Technische Universität Berlin

Blockchain Insights

Stefan Tai

ISEngineering
Information Systems Engineering

“Banks adopting blockchain dramatically faster than expected”

IBM, Sep 2016

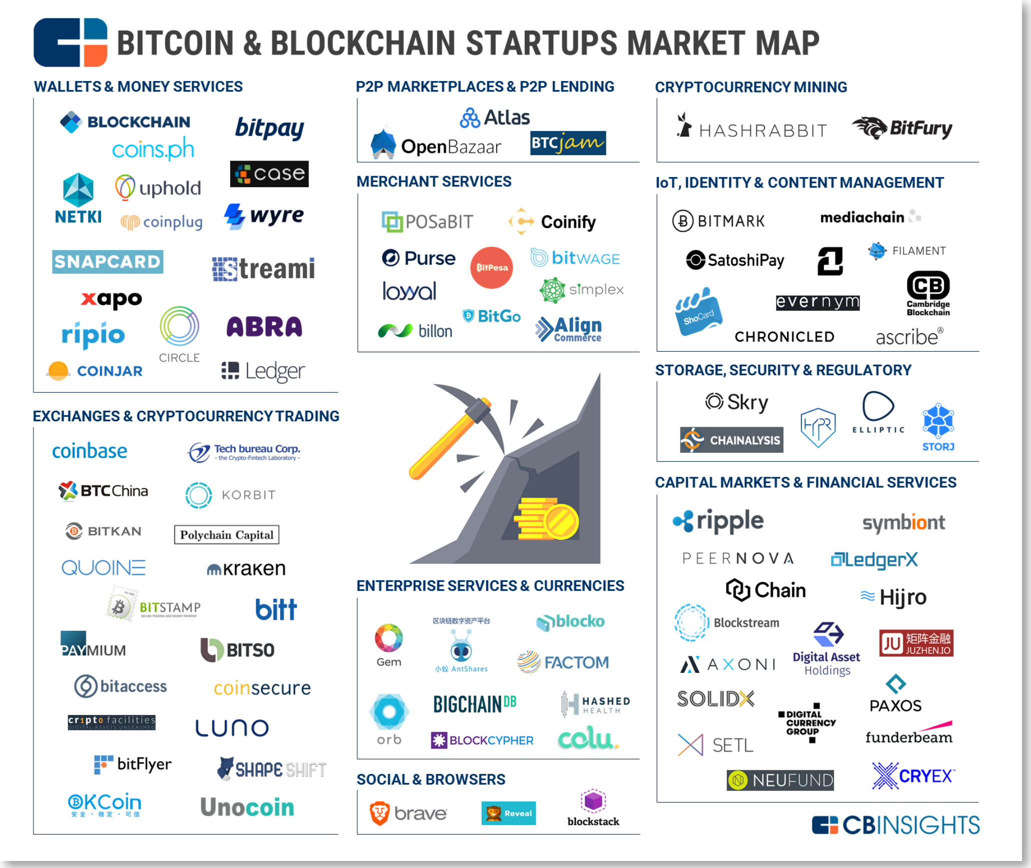
“Blockchain could save investment banks up to $12 billion a year”

Accenture, Jan 2017

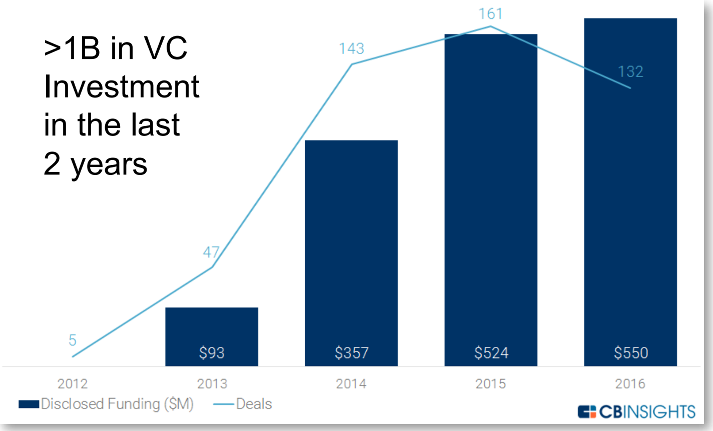
The practical applications for blockchain technology go way beyond financial assets. Essentially, any type of digital asset can be tracked and traded through a blockchain.

Experiments range from medical records to digital rights and micropayments, identity, and supply chain.

Harvard Business Review, March 2017



>1B in VC Investment in the last 2 years



The power and disruption of blockchain is evident...

"…but so are the challenges to its broad implementation."

MIT Sloan Management Review, March 2017

Technische Universität Berlin

So, what is a blockchain?

The Business View:

… a shared decentralized ledger, enabling trustless interactions and business disintermediation, thereby lowering transaction costs

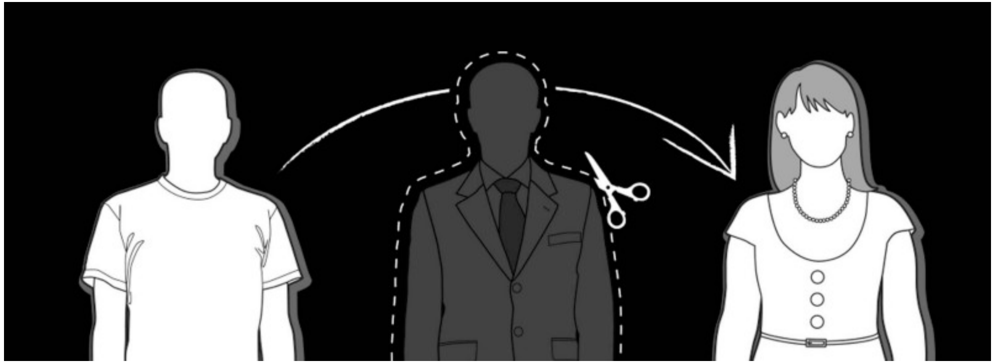
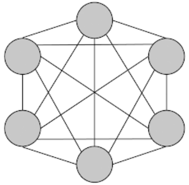


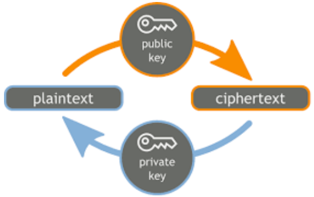
Figure source: LinkedIn / BlockSmiths

The Technology View:

… a peer-to-peer protocol for trustless execution and recording of transactions secured by asymmetric cryptography in a consistent and immutable chain of blocks



P2P network



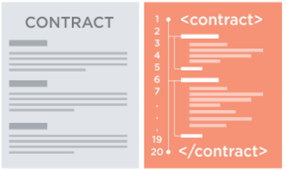
Asymmetric cryptography

Distributed storage

The IT Architect View:

…a shared information system, where no single party can modify any record without the consensus of all network participants, which decentralizes control and requires incentive mechanisms to provide for security and immutability.

Distributed storage



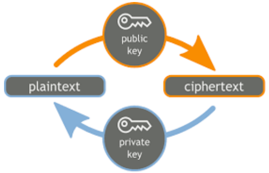
Digital contracts

Consensus protocols

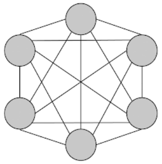
Incentive mechanisms

System Overview

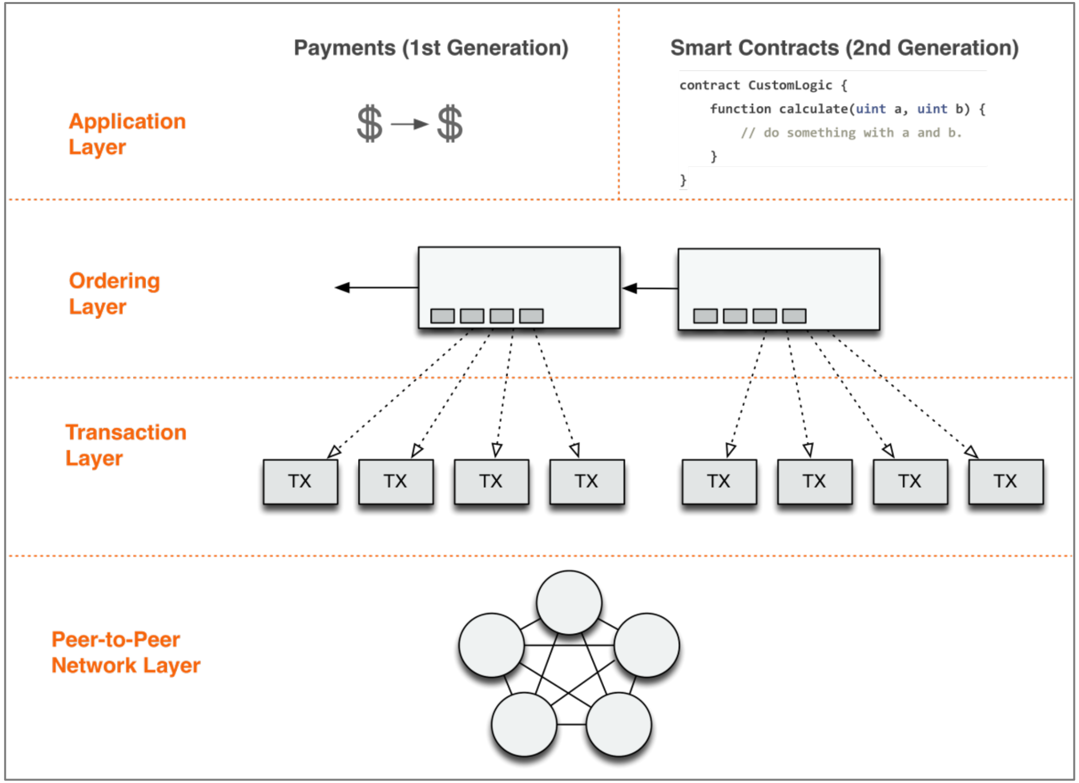
Distributed storage



Asymmetric cryptography



P2P network



Payments (1st Generation)

Smart Contracts (2nd Generation)

Application Layer

$ → $

```
contract CustomLogic {
    function calculate(uint a, uint b) {
        // do something with a and b.
    }
}
```

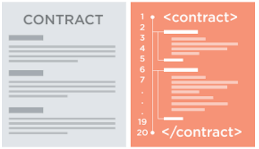
Ordering Layer

Transaction Layer

Peer-to-Peer Network Layer

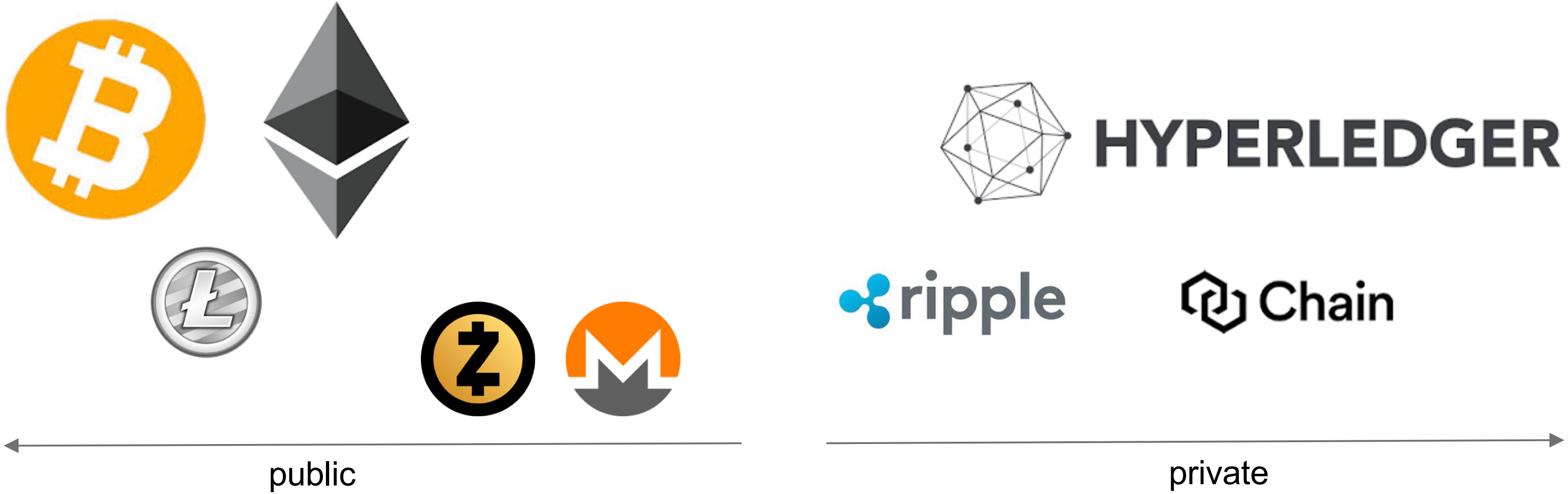
Incentive mechanisms

Consensus protocols



Digital contracts

A diversity of blockchain networks



Understanding decentralized data management:

What is a *blockchain transaction*?

Recall ACID transactions and relational databases (RDBMS)

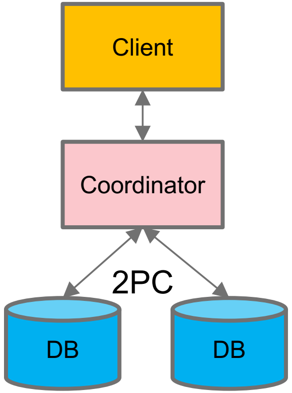
ACID Transaction

Atomicity – all or nothing

Consistency – only valid data

Isolation – no interference

Durability – committed data is never lost



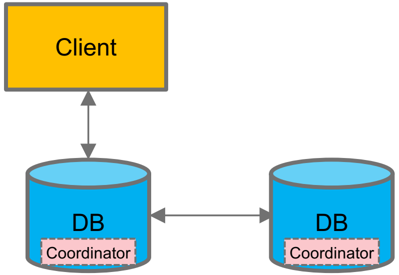
Recall BASE systems and NoSQL stores

BASE Systems

Basically Available –
partial system failures ok

Soft-state – system state can change
even without further updates

Eventually consistent – system will
become consistent if no new updates
are made



Blockchain transactions and blockchain systems:

Not ACID, not BASE, but SALT

Sequential – transactions are processed in sequential order

Agreed - community consensus determines transaction validity

Ledgered – all agreed-on transactions are added to an append-only ledger

Tamper-Resistant – A transaction cannot be manipulated or censored

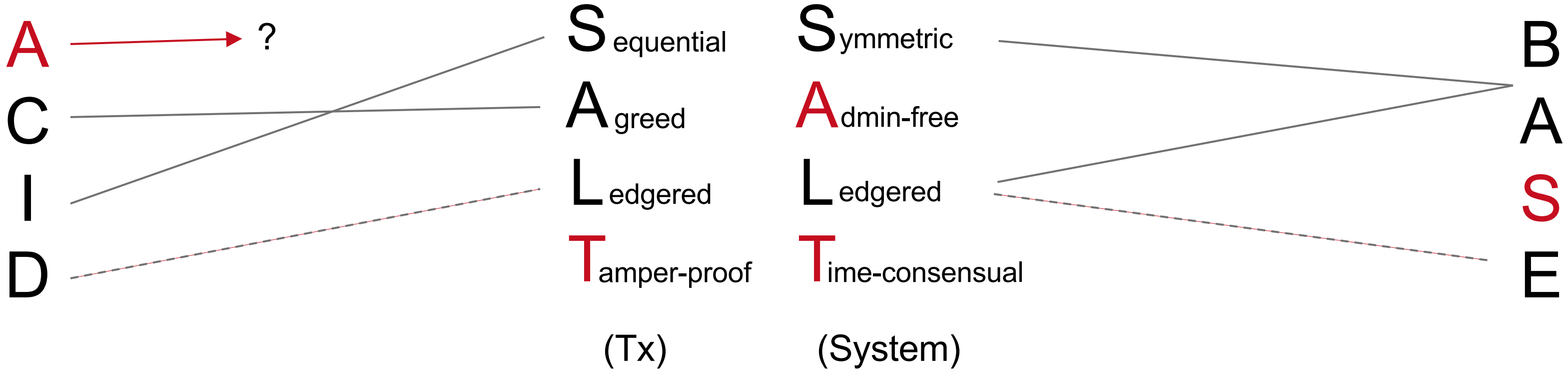
Symmetric – a peer-to-peer network with symmetric responsibilities

Admin-free – no concept of a system admin

Ledgered – all peers maintain a copy of the ledger

Time-consensual – working with block intervals

Comparing ACID, BASE, and SALT



A → ?
C
I
D

Sequential
Agreed
Ledgered
Tamper-proof

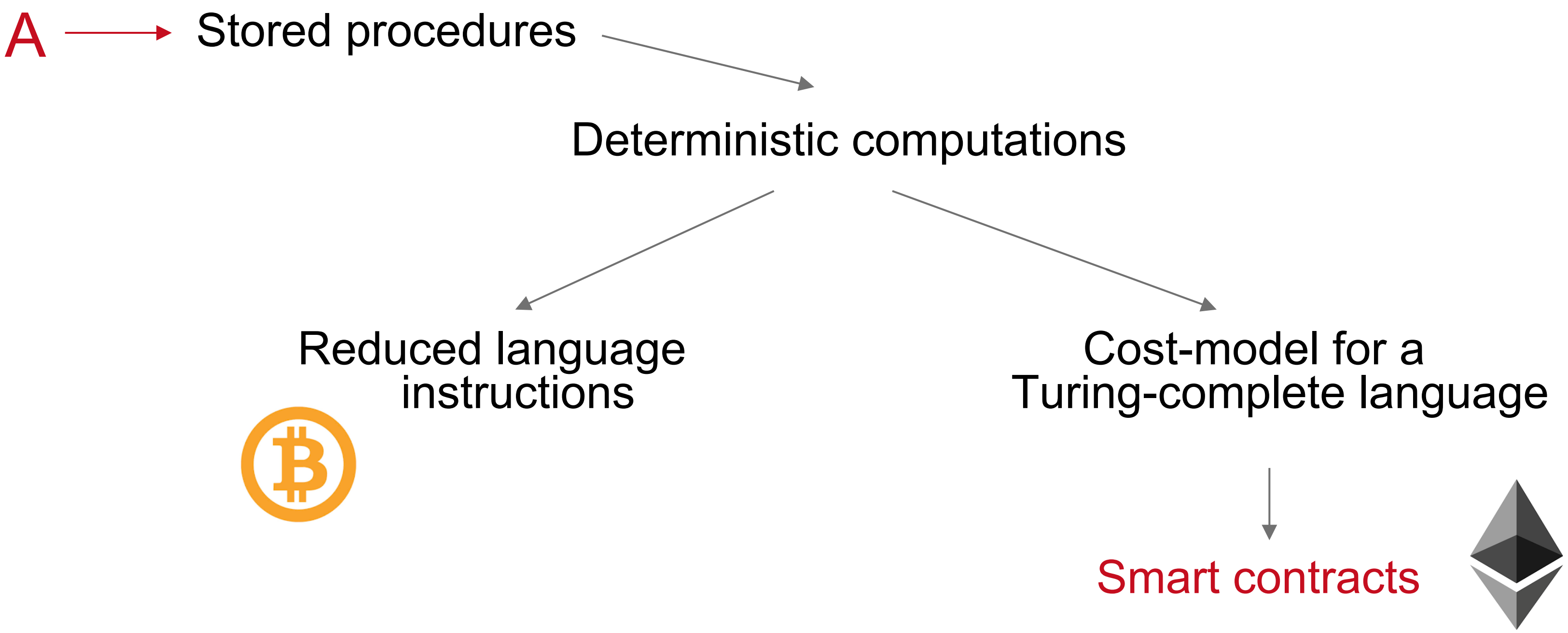
(Tx)

Symmetric
Admin-free
Ledgered
Time-consensual

(System)

B
A
S
E

T for Turing Complete?



A → Stored procedures

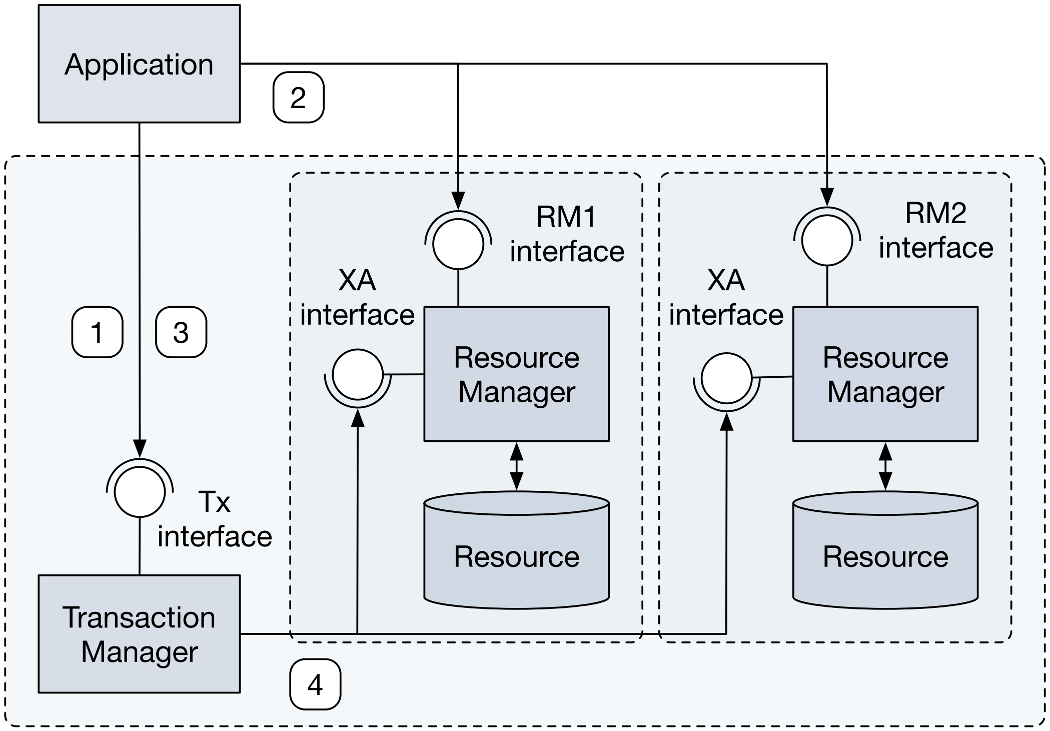
Deterministic computations

Reduced language instructions

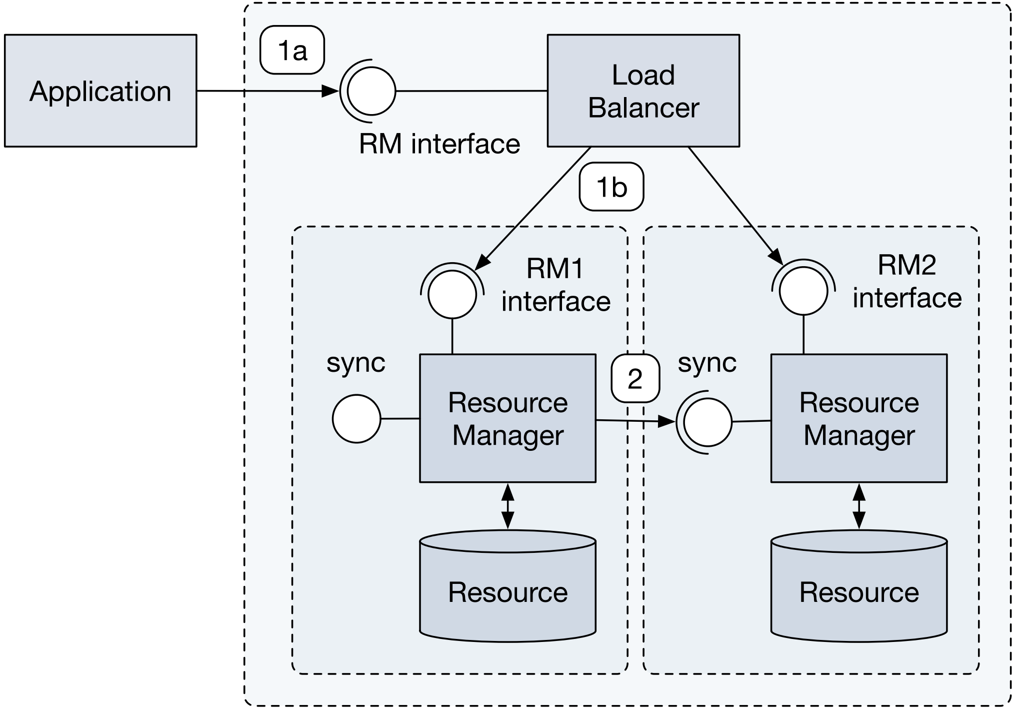
Cost-model for a Turing-complete language

Smart contracts

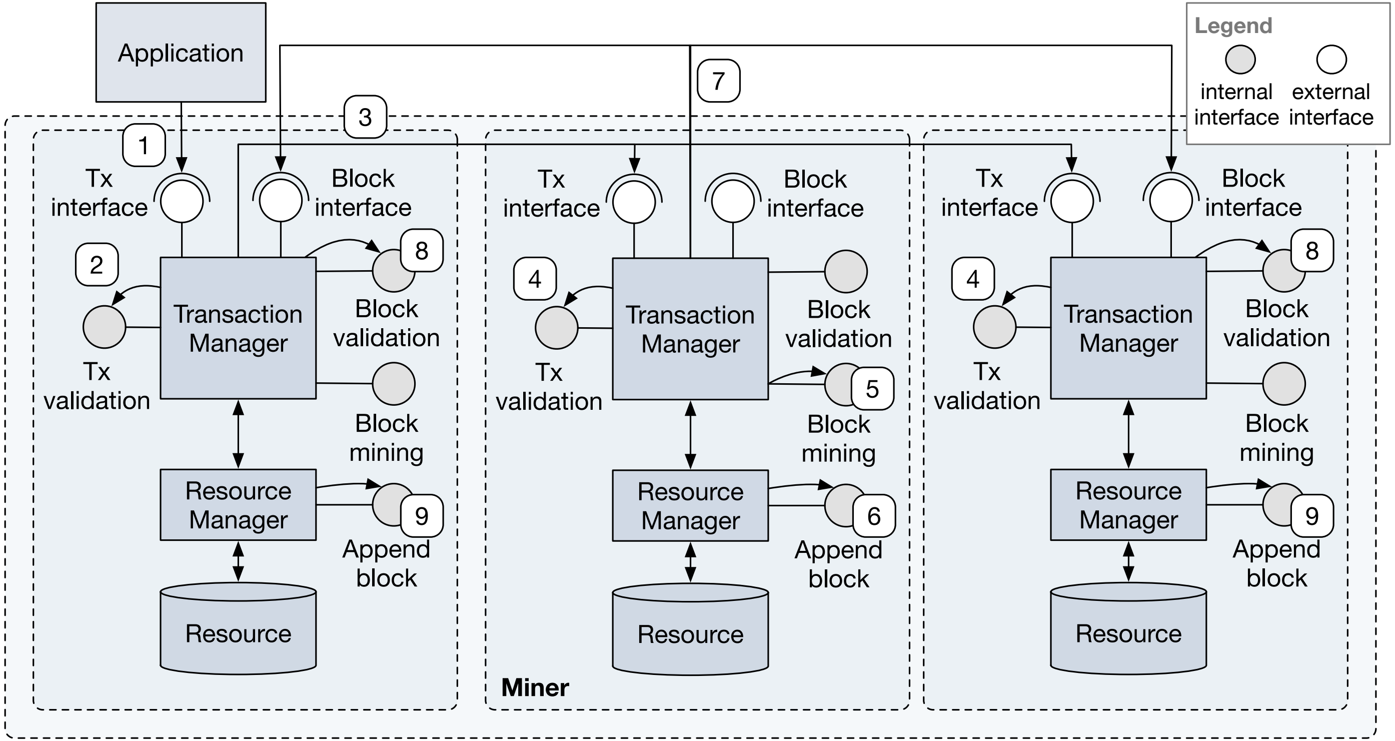
TP systems in support of ACID transactions



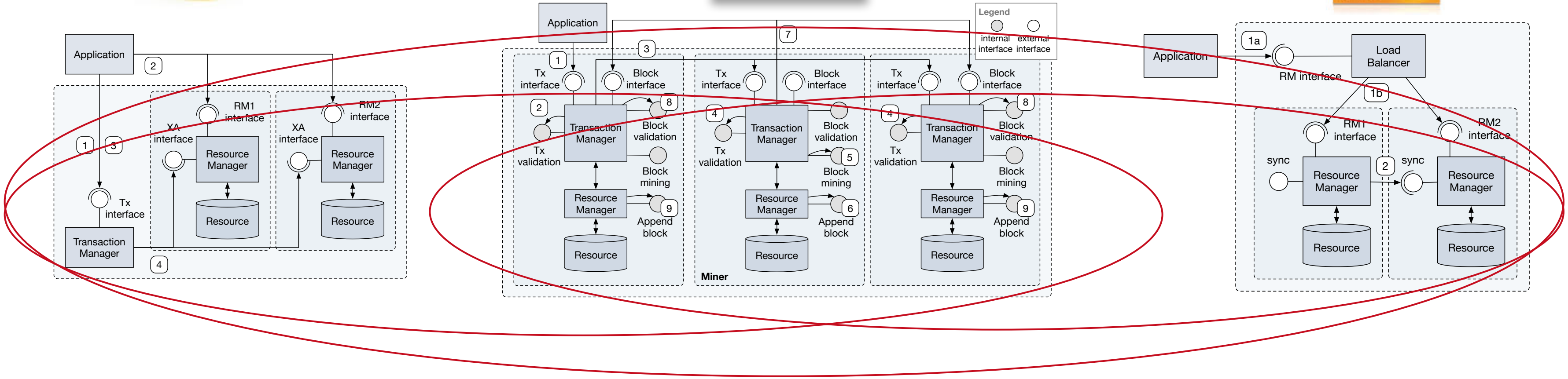
BASE Systems



Understanding SALT



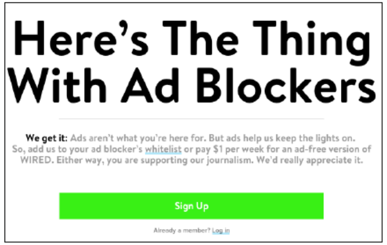
Applications will likely use a combination of all three transaction and system models



Still SALTy? Well-seasoned or just bad taste?

Blockchain Applications

Fintech



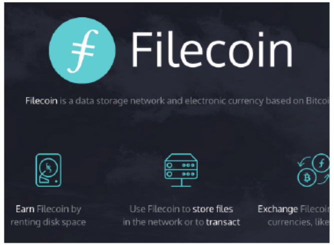
Here's The Thing With Ad Blockers

We get it: Ads aren't what you're here for. But ads help us keep the lights on. So, add us to your ad blocker's whitelist or pay $1 per week for an ad-free version of WIRED. Either way, you are supporting our journalism. We'd really appreciate it.

Sign Up

Already a member? Log in

New Business Models



Filecoin

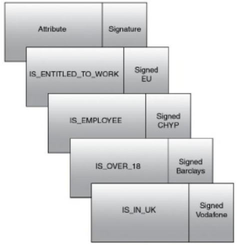
Filecoin is a data storage network and electronic currency based on Bitcoi

Earn Filecoin by renting disk space

Use Filecoin to **store files** in the network or to **transact**

Exchange Filecoi currencies, like

New Types of Platforms



Attribute | Signature

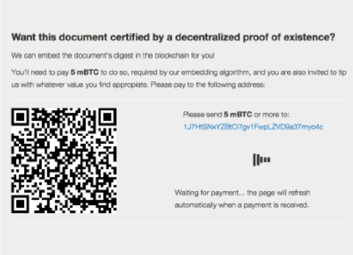
IS_ENTITLED_TO_WORK | Signed EU

IS_EMPLOYEE | Signed CHYP

IS_OVER_18 | Signed Barclays

IS_IN_UK | Signed Vodafone

Identity & Privacy



Want this document certified by a decentralized proof of existence?

We can embed the document's digest in the blockchain for you!

You'll need to pay **5 mBTC** to do so, required by our embedding algorithm, and you are also invited to tip us with whatever value you find appropiate. Please pay to the following address:

Please send **5 mBTC** or more to:
1J7HtSNxYZBtCi7gv1FwpLZVD9a37myo4c

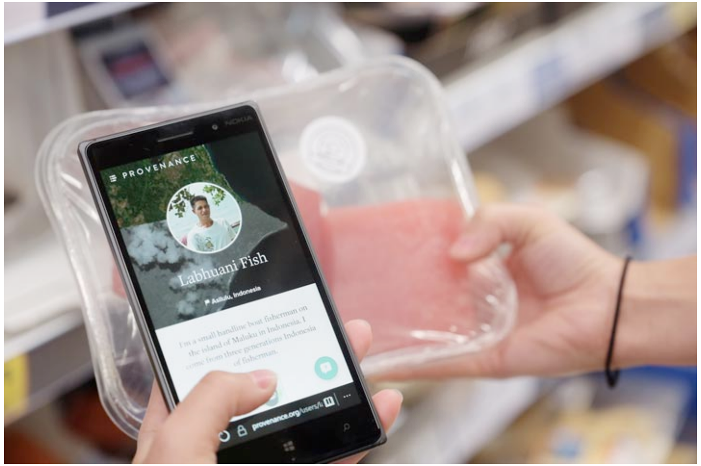
Waiting for payment... the page will refresh automatically when a payment is received.

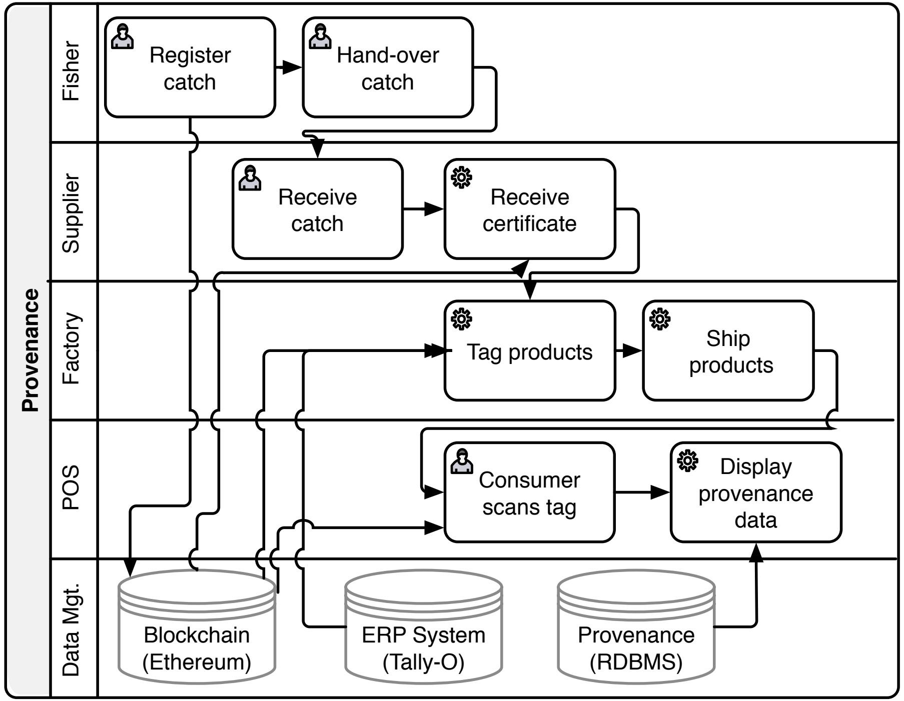
IP & Smart Contracts

IoT, AI Robotics

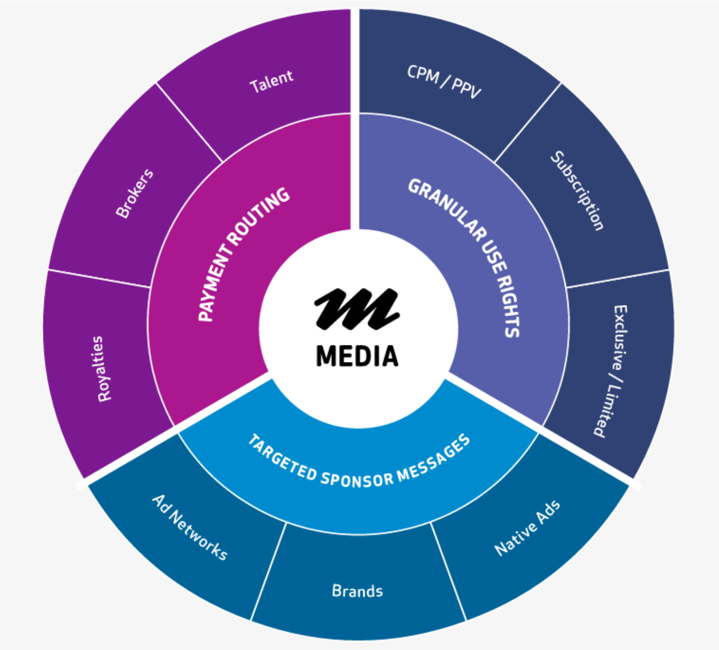
Source: Christian Catalini, MIT Sloan

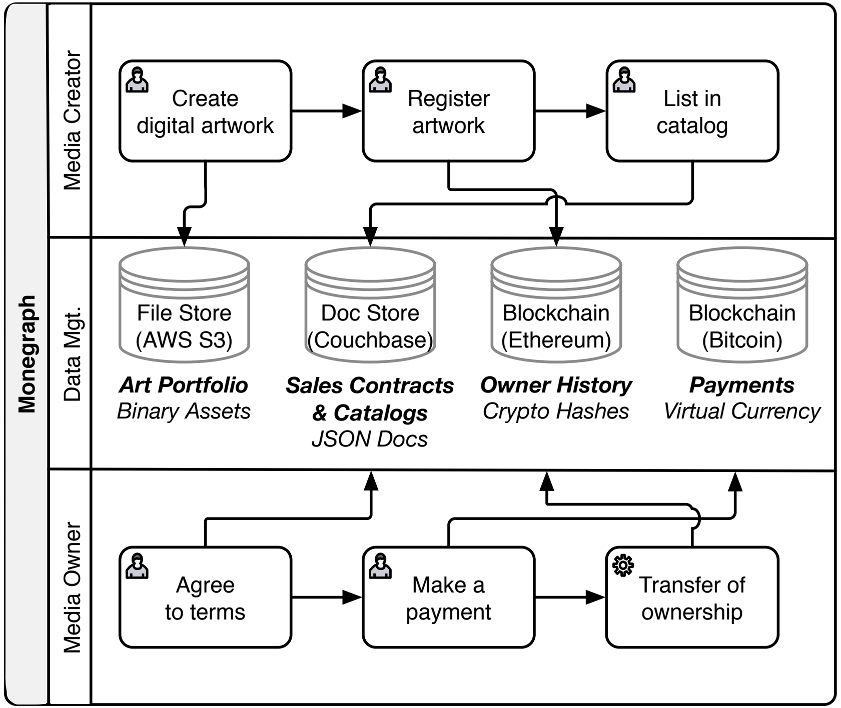
Food Provenance





Digital Artwork / Content Monetization





So, is there no way around blockchains?

What about “my” (next) application then?

And what about statements like:

- “Blockchains do not scale”
- “Blockchain tech not ready”
- “A solution for a problem that doesn’t exist”
- “Why trust a computer scientist rather than a corporation?”
- “Just too much hype”

Our Answer:

Devise and learn from experimental blockchain projects

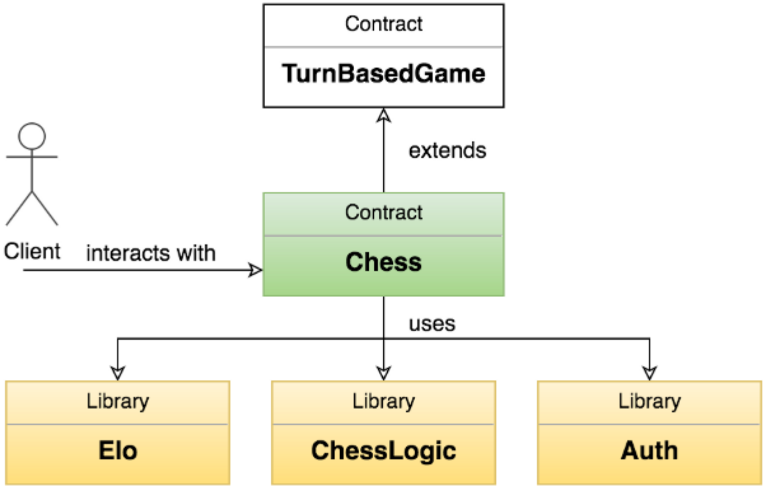
ALTCOINS

September 6, 2016 | **Jamie Redman** | 👁 25411 | 💬 **2**

Students at Berlin University Build Chess Game on Ethereum

https://news.bitcoin.com/berlin-students-chess-ethereum/

Simple chess game, tough challenges



- Checkmate condition is too complex to be checked on-chain. We need to find an alternative trustless way to check conditions.

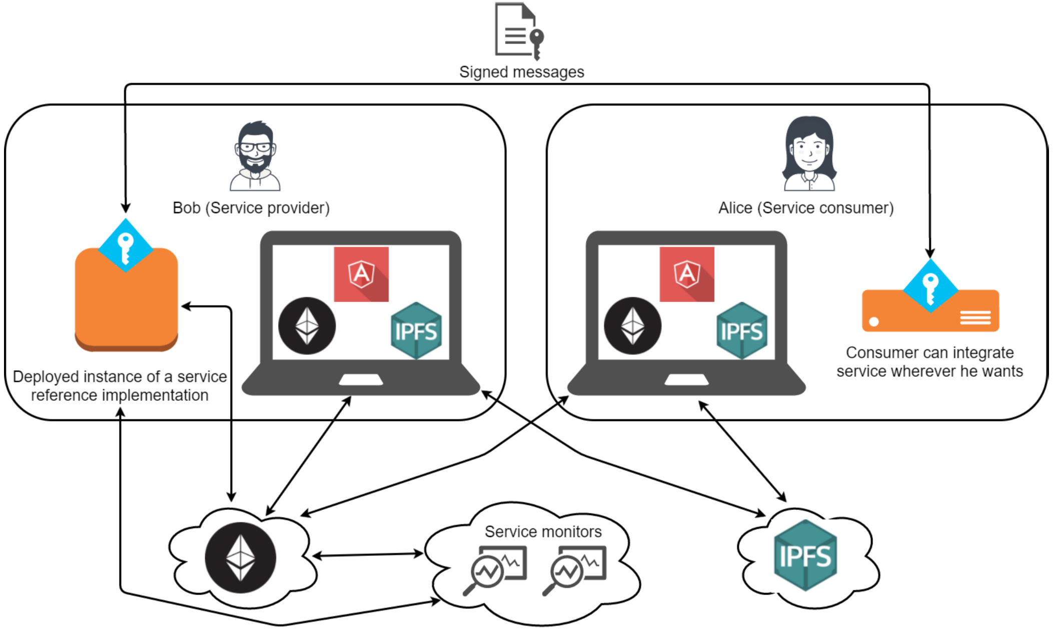
- Computations cost money. Hence, like in a physical chess game, we should have a player trigger endgame condition checks instead of doing them after every valid move.

The long-standing vision of a Service Marketplace…
…now decentralized

Old model:

Figure source: Instabug

Complex undertaking: Trustless Intermediation through Smart Contracts, more tough challenges


Signed messages
Bob (Service provider)
Alice (Service consumer)
Deployed instance of a service reference implementation
Consumer can integrate service wherever he wants
IPFS
IPFS
IPFS
Service monitors

- On-chain data storage is expensive and limited. We need to find a way to store data off the chain without giving up its manipulation-resistance.
- All on-chain data is visible to everyone in the network. Simple encryption brakes verifiability. We need to find a way to do computations on private data without revealing it.

Off-chaining Patterns

- …*move computation and data off the blockchain*
- can be used individually or in combination
- *while maintaining the key properties of blockchains*: include techniques to ensure that blockchain properties are not compromised to an unwanted degree

Five patterns [please see the ESOCC2017 keynote paper]

I. Challenge Response Pattern

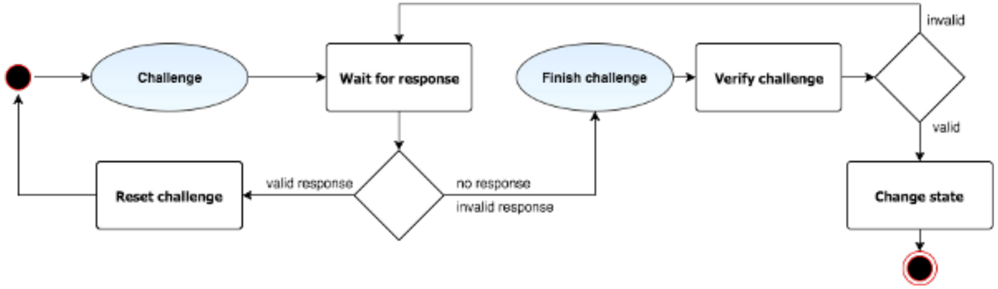
II. Off-chain Signatures Pattern

III. Content-Addressable Storage Pattern

IV. Delegated Computation Pattern

V. Low Contract Footprint Pattern

I. Challenge Response



Context:

- A smart contract models a state machine with well-defined final states.
- State transitions are cheap to compute, but checking whether a given state is a final state is expensive or may not be possible at all.

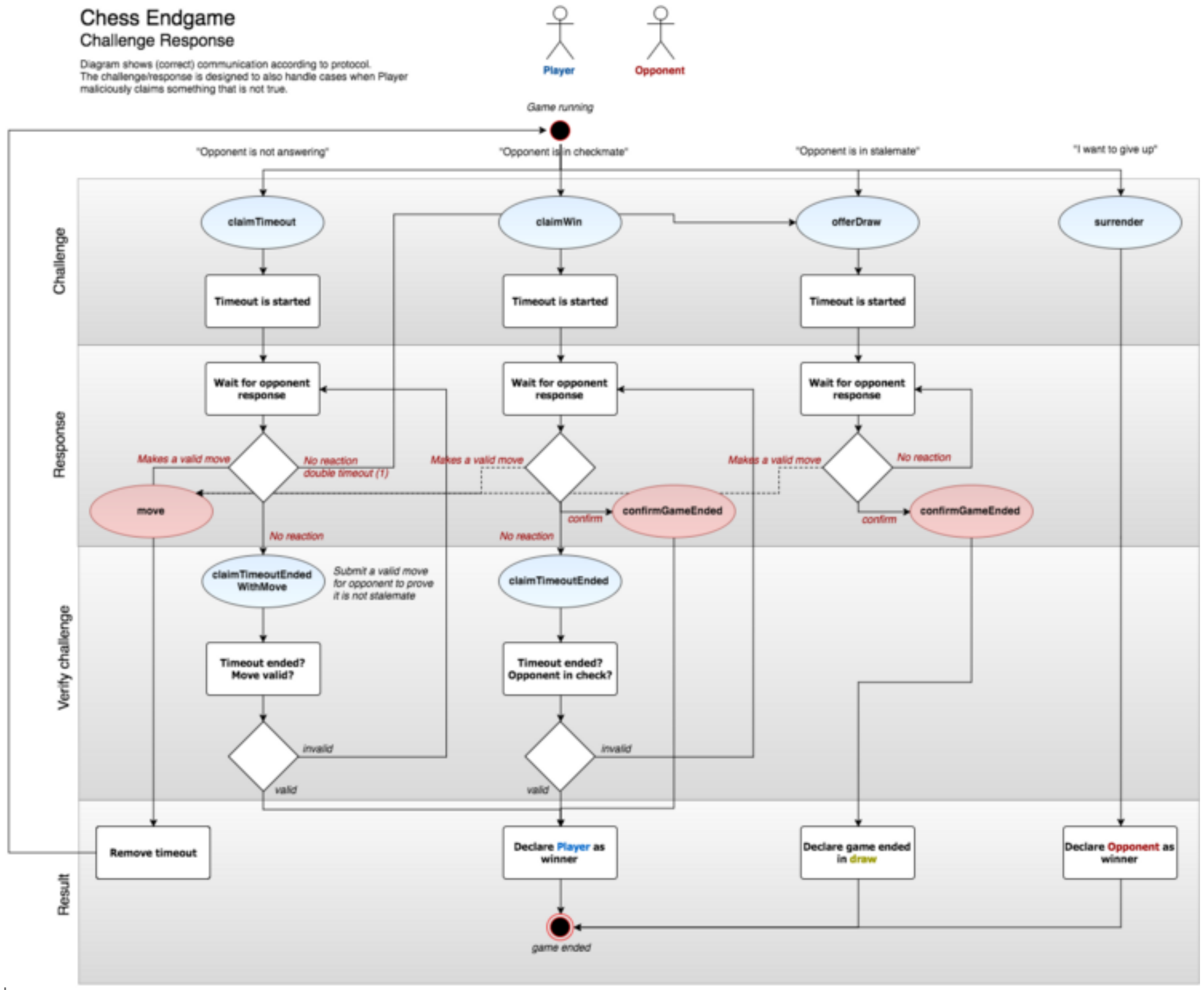
Solution:

- Perform the check off-chain on the client side. A client can notify a smart contract when a final state has been reached.
- Other clients can prove claims wrong by providing a valid state transition.

Chess Endgame

Challenge Response

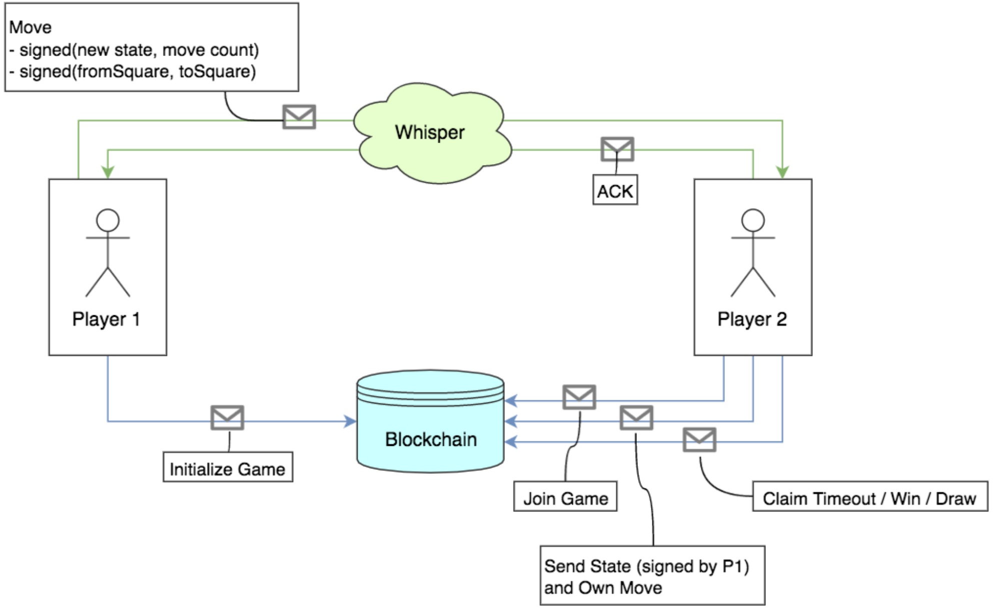
Diagram shows (correct) communication according to protocol.
The challenge/response is designed to also handle cases when Player maliciously claims something that is not true.



S. Tai 2017 | ise.tu-berlin.de

[1] In case of stalemate, if Player falsely claimed a win, neither the Player nor the Opponent would have a chance to do anything, because that state can only be resolved when there is a valid move. Because of that, an additional way to resolve the state is added: After two times the timeout, both players are allowed to offer a draw.

II. Off-Chain Signatures


Move
- signed(new state, move count)
- signed(fromSquare, toSquare)
Whisper
ACK
Player 1
Player 2
Blockchain
Initialize Game
Join Game
Claim Timeout / Win / Draw
Send State (signed by P1) and Own Move

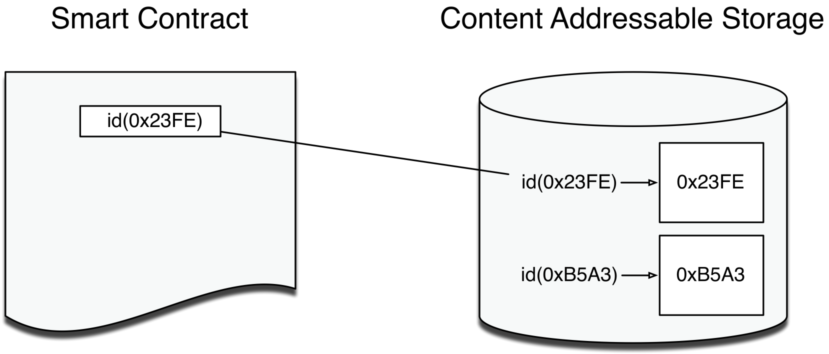
Context:

- Two network participants want to transact with each other multiple times in the future.
- They want to reduce the cost of these transactions or want to hide them from others.

Solution:

- Specify a smart contract including a function, which applies an external state given as argument to the contract state.
- This function includes a signature check to ensure both participants agree with the state change.
- The participants perform transactions purely off-chain and peer-to- peer, without involving the blockchain.
- Any transaction, signed by both parties, can then be sent to the smart contract by a participant at any point in time. After validating both signatures, the contract updates its state accordingly.

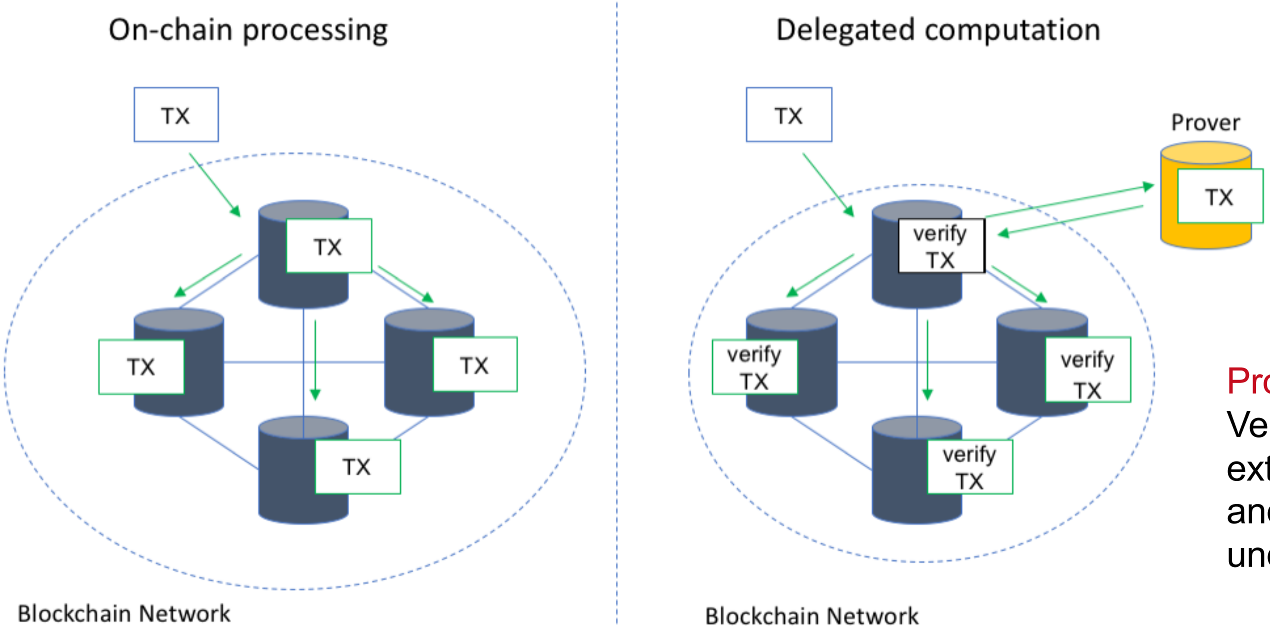
III. Content-Addressable Storage



Context:
A large amount of data is associated with a smart contract. On-chain storage is too expensive.

Solution:
Store the data off-chain in a content-addressable storage system and store the reference in the smart contract. Clients using the smart contract can retrieve the reference and based on that retrieve the data. Then, they can verify the data's correctness by recomputing its address from itself and comparing it to the reference stored in the smart contract.

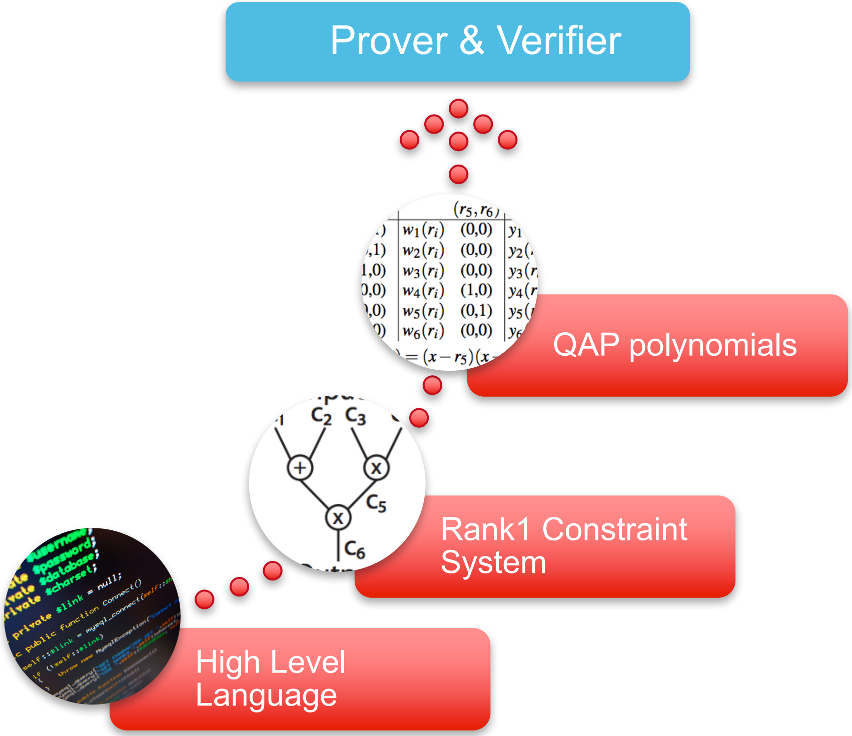
IV. Delegated Computation



Problem:
Verifiable computations are extremely complex to specify and require deep technological understanding

Solution: A higher-level language and compiler, which transforms a more convenient representation into verifiable programs based on zkSNARKS. Additionally, generate Ethereum Smart Contracts, which verify the results on-chain.

Technische Universität Berlin

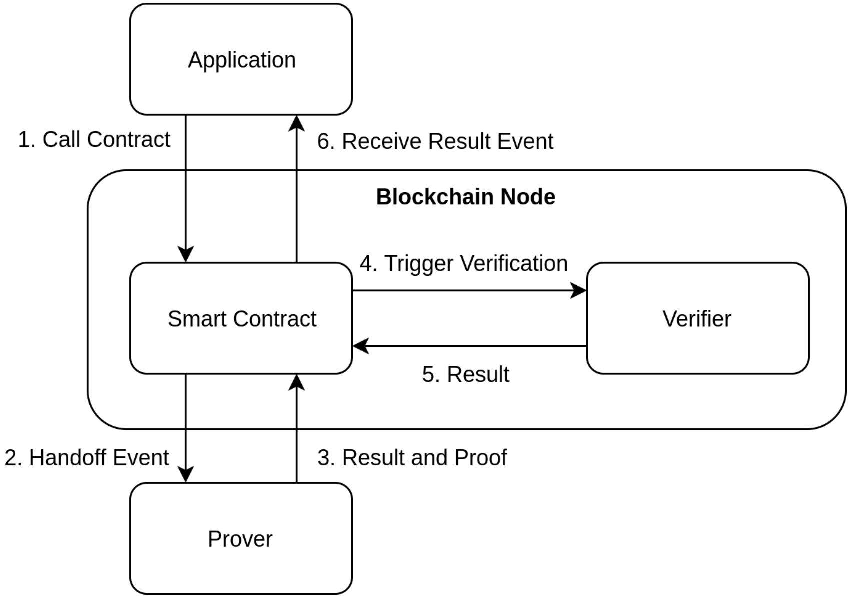


Prover & Verifier

QAP polynomials

Rank1 Constraint System

High Level Language



Application

1. Call Contract

6. Receive Result Event

Blockchain Node

4. Trigger Verification

Smart Contract

Verifier

5. Result

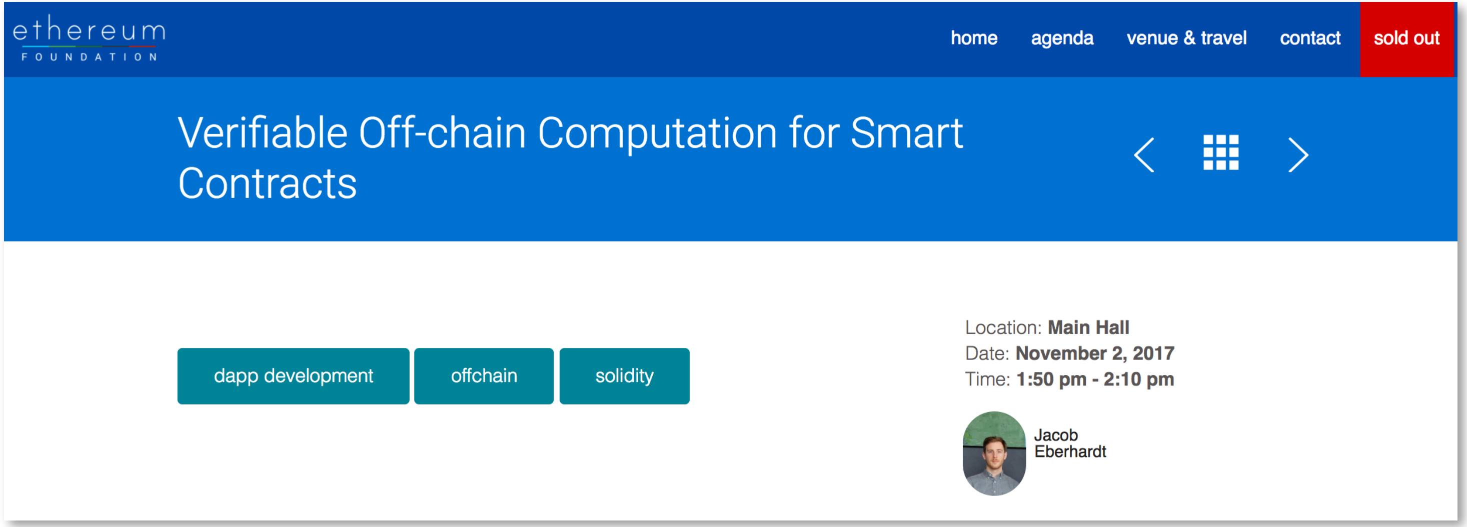
2. Handoff Event

3. Result and Proof

Prover

ISEngineering
Information Systems Engineering

Find out more:
Presentation and Code release during Ethereum Devcon 3 (Nov 17) by Jacob Eberhardt



Verifiable Off-chain Computation for Smart Contracts

Location: **Main Hall**
Date: **November 2, 2017**
Time: **1:50 pm - 2:10 pm**

Jacob Eberhardt

V. Low Contract Footprint

- Do not check conditions on-chain after a state change. Let nodes perform the condition check locally and trigger an on-chain check in case of success.
- Optimize for writes, not reads. Minimize writes and store information free of redundancy. Compute derived data locally during reads.

Examples from the service marketplace application:

- A service provider needs to make sure consumers are removed from the on-chain authorization list after the time period the consumer paid for is over. Instead of periodically triggering or linking the condition check to another contract function and risking frequent reevaluation, he tracks the access period locally and triggers the on-chain check after it has elapsed. This reduces the amount of on-chain evaluations to one.
- If the service provider wants to know the number of customers currently subscribed to his service, he should not add a counter to the smart contract. He can compute the number locally at any point from the authorization list. This saves storage space and counter update operations.

Conclusion

- The potential for blockchains to transform how organizations produce and capture value is huge and very real

- Blockchains are a fascinating synthesis of diverse concepts from computer science and economics
- Decentralized data and transaction management using blockchains is SALT (and not ACID, not BASE)

- Devise and learn from experimental blockchain projects to study applications and application verticals
- Patterns, and off-chaining patterns in particular, proved useful in engineering practice

Technische Universität Berlin

Join us in Berlin!

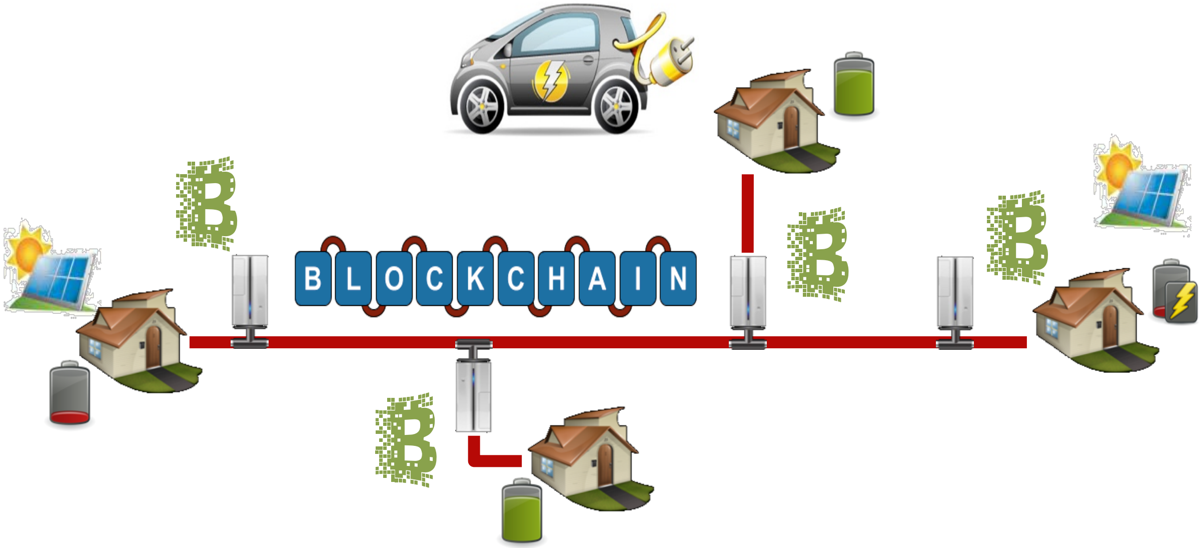
We are hiring!

…and are looking for passionate researchers
to do research projects with real-world impact…

Example project:
A blockchain blueprint for photo-voltaic energy systems
(starting Q1/2018)

Technische Universität Berlin

Bundesministerium für Wirtschaft und Technologie



Thank you!

Prof. Dr. Stefan Tai

TU Berlin, Sekr. EN14
Einsteinufer 17, 10587 Berlin, Germany

tai@tu-berlin.de

ise.tu-berlin.de