

BSI CRM & Blockchain

Einführung & mögliches Einsatzszenario

bsi·crm

Gemeinsam
BSI



SBB verkauft Bitcoin am Billettautomaten

Devisenhandel Das Projekt ist gestartet: Die SBB verkauft Bitcoins. An über 1000 Billettautomaten kann die Kryptowährung bezogen werden. Die Testphase dauert zwei Jahre.

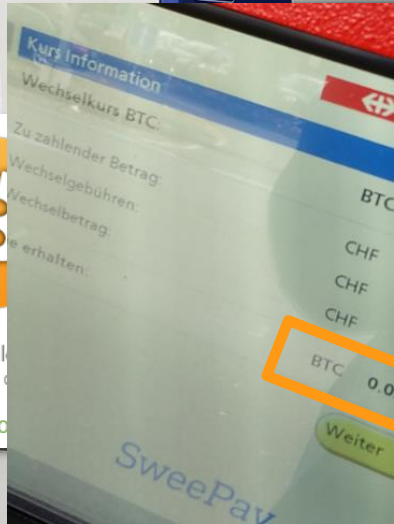
11.11.2016

Auf handelszeitung.ch suchen




MEISTGELESEN

1. Jetzt kommt das erste fliegende Auto der Welt
2. So treffen Milliardäre ihre Entscheidungen




Bitcoin

mBTC **26.45**
≈ CHF 18.55



Gratulation, du hast deine erste Zahlung erhalten! Hast du deine Wallet bereits gesichert, um dich gegen Verlust zu schützen?

▶ 14. November 12:25 ⋮
1Mk6 LVar nMt f **+ 26.45**
9YtU 316N qKQE
SM44 C3Ja 1e

◀ ANFORDERN SENDEN ▶ 

Nutzung auf eigene Gefahr. Lies die Sicherheitshinweise.

Technologie mit der wahrscheinlich größten Auswirkung auf die nächsten Jahrzehnte

„**Blockchain** stellt den Finanzsektor auf den Kopf“



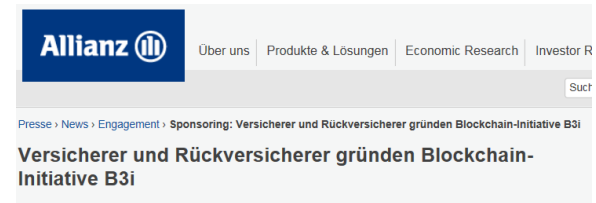
„...sehr vielversprechend mit Hinblick auf die Kostenreduzierung...“

Thomas Jordan: Präsident und Vorstandsvorsitzender der Schweizer Zentralbank

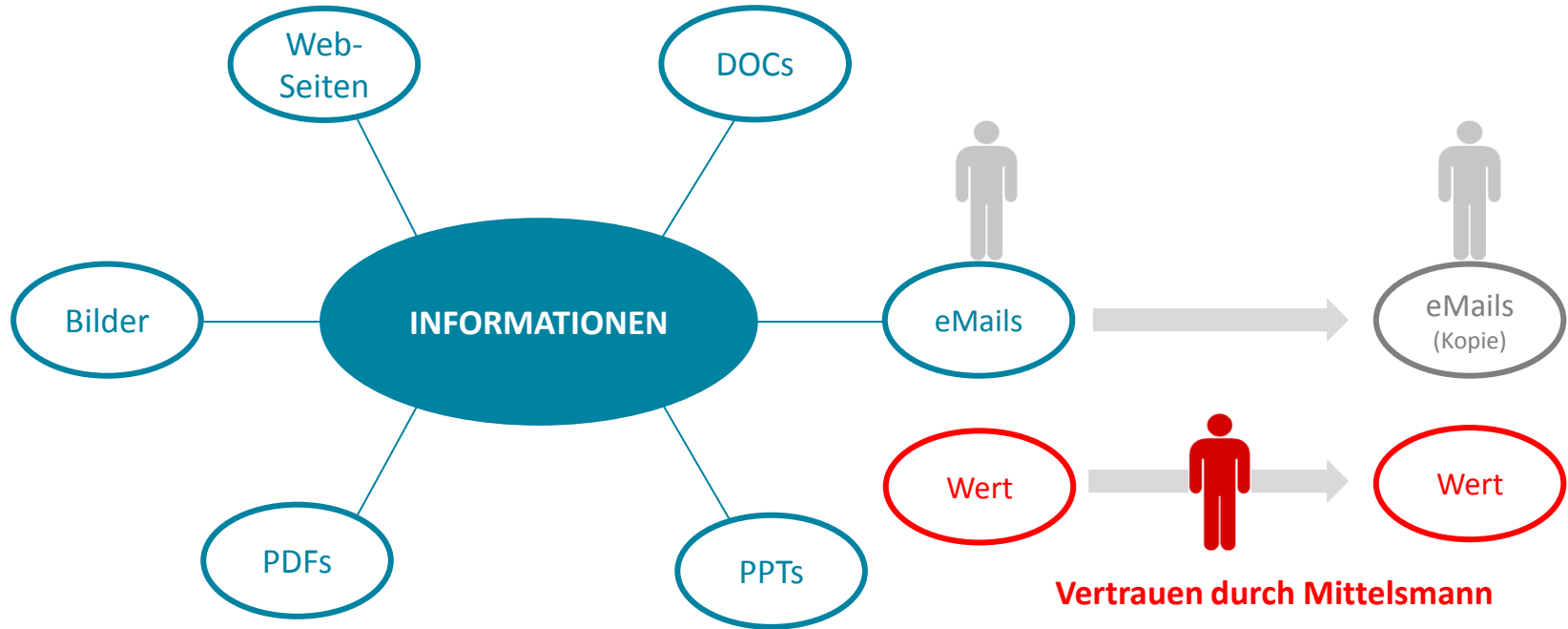
„**Versicherer und Rückversicherer gründen Blockchain-Initiative B3i**“

Ziele: Aufwand reduzieren... Informations-/Geldfluss beschleunigen...Überprüfbarkeit verbessern...

Aegon, Allianz, Munich Re, Swiss Re und Zurich

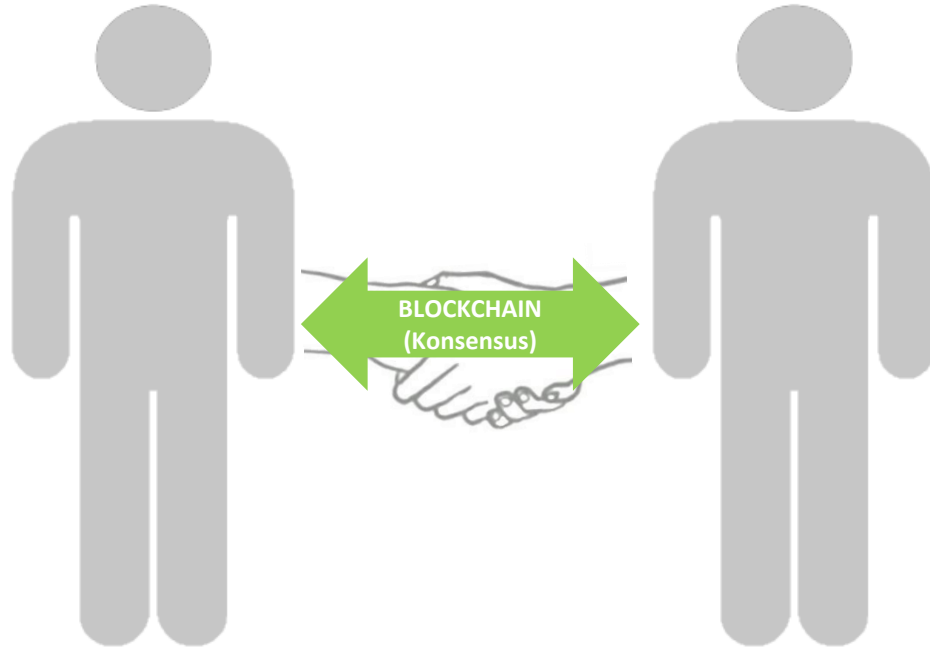


Internet für Informationen



Quelle des Beispiels: «How the Blockchain is changing money and business», Don & Alex Tapscott

Blockchain ersetzt Mittelsmann und schafft Vertrauen



durch kryptographisches Verfahren

Bitcoin (≠ Blockchain)

Etabliert eine neue Ära des Internets

2008 ist die **Finanzbranche kollabiert**

Satoshi Nakamoto realisiert ein Protokoll für elektronisches Geld

Digitale Werte (z.B. Cryptowährung) können **ohne Mittelsmann** ausgetauscht werden

Die **Vertrauensrolle** übernimmt die **Blockchain**



Preis: **\$ 713,40**

Marktvolumen: **\$ 11,1 Mrd.**

Transaktion (24h): **\$ 187,3 Mio.**

blockchain.info

Bitcoin verwendet die **Technologie Blockchain**

Bitcoin und Ethereum

Technische Einführung

Bitcoin

Kaffee bei Bob's



Adresse **1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA**
Betrag [฿] **0.015**
Name Empfänger **Bob's Café**

Was sind Bitcoin Adressen?

Eine Bitcoin Adresse entspricht einem **klassischen «Konto»**

Bitcoin Adressen sind **kodierte Zahlen**

- Beispiel: **1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA**
- Werden aus einem **privaten Schlüssel** berechnet
- Privater Schlüssel = 256-Bit Zufallszahl
- Im Prinzip genügen **«Münze, Papier und Bleistift»**

Wichtig

- Nur mit dem privaten Schlüssels lassen sich Bitcoins versenden
- Warnung: Privater Schlüssel verloren = Geld weg

Zurück zur Kaffeetransaktion

- Das Bitcoin-Netz bestätigt Kaffee TX nach ca 10 min.
- **Elemente** der TX

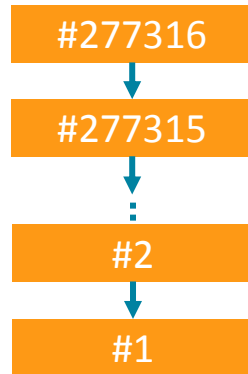
The screenshot shows a Bitcoin transaction page on blockchain.info. The URL is <https://blockchain.info/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a>. The page displays transaction details for ID 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2. It lists two outputs: one to address 1CdK9UzpbHBzqzX2A9JFP3Di4weBwqgmoQA (0.015 BTC) and another to address 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.0845 BTC). A green box indicates a total of 0.0995 BTC. A summary table shows transaction size (258 bytes), received time (2013-12-27 23:03:05), included in block 277316 (2013-12-27 23:11:54 + 9 minutes), and 159575 confirmations. An 'Inputs and Outputs' table shows a total input of 0.1 BTC, total output of 0.0995 BTC, fees of 0.0005 BTC, and an estimated BTC transacted of 0.015 BTC. Callouts point to 'Bob's Adresse' (1CdK9UzpbHBzqzX2A9JFP3Di4weBwqgmoQA), 'Preis Kaffee' (0.015 BTC), 'Meine Adresse' (1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK), and 'Link zum TX Block' (277316).

Summary		Inputs and Outputs	
Size	258 (bytes)	Total Input	0.1 BTC
Received Time	2013-12-27 23:03:05	Total Output	0.0995 BTC
Included In Blocks	277316 (2013-12-27 23:11:54 + 9 minutes)	Fees	0.0005 BTC
Confirmations	159575	Estimated BTC Transacted	0.015 BTC

Screenshot: blockchain.info

TX Blöcke und die Blockchain

- ➔ **Block #277316** mit der Kaffee TX, enthält noch 418 weitere TX
- ➔ **Link** zu Vorgängerblock



Block #277316	
Number Of Transactions	419
Output Total	10,322.07722534 BTC
Estimated Transaction Volume	777.75279147 BTC
Transaction Fees	0.09094928 BTC
Height	277316 (Main Chain)
Timestamp	2013-12-27 23:11:54
Difficulty	1,180,923,195.26
Bits	419668748
Size	218.629 KB
Version	2
Nonce	924591752
Block Reward	25 BTC

Hashes

Hash	0000000000000001b6b9a13b095e96db41c4928b97ef2d944a9b31b2cc7bdc4
Previous Block	000000000000002a7bbd25a417c0374cc55261021e8a9ca74442b01284f0569
Next	00

Network Propagation (Click To View)

Screenshot: blockchain.info

Bitcoin Mining

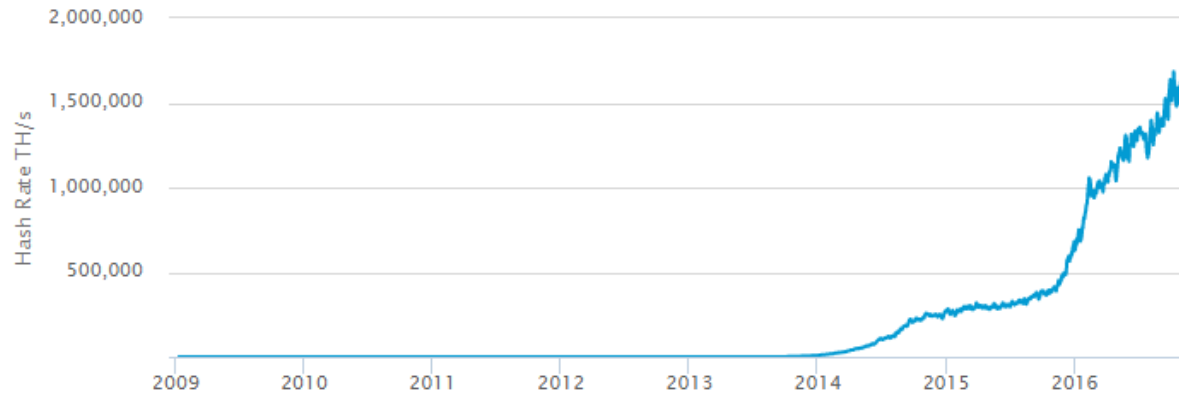
Wie neue Blöcke entstehen

1. Neue TX werden im Bitcoin Netzwerk via **Peer-to-Peer Technologie** verteilt
2. Alle Bitcoin Clients starten mit dem «**Mining**»
 - Sammeln aller «**pending**» TX in einem (lokalen) **Blockkandidaten**
 - Lösen des **Krypto-Rätsel** des Blockkandidaten
 - Um das Rätsel zu lösen müssen **VIELE Hashes** berechnet werden
 - Der schnellste Client gewinnt die **Belohnungssumme** und alle **TX Gebühren**
3. Der Gewinner-Client versendet seinen Block an das Bitcoin Netzwerk
4. Der Empfang eines neuen Blocks startet das nächste Rennen

Bitcoin Mining Infrastruktur

- Mining-Pools von Spezialrechnern (normale PC viel zu langsam)
- Stromkosten: Wieviele Hashes können pro KWh berechnet werden

Hashing Power über die Jahre



1.5×10^{18}

Rekapitulation Bitcoin

- Die Blockchain enthält alle TX seit Beginn
- Jeder Client hält eine aktuelle Kopie der Blockchain
- Mining-Clients «verbauen» TX in neuen Blöcken
- TX Historie kann nicht abgeändert werden (zu teuer)

Errungenschaften von Bitcoin

- Komplette dezentrale Währung (keine Zentralbank)
- «Gold Standard» unter Blockchain Technologien
- Sichere Plattform seit 2009
- Alles Open Source und Open Data

Ethereum

Vergleich mit Bitcoin



ethereum

Gemeinsamkeiten

- Lokale Clients mit kompletter Blockchain
- Prinzip von Transaktionen und Mining
- Virtuelle Währung (Ether)
- Open Source und Open Data

Unterschiede / Ergänzungen

- **Ethereum**: Neu und experimentierfreudig – **Bitcoin**: Konservativ
- Es gibt auch **Smart Contracts** (Programme)

Smart Contracts

Wie geht das?

1. Smart Contracts können mit **Solidity** (Programmiersprache) erstellt werden
2. Übersetzung des Contracts in **Bytecode**
3. Der Bytecode wird in eine TX gepackt und vom Besitzer signiert
4. Ein **Ethereum Client** sendet die TX an das Netzwerk
5. Mining und Update der Blockchain im Ethereum Netzwerk

Smart Contract und Geschäftsanwendung

Geschäftsanwendung

BSI CRM



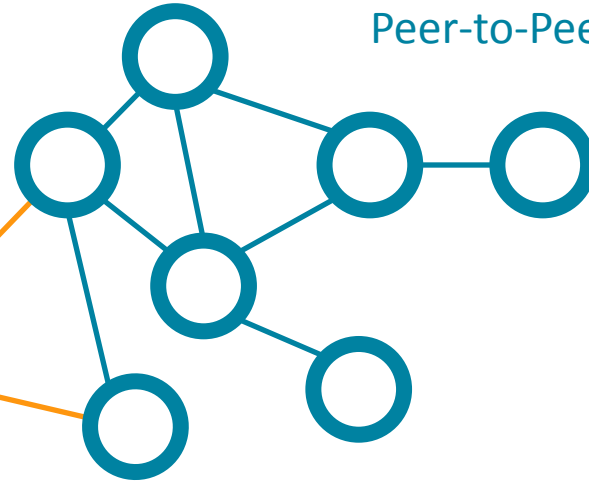
Interface
RPC

Lokaler Client
geth



Ethereum

Peer-to-Peer Netz



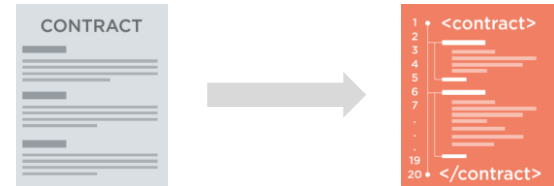
CRM & Blockchain

mögliches Einsatzszenario

Smart Contracts ermöglichen neue Einsatzszenarien

- Transaktionsprotokoll
 - **Kontrolliert** Vertragsbedingungen
 - **Führt** Vertragsbestimmungen aus
 - **Automatisiert**
 - **Permanent** („live“) verfügbar in der Blockchain (weltweit)

- Ermöglicht **neue Services** und **Geschäftsmodelle**
- Mit **großem Potenzial** bestehende Modelle zu optimieren



Fallbeispiel Lena Meier

KW46: Geschäftsreise (Ausland)



Unfall!!

KW47: Kinder zur Schule bringen



19./20.11.: Kurzurlaub



Blockchain ermöglicht folgendes Szenario



Unfall!!

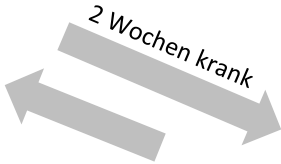
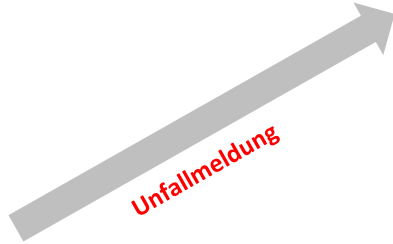
Notruf



Smart Insurance (KV) regelt:

- Versicherungsschutz
- Abrechnung

Unfallmeldung



2 Wochen krank

Profil - Lena Meier
(Blockchain)



1KDmTeq1akhdasRTE1ddZF5ss



Smart Planning:

- informiert Arbeitgeber & Familie
- organisiert Rücktransport
- regelt Termine
- bucht autonomes Auto



Smart Mobility regelt:

- ggf. Ersatzfahrzeug
- Bezahlung



Smart Insurance (KFZ) regelt:

- Abschleppung
- Reparatur
- Schadensregulierung
- Abrechnung



Planung Lena Meier automatisch aktualisiert

Rücktransport organisiert ✓



Schaden reguliert ✓

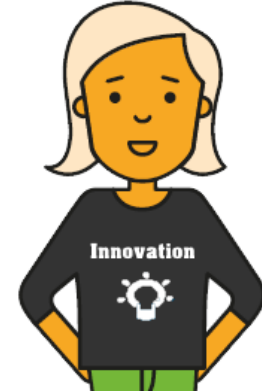


Kinder kommen zur Schule ✓



Quelle: Google

Professionell versorgt ✓



Kurzurlaub verschoben ✓



Blockchain ermöglicht:

Automatisierung, globale Verfügbarkeit, Flexibilität, Datenschutz



Hallo Lena Meier

Kostenübersicht >

Entwicklung der Leistungen >

1'700 Abgerechnet

1'300 Restbetrag

→ Zur Jahresübersicht



Auf einen Klick

- > Meine Adresdaten aktualisieren
- > Dokumente für Steuererklärung anfragen
- > Eine Schadenmeldung erfassen
- > Ein neues Produkt hinzufügen
- > Beratungstermin anfragen

Meine Buchungen Smart Contracts

Aktivität	Smart Contract	Zusatzkosten	Status
Unfall melden	Smart Mobility	-	Ok
Versicherungsschutz abwickeln	Smart Insurance-KV	2.300.-	Prüfung Bestätigung
Familie / Arbeitgeber informiert Termine geregelt	Smart Planning	-	Ok
Mobilität sicherstellen	Smart Mobility	Ersatzfahrzeug Rücktransport Auton. KFZ: 200.-	Ok
Schaden reguliert	Smart Insurance-KFZ	Selbstb.: 900.- Gesamt: 8.400.-	Prüfung Bestätigung

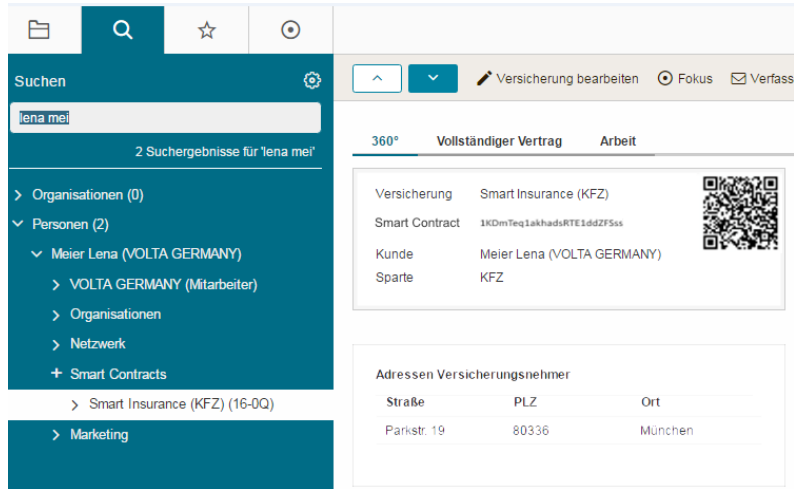
Neue Dokumente

ALLE >

- 28.3.2016 **Vertragsanpassung** >
- 28.2.2016 **Prämienübersicht 2015** >
- 15.01.2016 **Motorrad-Versicherung 16/1234** >
- 10.01.2016 **Factsheet Vorsorgeplanung** >

BSI CRM

Sicht: Versicherungsunternehmen



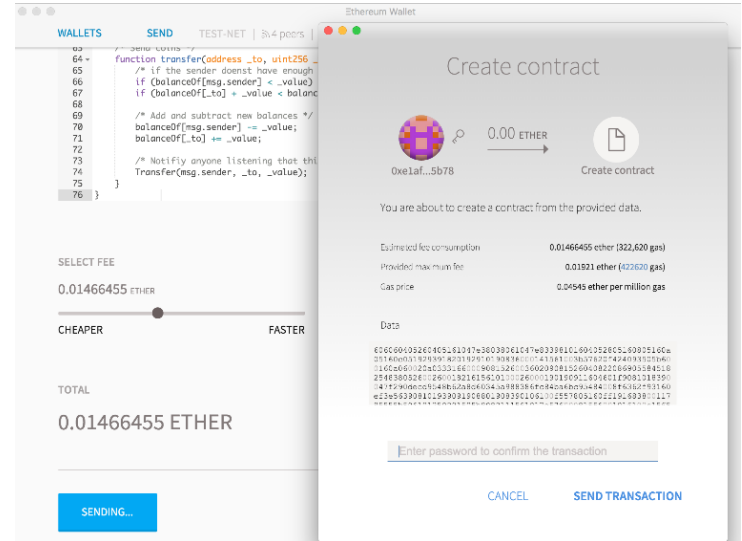
The screenshot shows a CRM interface with a search bar containing 'lena mei' and two search results. The main view displays details for a 'Vollständiger Vertrag' (Complete Contract) for 'Smart Insurance (KFZ)'. It includes a QR code, contract ID '1KdM7eqLakhadsRTE3ddZF5ss', customer name 'Meier Lena (VOLTA GERMANY)', and address details for the policyholder.

Adressen Versicherungsnehmer		
Straße	PLZ	Ort
Parkstr. 19	80336	München

Interessenten & Kundenmanagement
Verkauf Smart Insurance

Blockchain

Vertragsabwicklung
(Smart Contracts)



The screenshot shows an Ethereum wallet interface with a 'Create contract' dialog box. The dialog displays a smart contract code snippet for a transfer function. The transaction details show a fee of 0.01466455 ETH and a gas price of 0.04543 ether per million gas. The total amount to be sent is 0.01466455 ETH.

```
function transfer(address _to, uint256  
64+ /* if the sender doesn't have enough  
65 (if (balanceOf[msg.sender] < _value)  
66 if (balanceOf[_to] + _value < balanc  
67  
68  
69 /* Add and subtract new balances */  
70 balanceOf[msg.sender] -= _value;  
71 balanceOf[_to] += _value;  
72  
73 /* Notify anyone listening that thi  
74 Transfer(msg.sender, _to, _value);  
75  
76 }
```

(Ethereum)

CRM und Blockchain (Integration)

Interessenten, Kundenmanagement
& Verkauf



Klassische IT-Lösung
(zentralisiert, Austausch von Informationen)

Automatisierte Vertragsabwicklung



Dezentrale Lösung
(dezentral, Austausch von Wert)

CRM & Blockchain

Q&A

**Wie geht`s weiter?
Dinner Party, Cheers!**

Vielen Dank

Christoph Langewisch & Matthias Zimmermann

Christoph.langewisch@bsi-software.com matthias.zimmermann@bsi-software.com, [@ZimMatthias](https://twitter.com/ZimMatthias)