Blockchain Anwendungen für IoT

ECC2017

5.Sept 2017 Alain Brenzikofer

Supercomputing Systems AG

Vision trifft Realität.

Supercomputing Systems AG
Technopark 1
8005 Zürich

Phone +41 43 456 16 00
Fax +41 43 456 16 10
www.scs.ch

super computing systems

Inhalt

- Bitcoin
- Was eine Blockchain jenseits von Kryptowährungen ermöglicht
- Wie funktioniert ein Smart Contract?
- Anwendungsbeispiele für IoT
- Praktisches Anwendungsbeispiel «MeasPub»
- Herausforderungen der praktischen Umsetzung
- Vorteile beim Einsatz von Blockchain Technologie

Bitcoin

Seit 2009 gibt es Bitcoin. Je nach Betrachter ist Bitcoin

- Ein Online-Zahlungsmittel
- Ein spekulatives Asset
- Eine Währung

Die Technologie, welche Bitcoin zugrunde liegt ist die Blockchain, ein P2P Netzwerk, welches durch Kryptografie und ökonomische Anreize gesichert wird.

ledger wallet

generalbytes

mining racks

Was eine Blockchain ermöglicht
Jenseits von Kryptowährungen

Eine dezentrale Datenbank mit

- **Konsens** weltweit
  - *“Ich sehe was Du siehst und ich weiss, dass das was ich sehe dasselbe ist was Du siehst*
  - *“Ich weiss, dass Du weisst, dass ich weiss”*
- **Gültigkeit**
  - Jeder Eintrag ist validiert
- **Einmaligkeit**
  - Es gibt nur eine gültige Version der Public Chain (die grösste). Ein Token kann nicht zweimal ausgegeben werden.
- **Unveränderbarkeit**
  - Aber Achtung! Dies kann global «demokratisch» übersteuert werden (siehe ethereum DAO fork)

Blockchain vs. zentralisierte Datenbank

- **Vermittlerrolle**. Blockchains ermöglichen es mehreren Parteien, welche einander nicht vollständig vertrauen, eine gemeinsame Datenbank ohne vertrauenswürdigen Vermittler sicher zu betreiben.
- **Öffentlichkeit**: Alle Teilnehmer an einer Blockchain sehen alle Transaktionen. Auch wenn Pseudonyme und Verschlüsselung verwendet werden gibt eine Blockchain mehr Informationen Preis als eine zentrale Datenbank

Blockchains sind dann ideal als Datenbank, wenn jeder Benutzer alles sehen darf, aber kein einzelner Aktor kontrollieren können soll, wer was schreiben darf.

(C) http://www.multichain.com/blog/2016/05/four-genuine-blockchain-use-cases/

Was ist ein *Smart Contract*?

Blockchains der zweiten Generation haben zusätzlich Möglichkeiten:

- Selbstvollstreckender Vertrag
  - macht Sinn, wenn dem Vertrag der volle Betrag hinterlegt werden kann, welcher im äussersten Fall fällig wird. (Der Vertrag kann nur on-chain vollstrecken – und nur mit den Mitteln, über die er verfügt)
- *Smart Contracts* à la Ethereum machen nur Sinn auf Public Blockchains, ansonsten gibt es günstigere Lösungen bei welchen nicht jeder Knoten sämtlichen Code ausführen muss.

http://www.multichain.com/blog/2015/11/smart-contracts-good-bad-lazy/

Wie funktioniert ein *Smart Contract*? (Ethereum)

```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
}
```

- Ein SC ist ein Programm, welches in einer Blockchain gespeichert wird.
- Funktionsaufrufe sind Transaktionen auf der Blockchain, welche Argumente enthalten können

Wie funktioniert ein *Smart Contract*? (Ethereum)

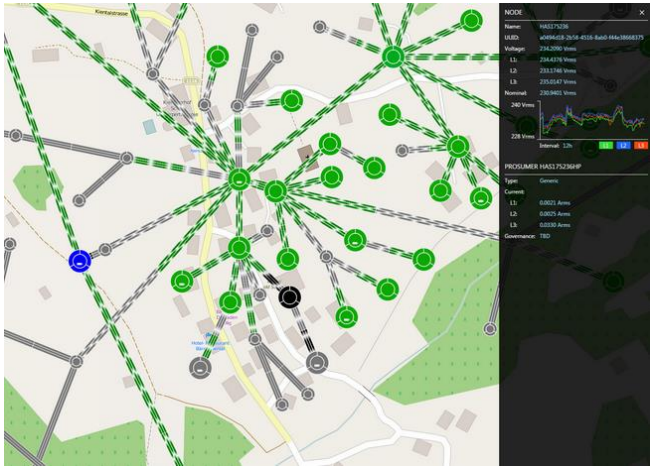
- Jeder Aufruf einer Funktion eines SC wird von sämtlichen Teilnehmern im Ethereum Netzwerk ausgeführt. Da sowohl Eingabewerte wie auch Programmcode in die Blockchain geschrieben werden besteht immer ein Konsens über die Rückgabewerte und die internen Zustände des Programms.

Beispiele möglicher IoT Applikationen M2M Verrechnung: p2p Smart Grid

- Smart Meter kann direkt mit PV Anlage in der Nachbarschaft einen Strompreis verhandeln und abrechnen.

Quelle: Brooklyn Microgrid

- Das Verteilnetz kann regionale Optimierung der Netzauslastung dank dezentralem Marktplatz betreiben



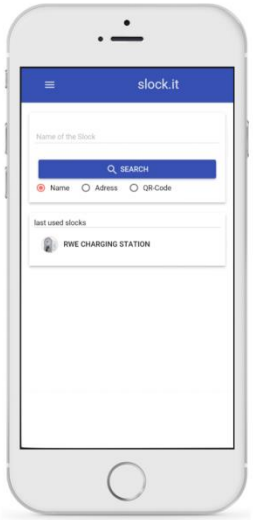
Quelle: GridBox Pilot Projekt

Beispiele möglicher IoT Applikationen
M2M Verrechnung: Sharing Economy

Quelle: slock.it

- Ein Türschloss kann aufgehen unter der Bedingung, dass eine Reservation und/oder eine Bezahlung vorliegt.

- Ein Elektromobil kann eine öffentliche Ladestation reservieren und kontinuierlich pro kWh bezahlen.
  - potentiell mit gutem Schutz der Privatsphäre (Bewegungsprofil)



super computing systems

Beispiele möglicher IoT Applikationen
M2M Verrechnung

- Fog Computing: Geräte können ihre freien Ressourcen verkaufen (Speicherplatz, Rechenzeit, Bandbreite) sonm.io / golem.network

- Sensoren können ihre Messwerte verkaufen *(SCS Demo am Stand)*

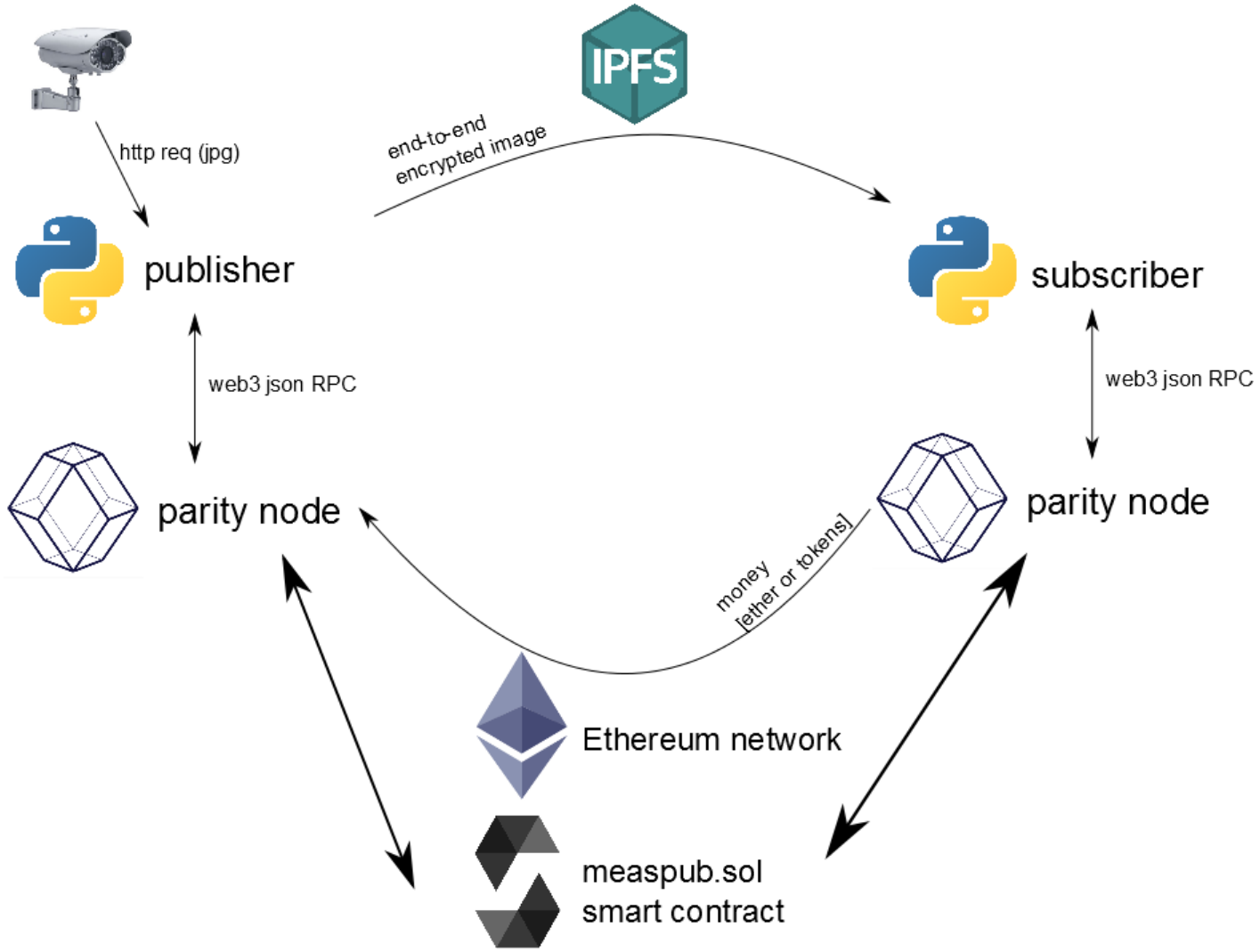
Beispiele möglicher IoT Applikationen

- Sicheres Register
  - Globales Identitätsmanagement für Personen und Geräte. uport.me
  - Herkunftsnachweis entlang gesamter Lieferkette diverser Güter. everledger.io
    - Ihr Kühlschrank kann Bioprodukte nachbestellen, bezahlen und prüfen, ob Lieferung wirklich Bio ist.
- Notariat für Maschinen
  - Trusted Origination & Trusted Timestamping für Sensordaten (SCS Whitepaper)

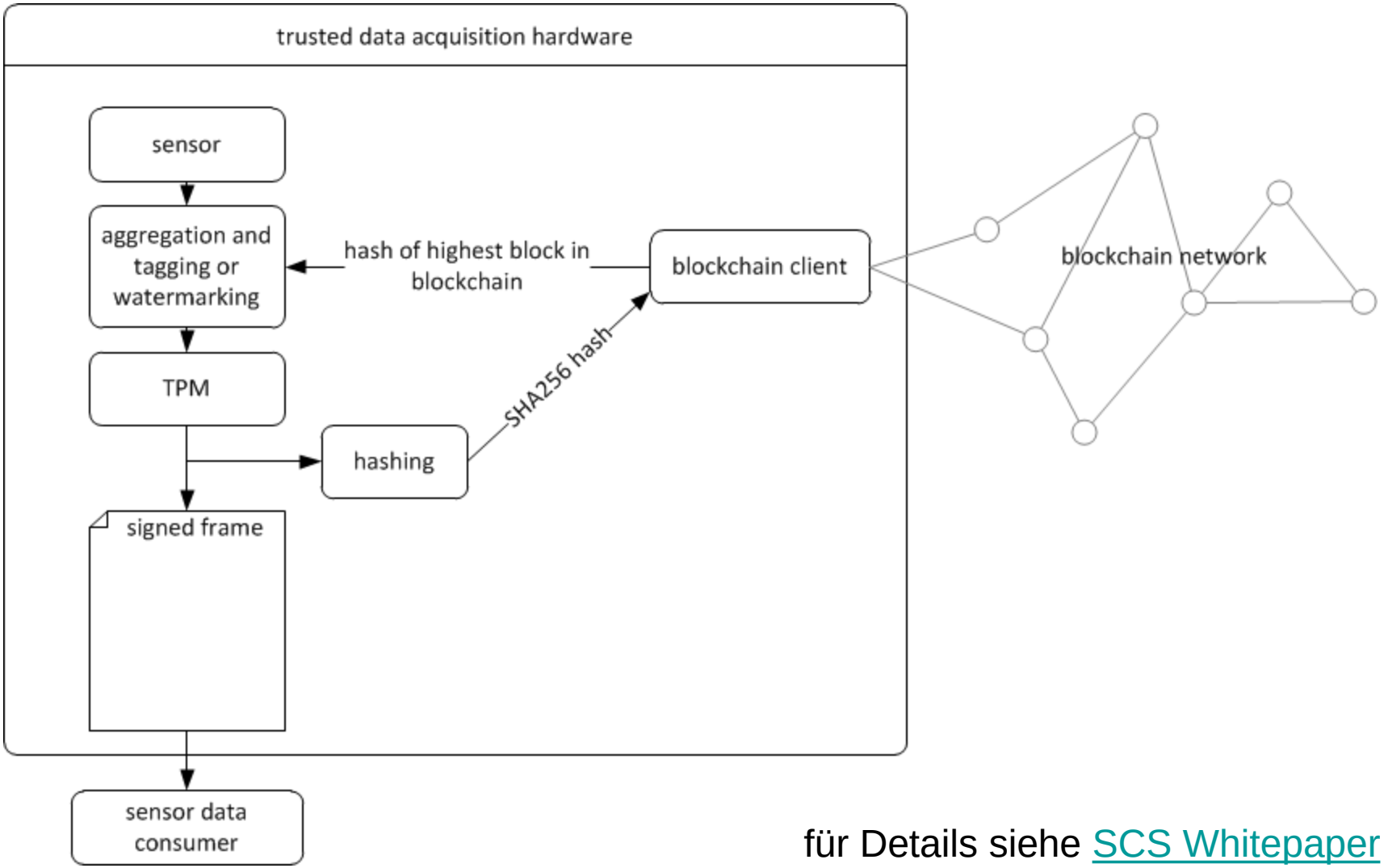
BIO

FAIRTRADE

MeasPub DApp demonstrator



Trusted Sensor: proof-of-existence enabled

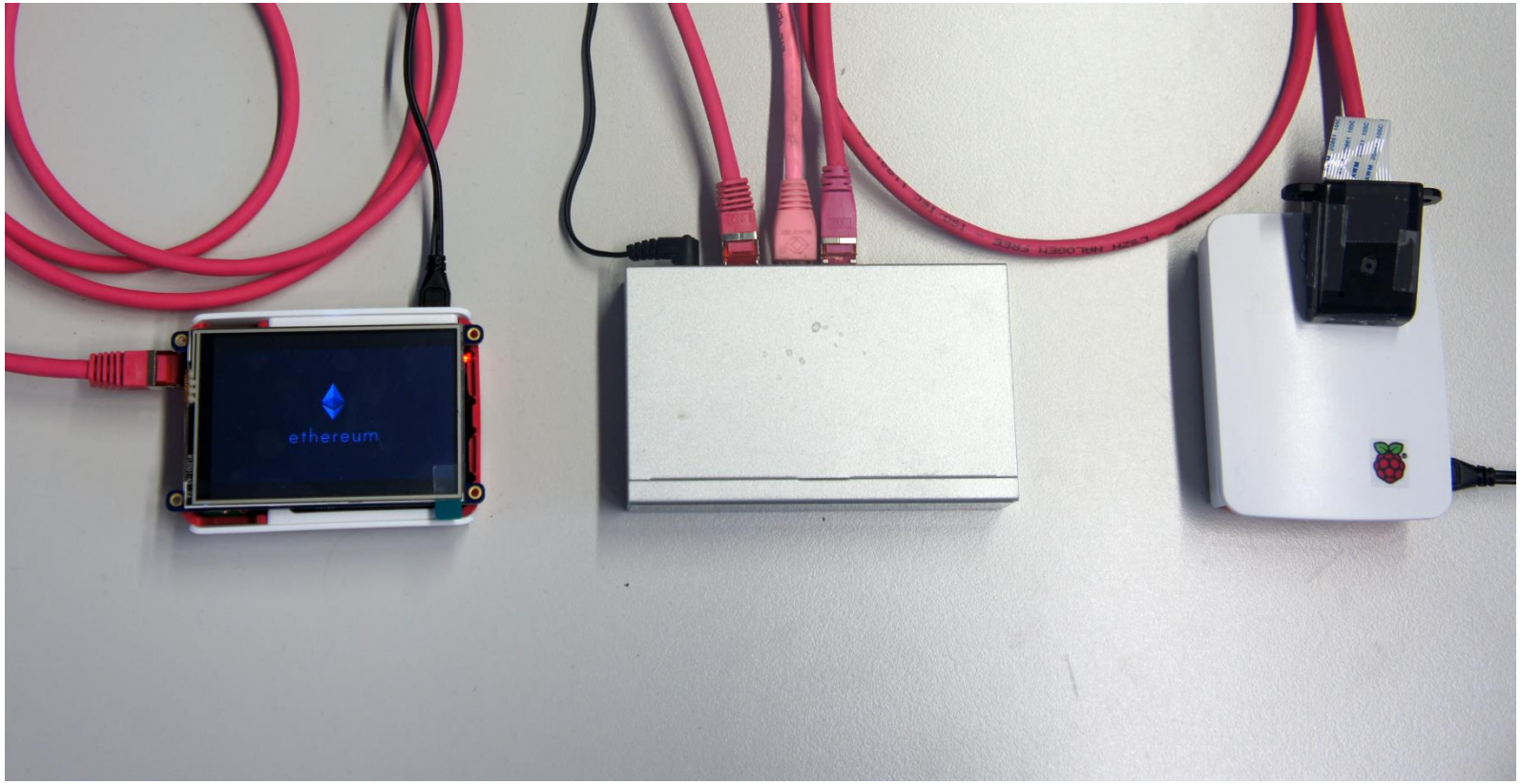


für Details siehe [SCS Whitepaper]

super computing systems

Demonstration

besuchen Sie uns am Stand für eine Live Demo!



Herausforderungen der praktischen Umsetzung

- **Ständig ändernde Umgebung**
  - API's ändern alle paar Monate
  - (Test) Chains verschwinden (Ethereum Ropsten), neue entstehen (Ethereum Kovan)

  ⇒Heute muss mit hohen Betriebsaufwänden gerechnet werden, um eine DApp auf einer Public Blockchain am Laufen zu halten.
- **Skalierbarkeit** (noch) nicht gegeben. (Anzahl Transaktionen pro Sekunde)
  - Es sind aber Lösungsansätze für Teile der möglichen Applikationn in Sicht: *Ethereum Raiden* (state channels), *Cosmos* (Blockchain Interoperabilität) oder *IOTA* (keine serielle Blockchain, sondern ein gerichteter, azyklischer Graph. Keine Transaktionsgebühren)
- **Datenschutz**
  - Private Transaktionen möglich mit kn-SNARKS. Zcash

Vorteile beim Einsatz von Blockchain Technologie

- Blockchains ermöglichen die sichere, dezentrale, unveränderliche Speicherung von Daten ohne vertrauenswürdige zentrale Instanz oder Inftrasturktur.
- Wichtige Informationen wie Zeitstempel oder Herkunft können bewiesen werden.
- Smart Contracts erlauben die automatisierte Abwicklung von Verträgen die in Blockchains als Programme gespeichert sind

Blockchains haben das Potential, verschiedene Industrien radikal zu verändern (z.b. Geldüberweisung ins Ausland)

Supercomputing Systems AG

alain.brenzikofer@scs.ch +41 43 456 16 00

Vision meets reality.