Technologie Blockchain – Überblick, Chancen & Potenzial

ECO: Konstituierende Sitzung der Kompetenzgruppe Blockchain

Wolfgang Prinz

Fraunhofer FIT
RWTH Aachen

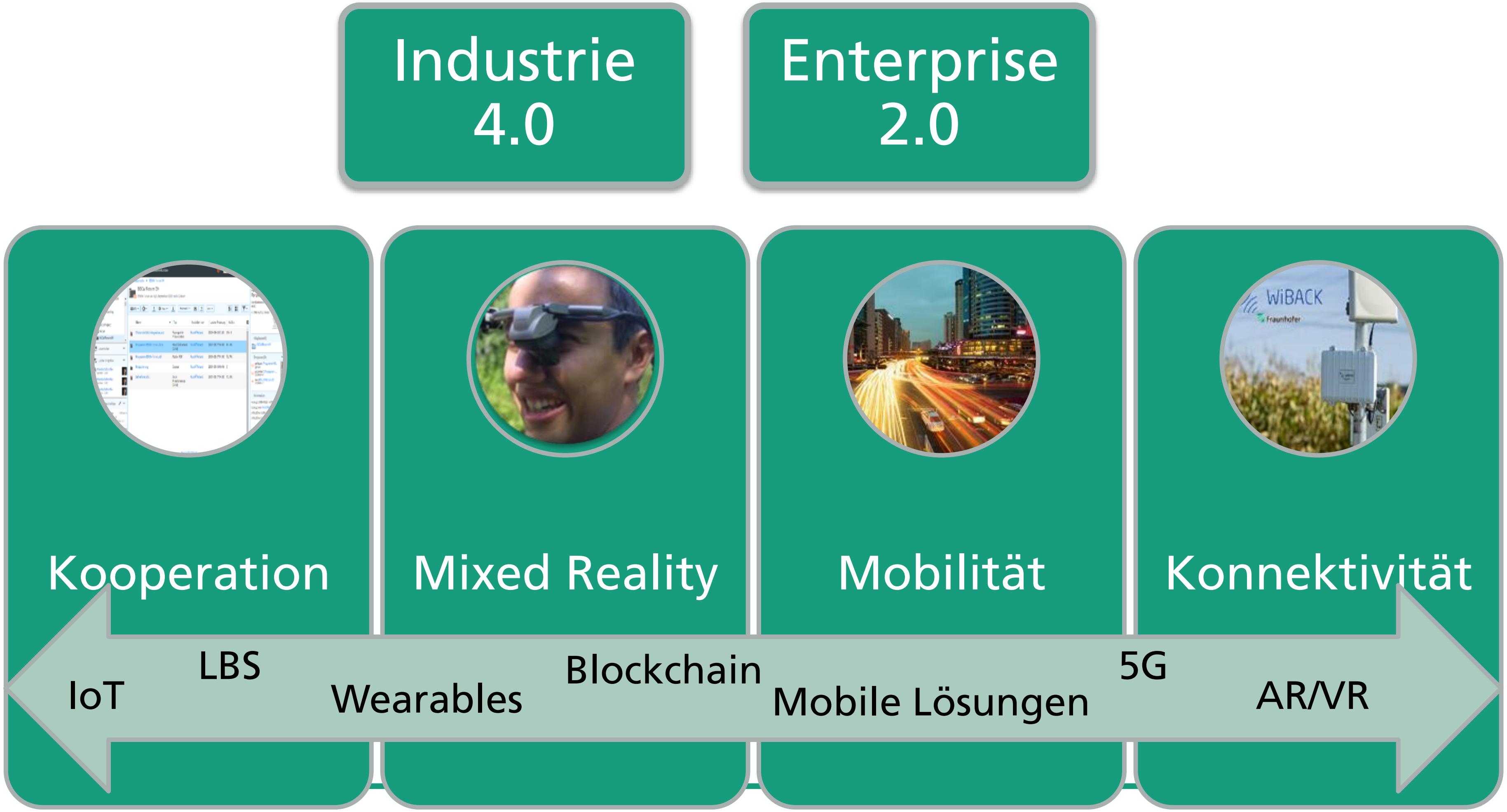
13. Dezember 2016

Schloss Birlinghoven

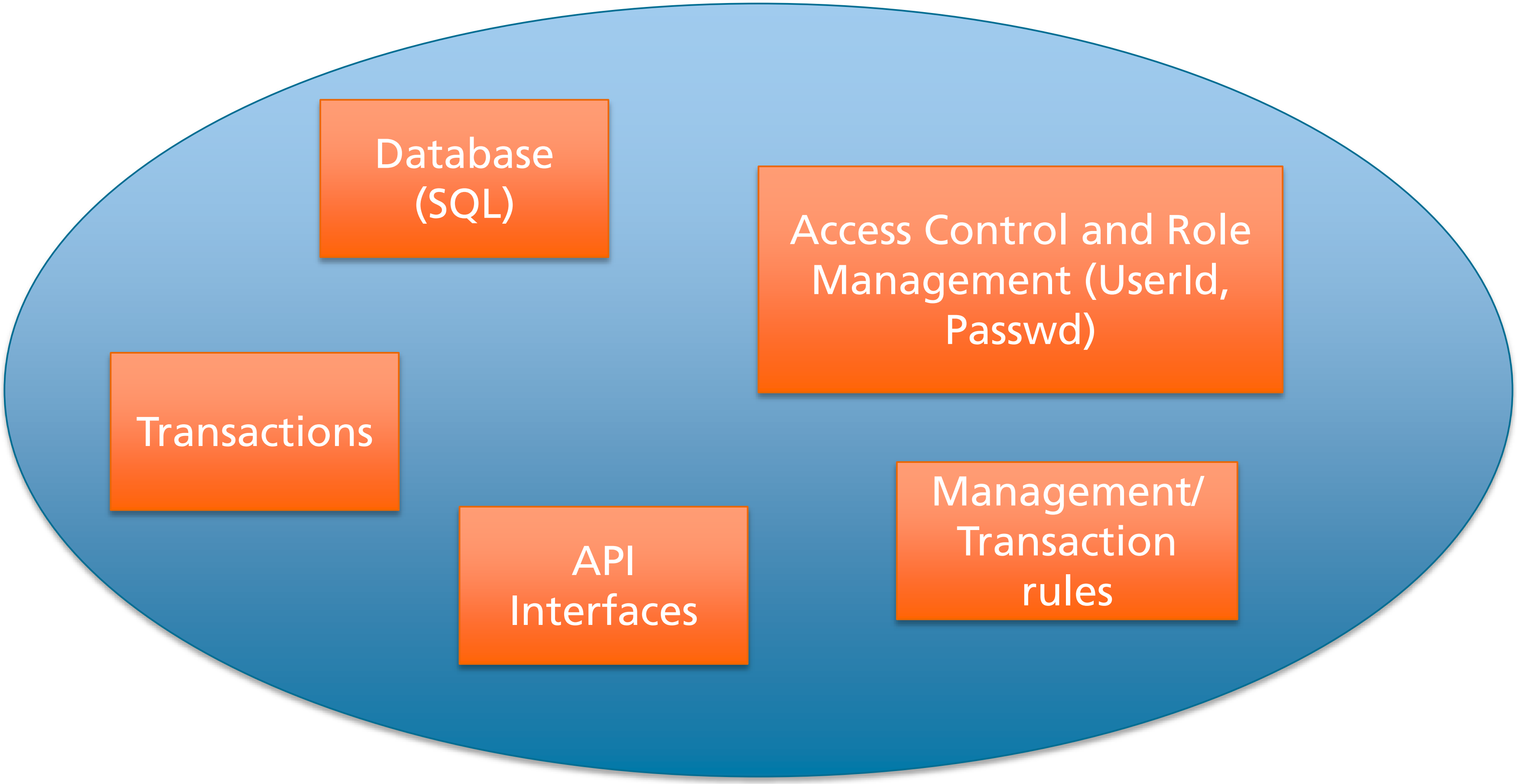
Gefällt mir http://www.facebook.com/fraunhofer.fit

Fraunhofer
FIT

Fraunhofer FIT
Kooperative Lösungen für Herausforderungen der Digitalisierung



Building blocks of a classic legder



Database (SQL)

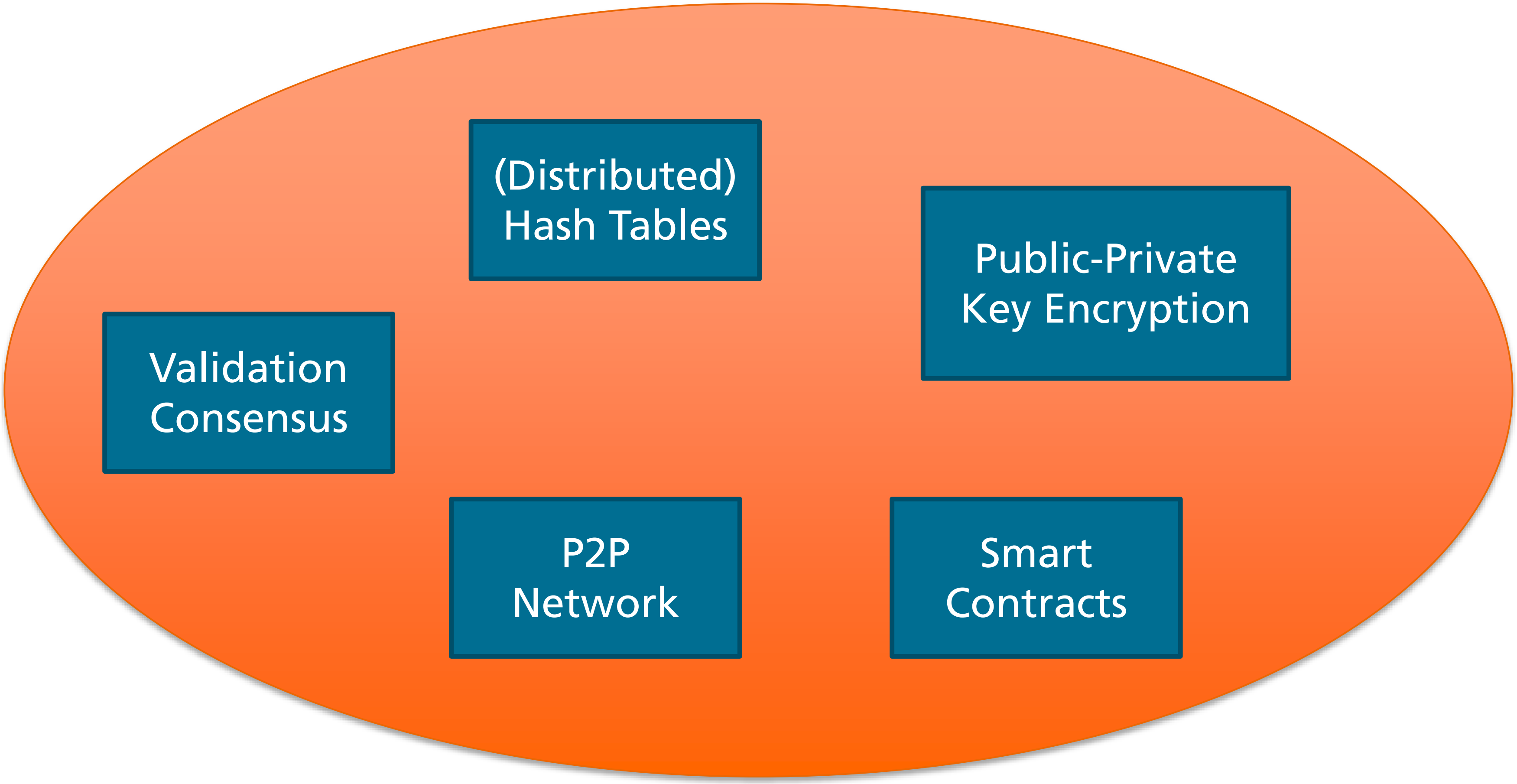
Access Control and Role Management (UserId, Passwd)

Transactions

Management/ Transaction rules

API Interfaces

Building blocks of a distributed legder - Blockchain


(Distributed) Hash Tables

Public-Private Key Encryption

Validation Consensus

P2P Network

Smart Contracts

Authentication and Authorization in a Blockchain

- Public / Private Key Mechanisms
  - Authentication towards the system
  - Identification of transaction source and destination
  - Encryption

https://www.bitaddress.org

- How to handle and remember the keys?
- How to avoid loosing the keys?

- Pseudoanonymization is not privacy!

- Who is managing the Identity-Directory of the IoT?

When did you send your last digitally signed or encypted email?

Data Distribution and Storage in a Blockchain

P2P Network

- Flexible
- Dynamic
- Open
- Replicated
- Difficult to control
- Difficult to attack
- Unpermissioned

Centralised/distributed database

- Controllable
- Easier to attack
- Limited replication
- Access API vs. Participation
- Permissioned

Distributed Hash Table

- Integrity
- Chaining
- Payload linkage

Validation of Transactions in Blockchains – Consensus building

- **Proof of Work**
  - Validation by solving a mathematical problem, e.g. finding the right random number to satisfy a specific condition
  - Requires computing power, energy, time
  - *E.g. Bitcoin, Ethereum*
- **Proof of Stake**
  - Validation by those nodes that hold larger amounts of money – „trust the bosses“
    - The more value a node owns, the higher is the chance to be selected Participants need to bed on a validation to avoid multiple validations on sub-chains
  - Faster, more trust based
  - *E.g. Peercoin, NXT*

Validation of Transactions in Blockchains – Consensus building

- **Lottery Protocol**
  - Randomly selected nodes perform the validation
  - Requires a trusted lottery mechanism – hardware?
  - E.g. Sawtooth Lake: Proof of elapsed Time: Intel® Software Guard Extensions (SGX) → SGX computes random waiting time – participant with shortest time may validate.
- **Explicit Validation Nodes**
  - Selected nodes have the right to validate
    z.B. BigchainDB, erisDB
  - Permissioned access to the Blockchain

A combination of all methods is also possible!

Smart Contracts turn a passive Blockchain in widely distributed computing ecosystem

- **Smart Contracts are**
  - represented as programm code.
  - represented as scripts within the transactions.
  - executed within the blockchain system.

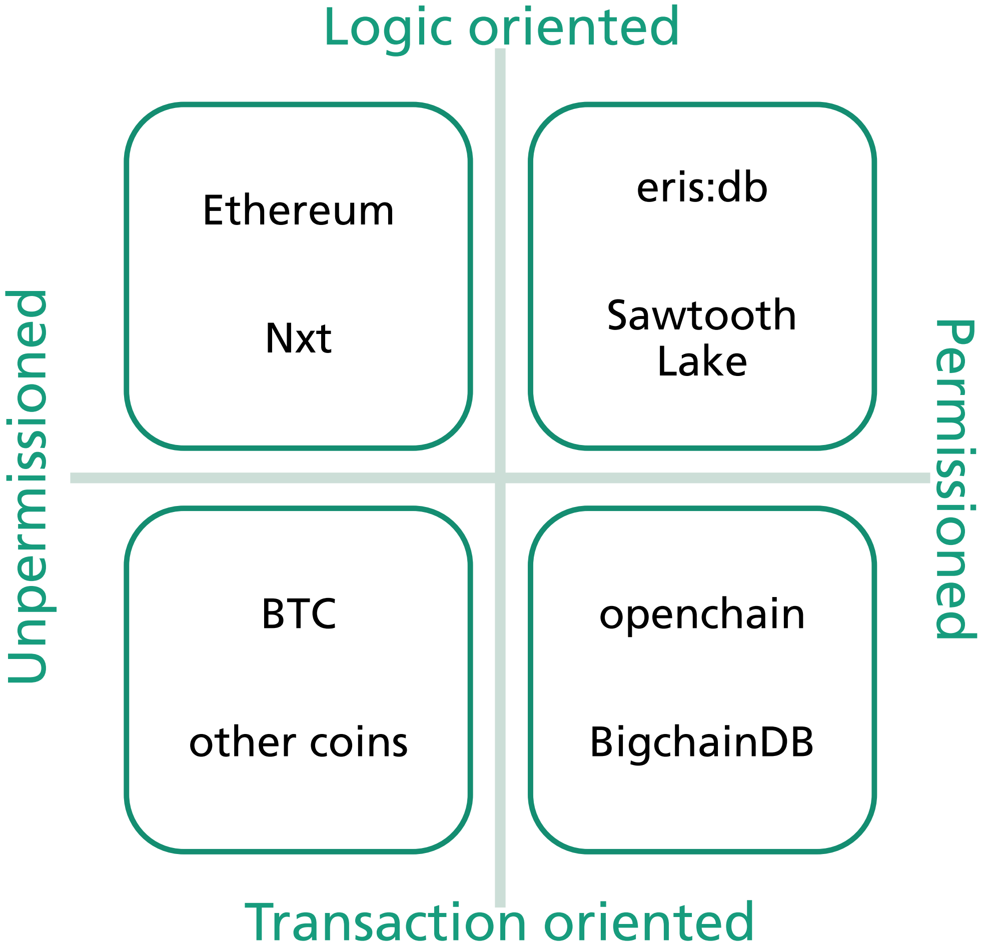
- **Smart Contracts**
  - enable the creation of a new ecosystem.
  - make the blockchain IoT ready.

- **Smart Contracts may also become a nightmare**
  - of administration.
  - of uncontrolled/able and irreversible autonomous activities.
  - *Remind me on email-worms*

Building Blocks of Blockchains

Public-Private Key Encryption	• Authentication of transaction partners • Transaction signatures and encryption
P2P Network	• Transaction distribution • Scalability
(Distributed) Hash Tables	• Payload references • Block-Chaining
Validation	• Proof of Work • Proof of Stake
Smart Contracts	• Negotiation • Contract Execution

The Blockchain Design Space



Logic oriented

Unpermissioned

Ethereum

Nxt

eris:db

Sawtooth Lake

Permissioned

BTC

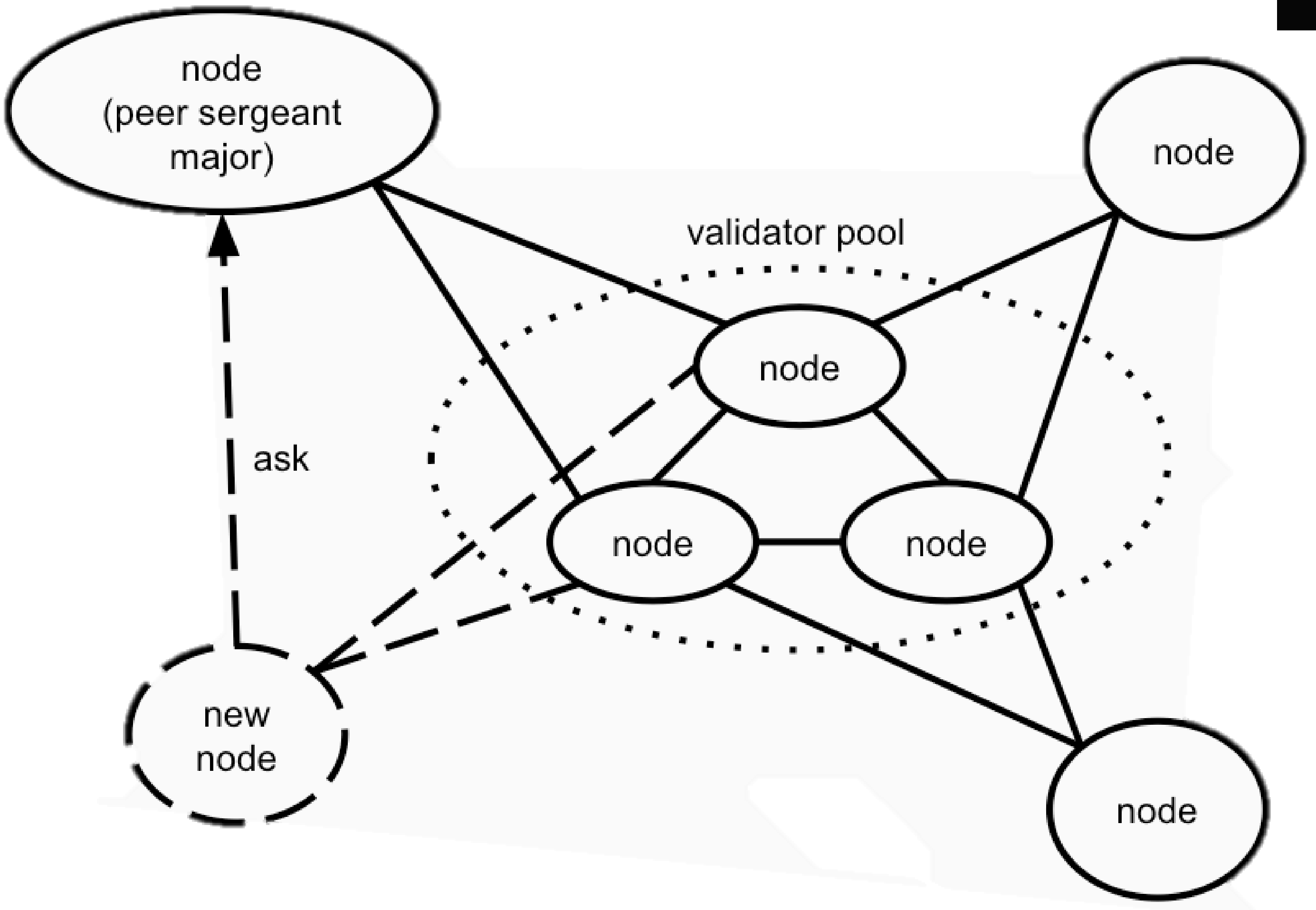
other coins

openchain

BigchainDB

Transaction oriented

Eris:db – a permissioned logic oriented Blockchain

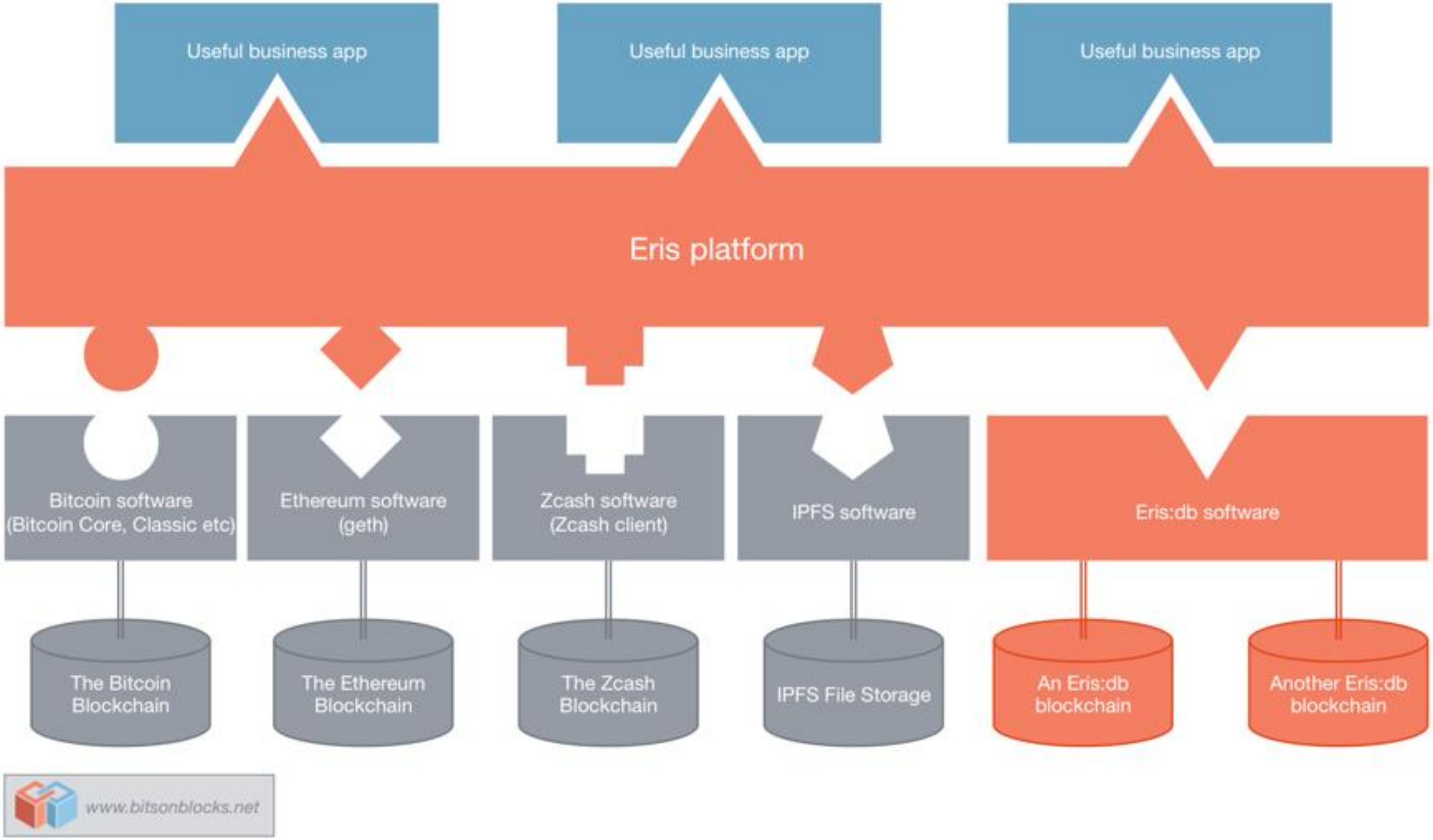


Logic oriented

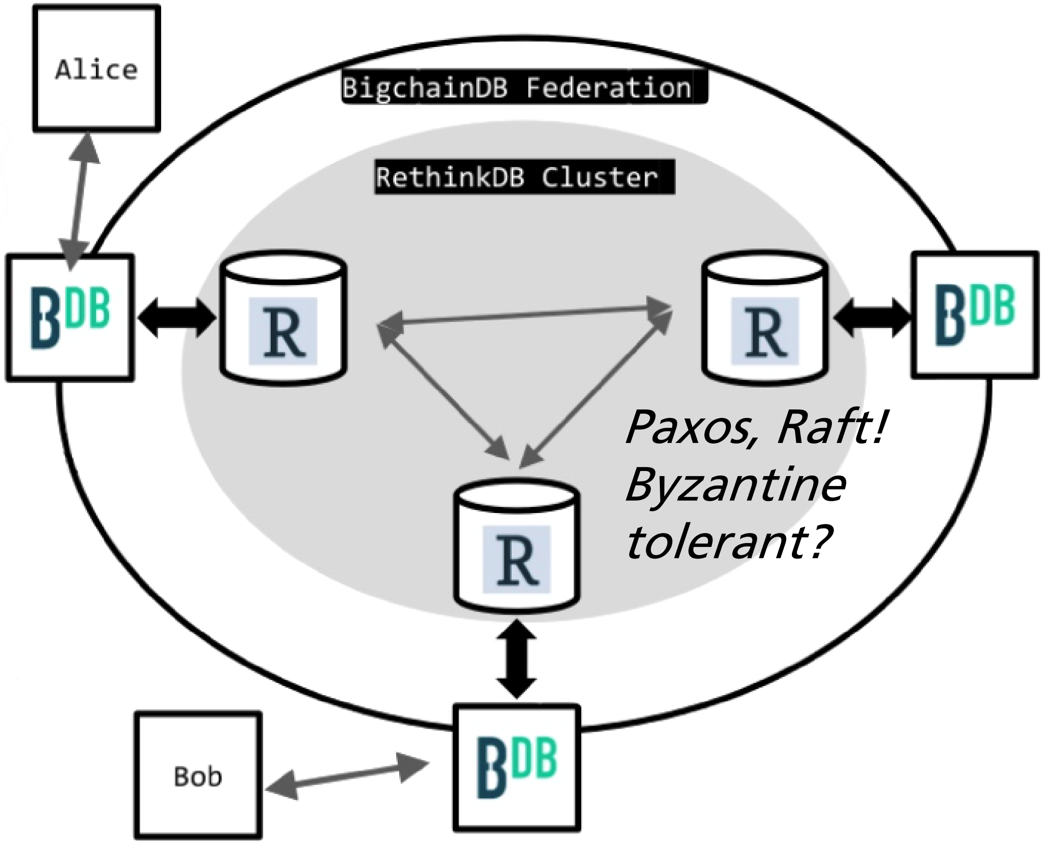
Unpermissioned	Permissioned
Ethereum Nxt	eris:db Sawtooth Lake
BTC other coins	openchain BigchainDB

Transaction oriented

A blockchain full of blockchains



Bigchain DB – a permissioned transaction oriented Blockchain



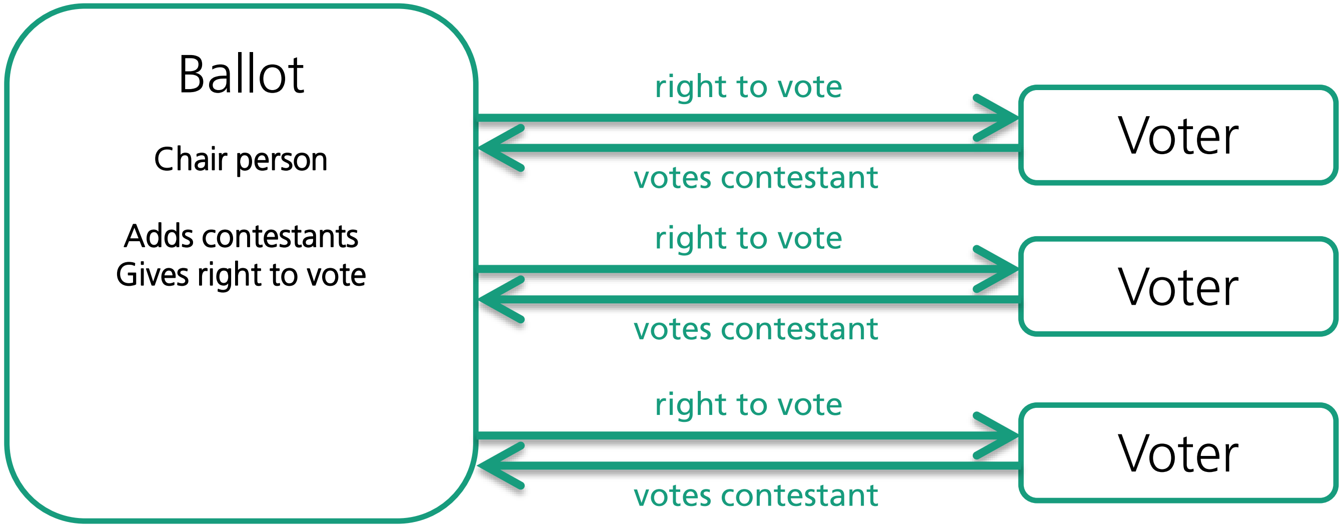
Paxos, Raft! Byzantine tolerant?

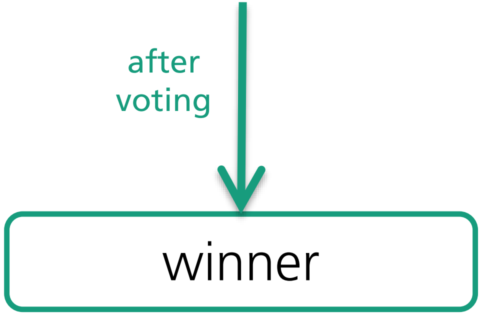
BIGCHAIN DB

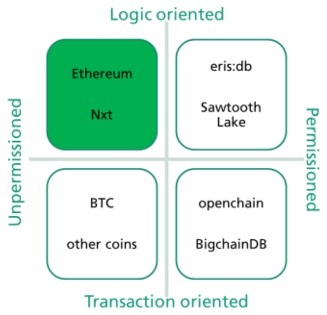
	Unpermissioned	Permissioned
Logic oriented	Ethereum Nxt	eris:db Sawtooth Lake
Transaction oriented	BTC other coins	openchain BigchainDB

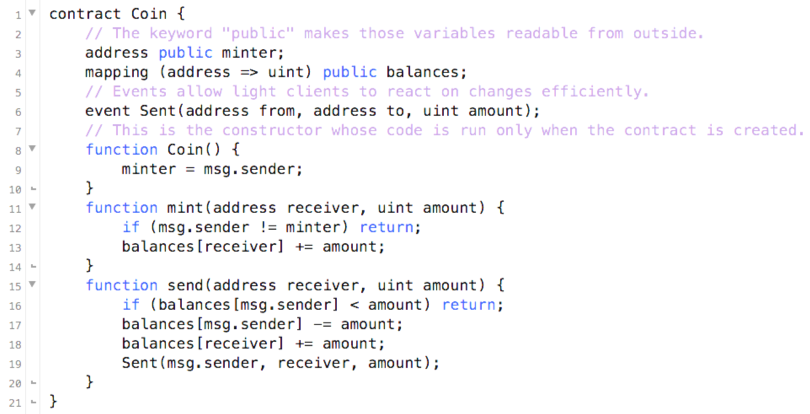
https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

Ethereum – an unpermissioned logic oriented Blockchain used to implement a voting system









```
contract Coin {
    // The keyword "public" makes those variables readable from outside.
    address public minter;
    mapping (address => uint) public balances;
    // Events allow light clients to react on changes efficiently.
    event Sent(address from, address to, uint amount);
    // This is the constructor whose code is run only when the contract is created.
    function Coin() {
        minter = msg.sender;
    }
    function mint(address receiver, uint amount) {
        if (msg.sender != minter) return;
        balances[receiver] += amount;
    }
    function send(address receiver, uint amount) {
        if (balances[msg.sender] < amount) return;
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        Sent(msg.sender, receiver, amount);
    }
}
```

What to do if your application or process requires …

- A combination with heavy external data?
  - Use hashes to represent your external data in the blockchain preserving integrity
- Privacy?
  - Encrypt your data/payload. But what happens if your key become insecure? A re-encryption is not possible!
- Speed?
  - Select proof of stake or lottery based validation mechanisms
- Resource awareness (IoT)?
  - Hybrid approaches with different node capabilities (slock.It Ethereum computer)

https://slock.it/ethereum_computer.html

What to do if your application or process requires …

- Autonomy?
  - Apply smart contracts
- Scalability?
  - Select proof of stake or lottery based validation mechanisms including hybrid nodes and multiple blockchains
- IoT payment
  - Smart contracts,
  - But solve the dilemma between a clever solution for managed micro payments and resource limitations

In search of suitable use cases?

You should look for a process:

- for which you plan to eleminate the intermediate
- for which you need to establish an intermediate
- that involves different stake holders or cooperation partner that do not yet have a trust relation
- that involves a flexible and volatile set of cooperartion partners that require a stable trust and transction-documentation base

To make life easier

- avoid processes that underly strong regulations
- move your focus away from a crypto-currency based application

Summary

- The design space for blockchain applications offers many dimensions.

- Speed and scalabilty inform the selection of the validation method.

- Permissioned or unpermissioned approaches inform the selection of the network approach.

- Unchaining the blockchain in its unique elements to resemble it for a speciifc application can be a solution
  - We need open blockchain building blocks

Kontakt

Prof. Wolfgang Prinz, PhD

Fraunhofer FIT

Schloss Birlinghoven

53754 Sankt Augustin

Tel: 02241 – 14 2730

wolfgang.prinz@fit.fraunhofer.de

Visit our blockchain lab:

http://www.fit.fraunhofer.de/de/fb/cscw/blockchain.html

Geschäftsmodell
Fraunhofer FIT
Technologie
Recht