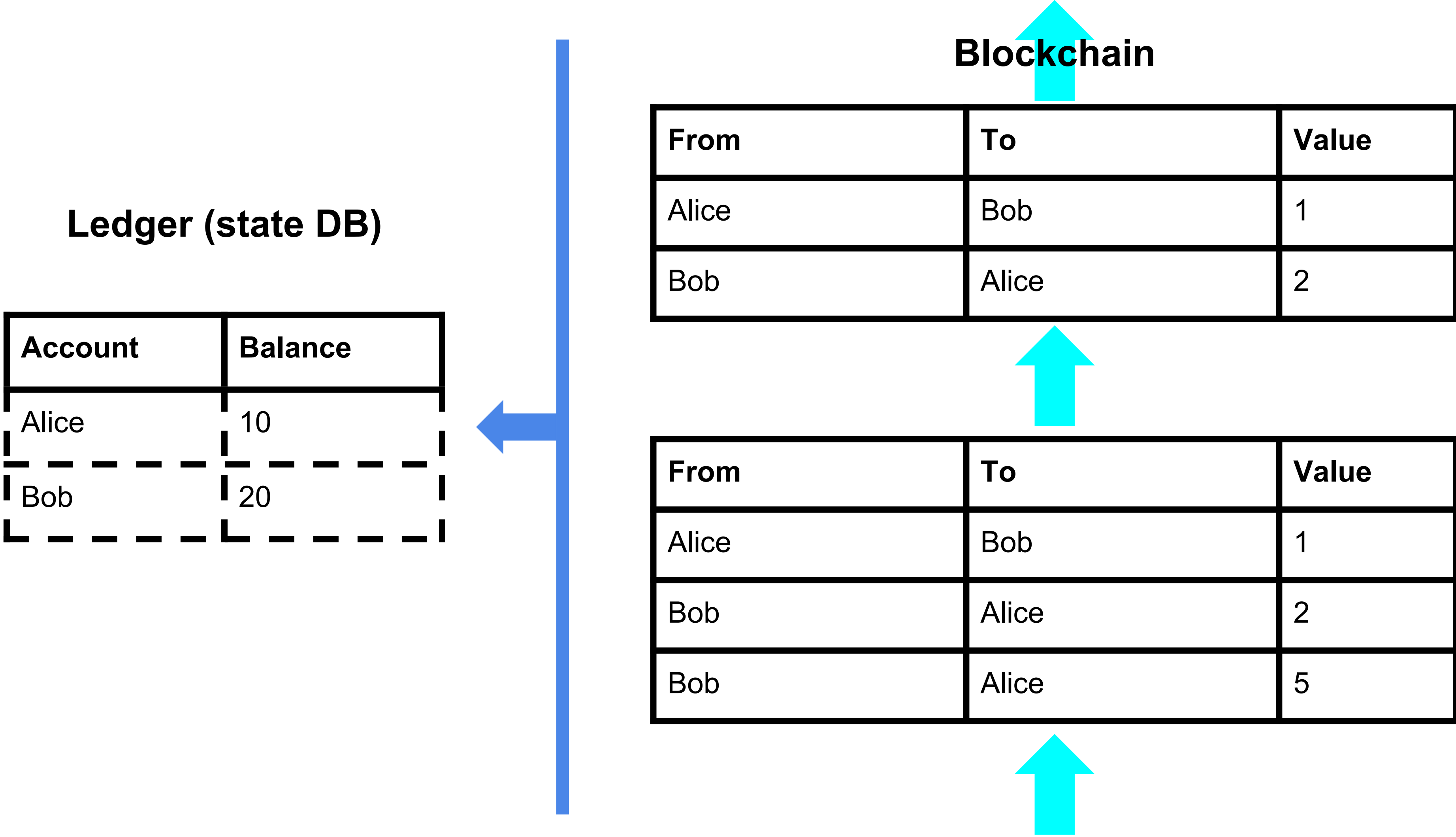
Previous block:
00000090b41bx

Transacton
555lbj4j12

Transacton
bn24xa0201

Alice -> Bob

Blockchain vs DLT



Ledger (state DB)

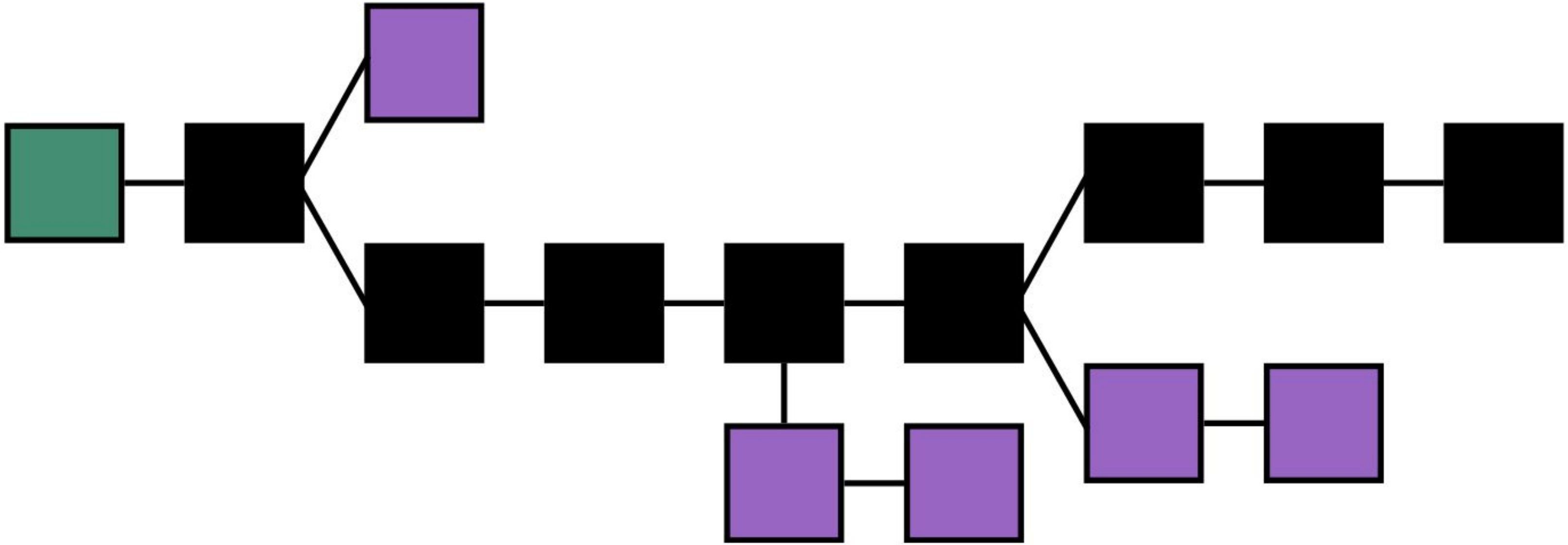
Account	Balance
Alice	10
Bob	20

Blockchain

From	To	Value
Alice	Bob	1
Bob	Alice	2

From	To	Value
Alice	Bob	1
Bob	Alice	2
Bob	Alice	5

Consensus algorithms



Consensus: longest and “strongest” chain considered valid

- Proof of Work **is not** a consensus algorithm
- It is an **anti-sybil attack** mechanism

Consensus algorithms:

- PBFT
- Ben-Or
- Tendermint/Cosmos
- Avalanche

Blockchain vs DB

Blockchain	**Database**
No admin with full control	Centralized control
Immutable transaction history	Possible to alter transaction history
No data privacy **(?)**	High level of data privacy
Low throughput **(?)**	High transaction speed

What are Smart Contracts and their limitations

*“**By using cryptographic and other security mechanisms, we can secure many algorithmically specifiable relationships** from breach by principals, and from eavesdropping or malicious interference by third parties, up to considerations of time, user interface, and completeness of the algorithmic specification.”*

Nick Szabo, 1994

- **Applications that run exactly as programmed** without any possibility of downtime, censorship, fraud or third party interference

- “**Code is law**”

Distributed Computer

- Blockchain network acts as a "Distributed Virtual Machine" (**DVM**) which

- **Combines logic with ledger** to achieve distributed automation of business processes

- Main advantage of Smart Contracts is **not automation** but the **decentralized execution environment**

Loan Collateral Smart Contract Example

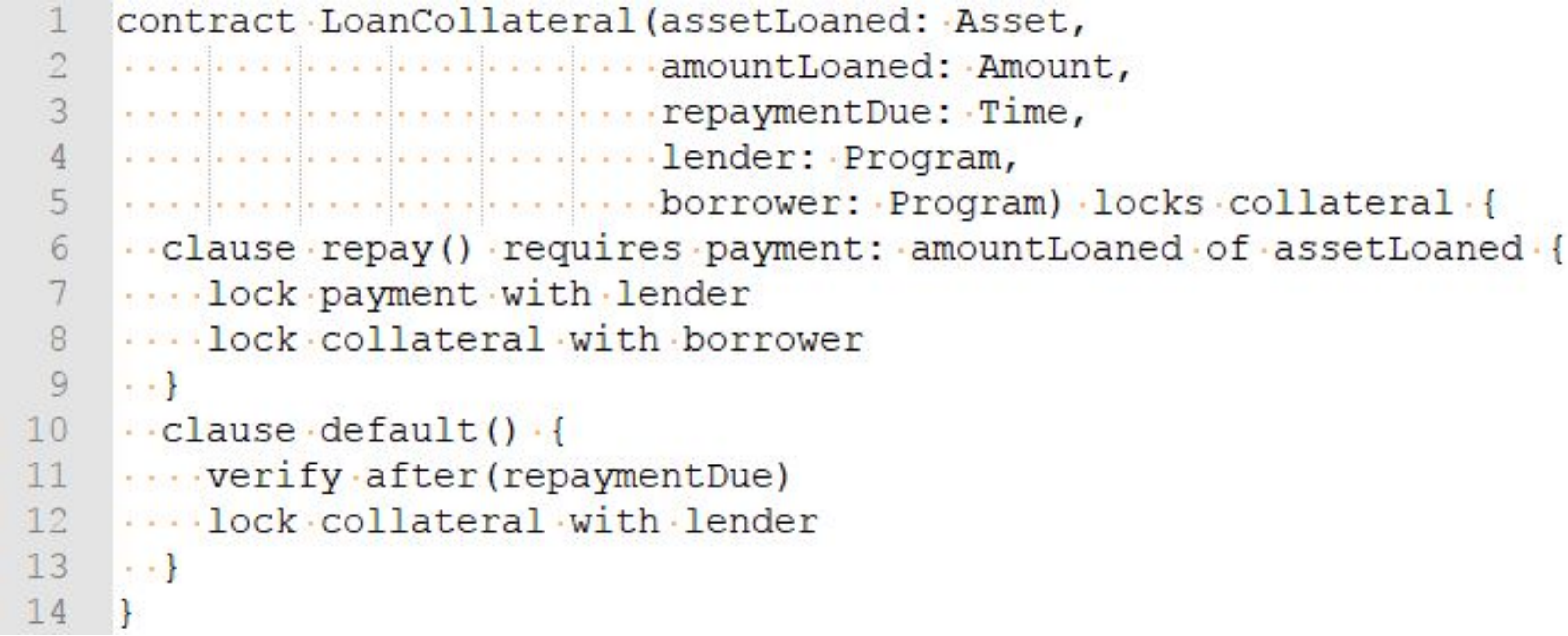
State:

- Asset loaned
- Amount loaned
- Repayment Due
- Lender
- Borrower

Behavior:

- Reapy
- Default

Loan Collateral Smart Contract Example



```
contract LoanCollateral(assetLoaned: Asset,
                        amountLoaned: Amount,
                        repaymentDue: Time,
                        lender: Program,
                        borrower: Program) locks collateral {
  clause repay() requires payment: amountLoaned of assetLoaned {
    lock payment with lender
    lock collateral with borrower
  }
  clause default() {
    verify after(repaymentDue)
    lock collateral with lender
  }
}
```

Limitations

- Non-upgradable (?)
- Limited number of operations
- Can’t access external data (?)
- No “self execution”
- Code must be deterministic

Public vs private Blockchain

(Internet vs intranet)

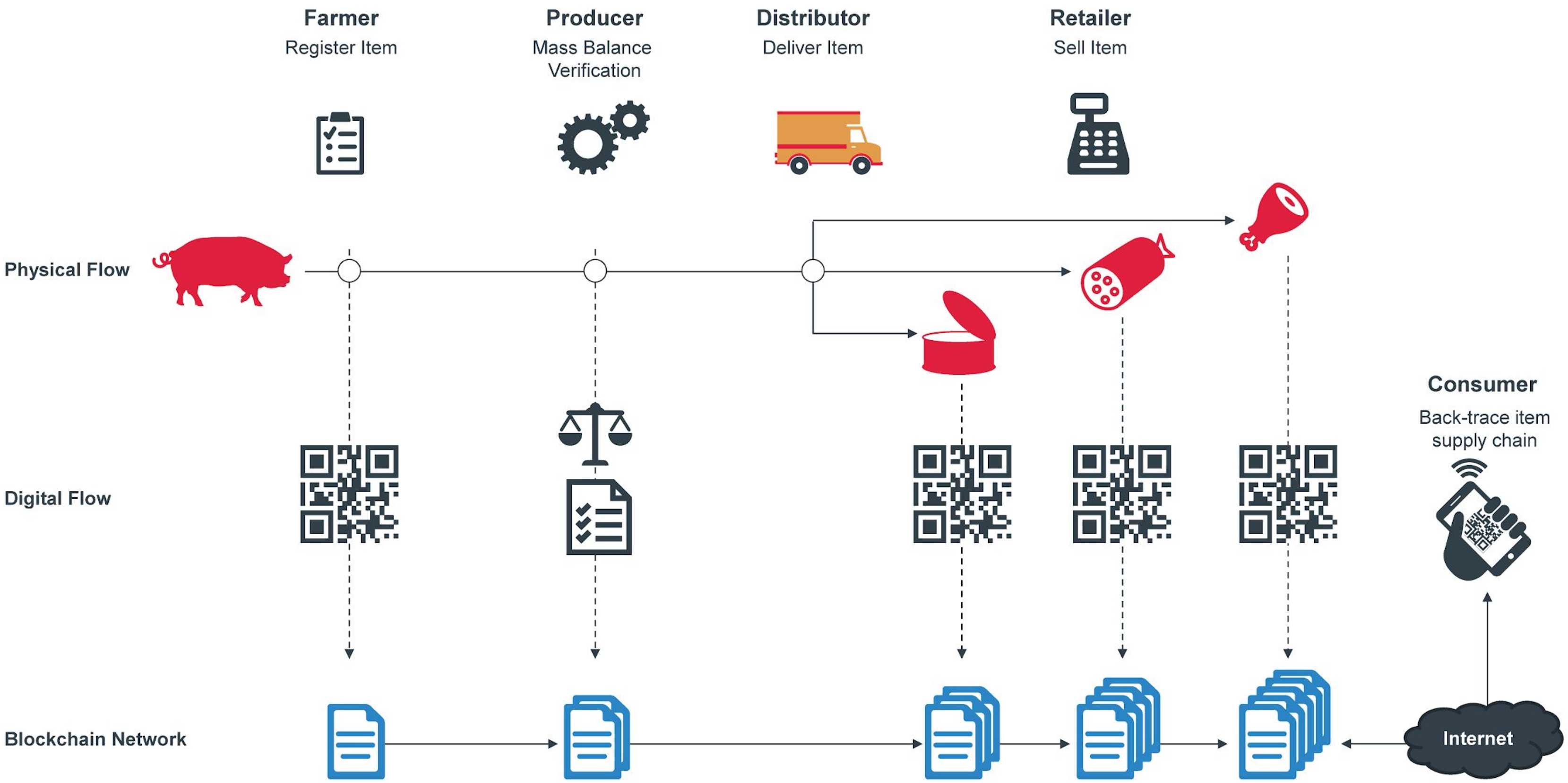
Public Blockchains:

- Everyone can join the network without a permission (**permissionless**)
- Client can choose a role in the system
- It is possible to join and leave the network anytime
- No need for user identification/authorization

Private Blockchains:

- Permission required to join the network (**permissioned**)
- User identification/authorization mandatory
- Predefined user roles
- No native token required

Blockchain and physical world



Problem: cost of “breaking” the identifier < value of the product

Thank you!

tomasz.korwin-gajkowski@p2p.systems

P2P.SYSTEMS