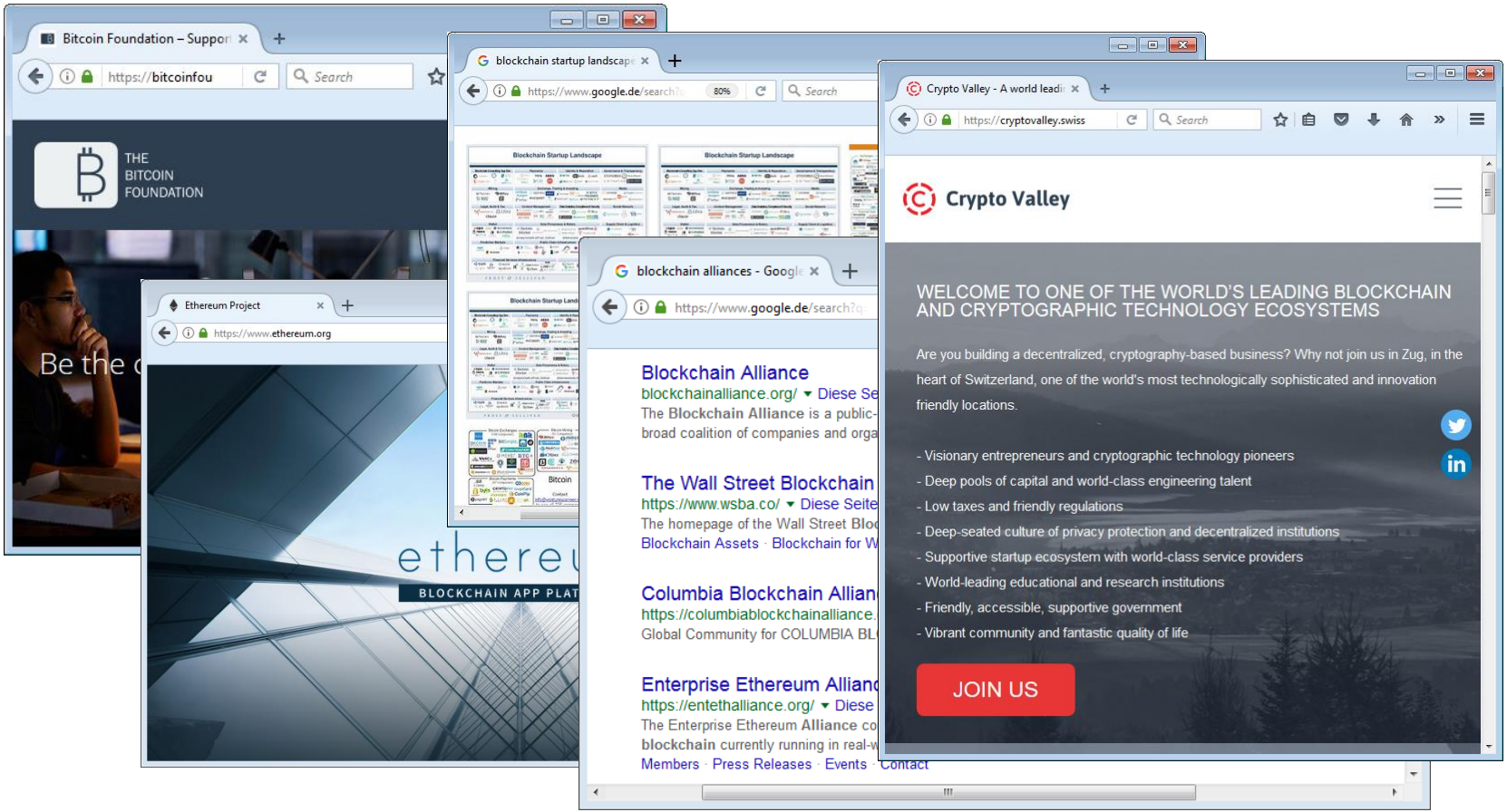
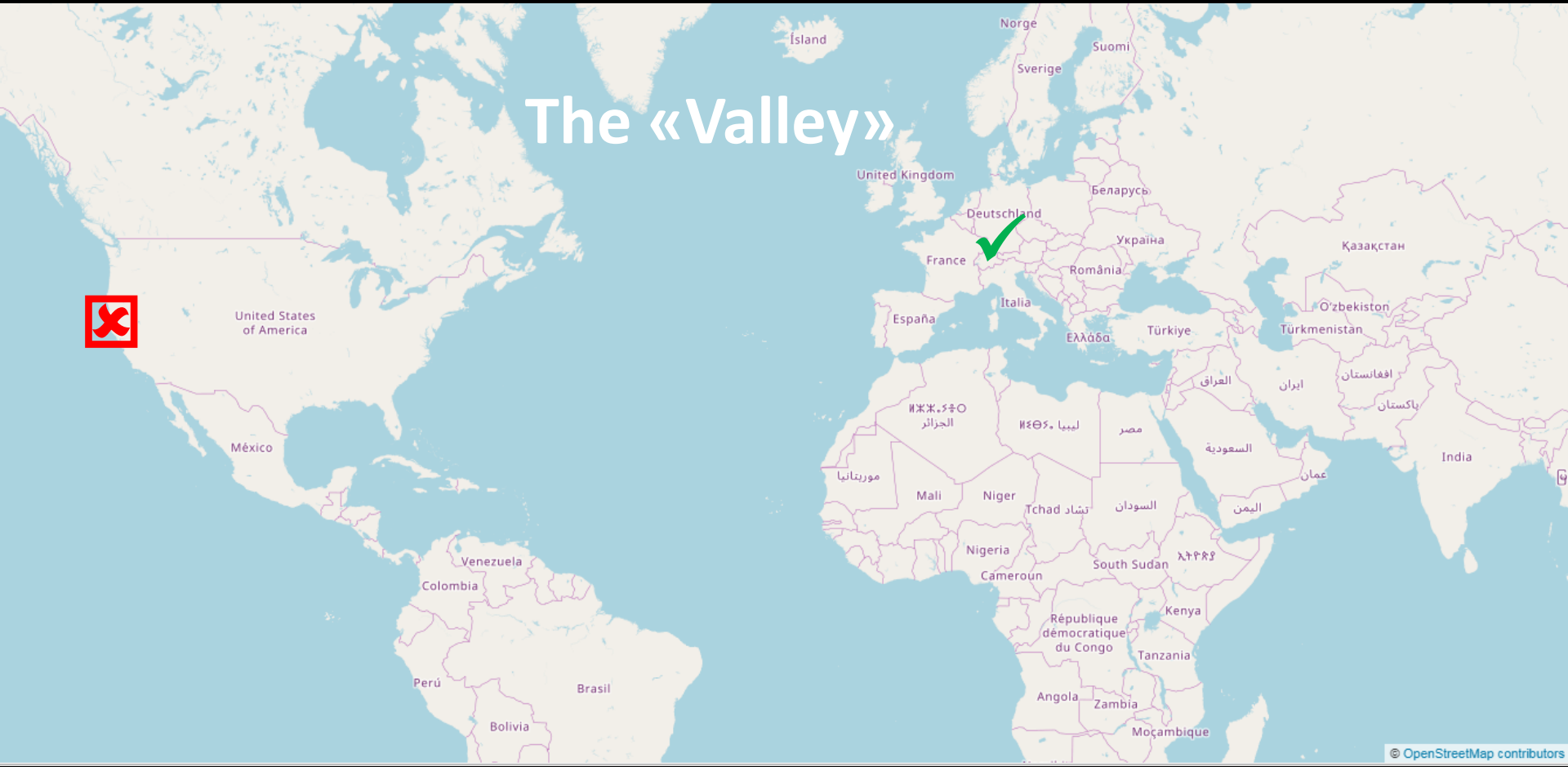
Blockchain, Ethereum and Business Applications

@ZimMatthias Matthias Zimmermann
BSI Business Systems Integration AG


Bitcoin Foundation – Suppor
https://bitcoinfou
Search
THE
BITCOIN
FOUNDATION
Be the
Ethereum Project
https://www.ethereum.org
ethereu
BLOCKCHAIN APP PLAT
blockchain startup landscape
https://www.google.de/search
80%
Search
Blockchain Startup Landscape
Blockchain Startup Landscape
Bitcoin
blockchain alliances - Google
https://www.google.de/search
Blockchain Alliance
blockchainalliance.org/ ▾ Diese Se
The Blockchain Alliance is a public-
broad coalition of companies and orga
The Wall Street Blockchain
https://www.wsba.co/ ▾ Diese Seite
The homepage of the Wall Street Bloc
Blockchain Assets · Blockchain for W
Columbia Blockchain Allian
https://columbiablockchainalliance.
Global Community for COLUMBIA BL
Enterprise Ethereum Allianc
https://entethalliance.org/ ▾ Diese
The Enterprise Ethereum Alliance co
blockchain currently running in real-w
Members · Press Releases · Events · Contact
Crypto Valley - A world leadi
https://cryptovalley.swiss
Search
Crypto Valley
WELCOME TO ONE OF THE WORLD'S LEADING BLOCKCHAIN AND CRYPTOGRAPHIC TECHNOLOGY ECOSYSTEMS
Are you building a decentralized, cryptography-based business? Why not join us in Zug, in the heart of Switzerland, one of the world's most technologically sophisticated and innovation friendly locations.
- Visionary entrepreneurs and cryptographic technology pioneers
- Deep pools of capital and world-class engineering talent
- Low taxes and friendly regulations
- Deep-seated culture of privacy protection and decentralized institutions
- Supportive startup ecosystem with world-class service providers
- World-leading educational and research institutions
- Friendly, accessible, supportive government
- Vibrant community and fantastic quality of life
JOIN US

The «Valley»


Ísland
Norge
Suomi
Sverige
United Kingdom
Беларусь
Deutschland
Україна
France
România
Italia
España
Ελλάδα
Türkiye
Қазақстан
O'zbekiston
Türkmenistan
United States of America
العراق
ایران
افغانستان
پاکستان
الجزائر
ليبيا
مصر
السعودية
India
عمان
موريتانيا
Mali
Niger
Tchad تشاد
السودان
اليمن
México
Nigeria
South Sudan
Cameroun
Venezuela
Colombia
Kenya
République démocratique du Congo
Tanzania
Perú
Brasil
Angola
Zambia
Bolivia
Moçambique
© OpenStreetMap contributors

Blockchain Market

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	$96,108,095,812	$5779.73	$1,929,760,000	16,628,475 BTC
2	Ethereum	$31,326,302,991	$329.24	$482,471,000	95,147,607 ETH
3	Ripple	$9,936,089,410	$0.257869	$866,836,000	38,531,538,922 XRP *
4	Bitcoin Cash	$5,864,609,962	$351.12	$346,000,000	16,702,438 BCH
5	Litecoin	$3,358,412,564	$62.88	$188,348,000	53,412,332 LTC
6	Dash	$2,307,274,645	$302.54	$38,470,400	7,626,321 DASH
7	NEM	$2,025,387,000	$0.225043	$8,065,810	8,999,999,999 XEM *
8	Monero	$1,451,708,799	$95.32	$31,838,500	15,229,142 XMR

List by the International Monetary Fund (Partial forecasted estimates for 2017)[5]

Rank	Country	GDP (millions of Int$)
	World	**126,687,917**
1	China[n 1]	23,194,411
—	*European Union*[n 2]	20,852,702
2	United States	19,417,144
84	Croatia	100,006
85	Côte d'Ivoire	95,887
125	Macedonia	31,924
126	Cyprus	31,093

elizabeth stark gefällt das

Neil Woodfine 聂尔 @nwoodfine · 9 Std.

Understanding bitcoin VS. when to buy and when to sell

Original (Englisch) übersetzen

23 357 818

Towards understanding Bitcoin …

«history's first» Blockchain

- Satoshi Nakamoto (?)
- White Paper 2008
- Open Source Software 2009

Coffee at Bob‘s

Source: «Mastering Bitcoin», *Andreas M. Antonopoulos*

What is a Bitcoin Address?

Addresses == **«Accounts»**

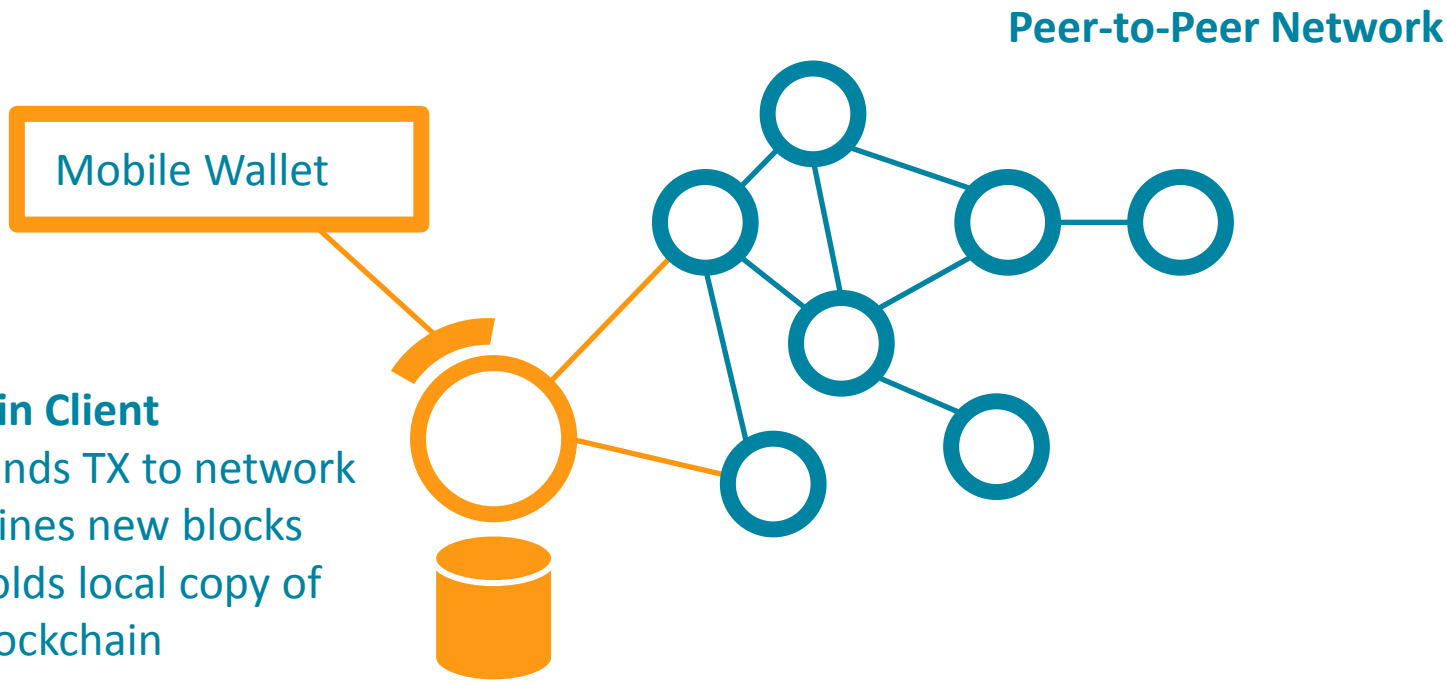
Encoded Numbers

- ➔ Example: `1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA`
- ➔ Derived from a **public/private key pair**

Getting, using and loosing it

- ➔ Create your own addresses, no need to ask anyone
- ➔ No ID required, no showing up at local branch, …
- ➔ To send Bitcoins you need your private Key
- ➔ **You loose your private key → you loose your money**

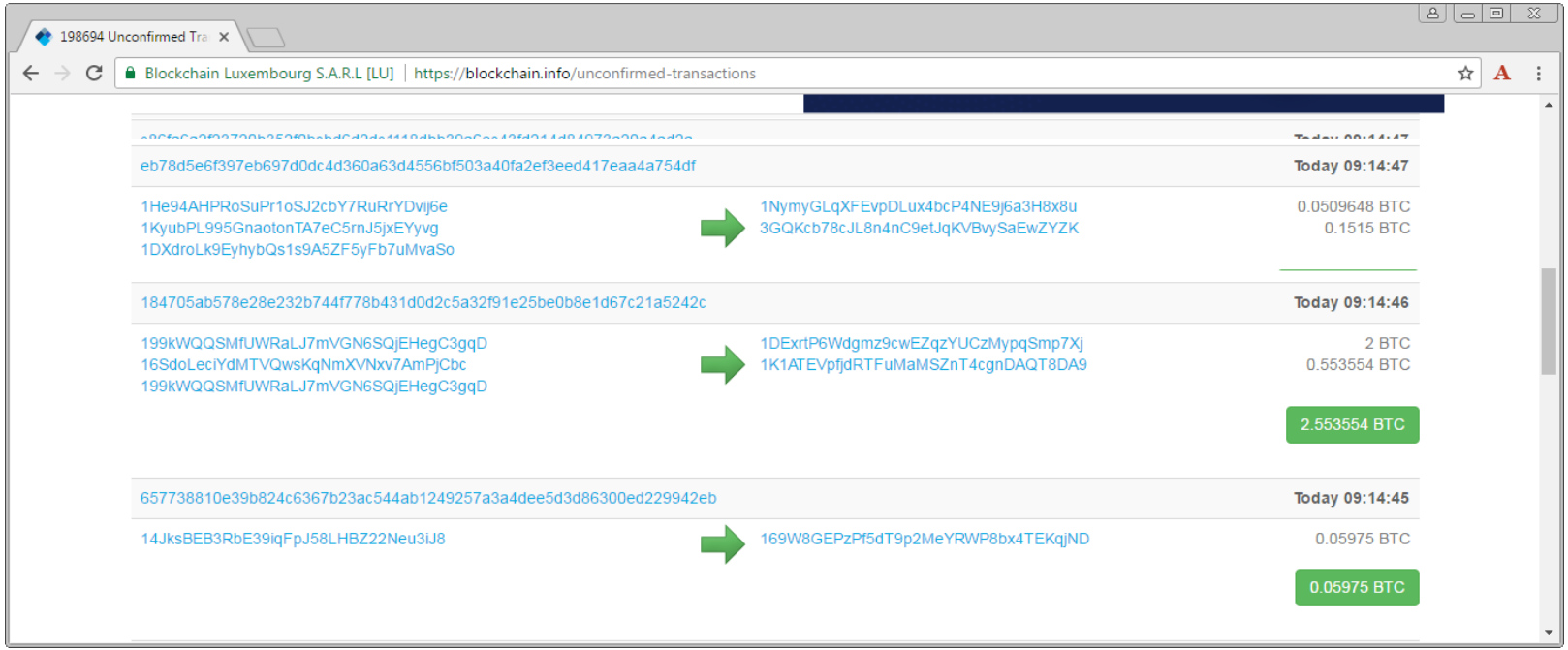
Bitcoin Network



Bitcoin Client

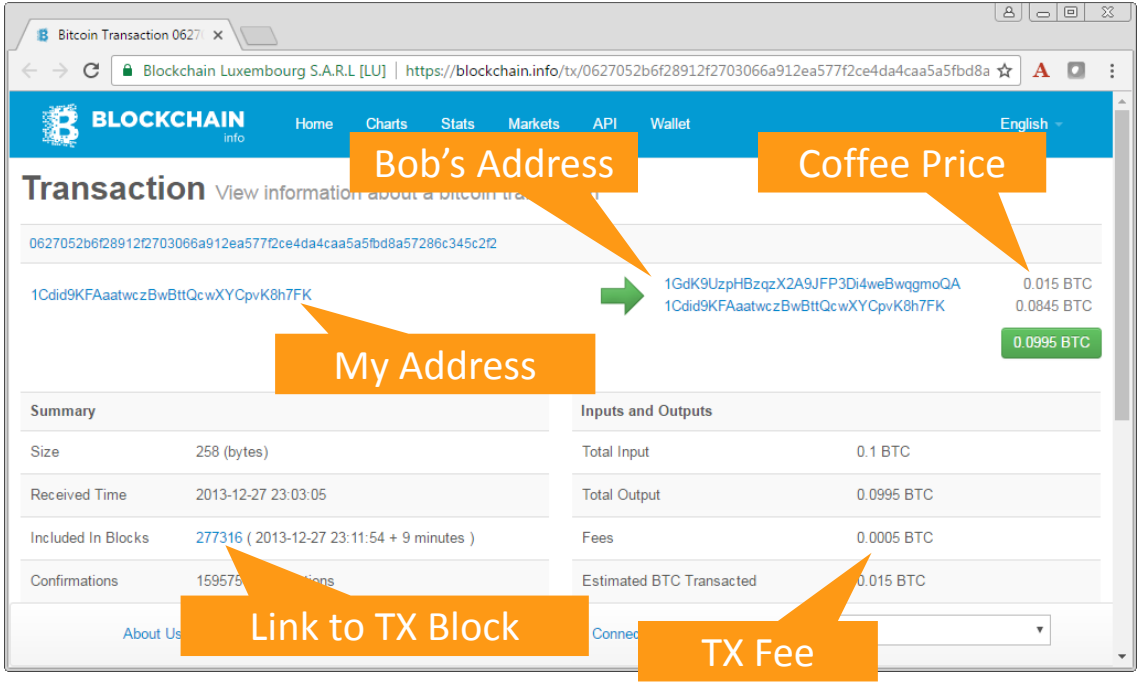
- Sends TX to network
- Mines new blocks
- Holds local copy of blockchain

Distribution of unconfirmed TX



The Coffee Transaction

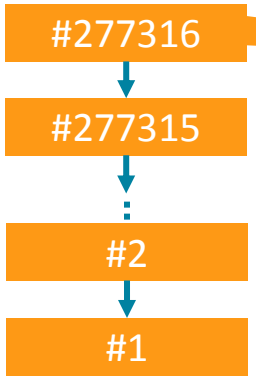
- To confirm TX:
  - TX mined into block
  - 5 new blocks on top
- Network mines TX in ~ 10 min.
- Sometimes this takes hours …

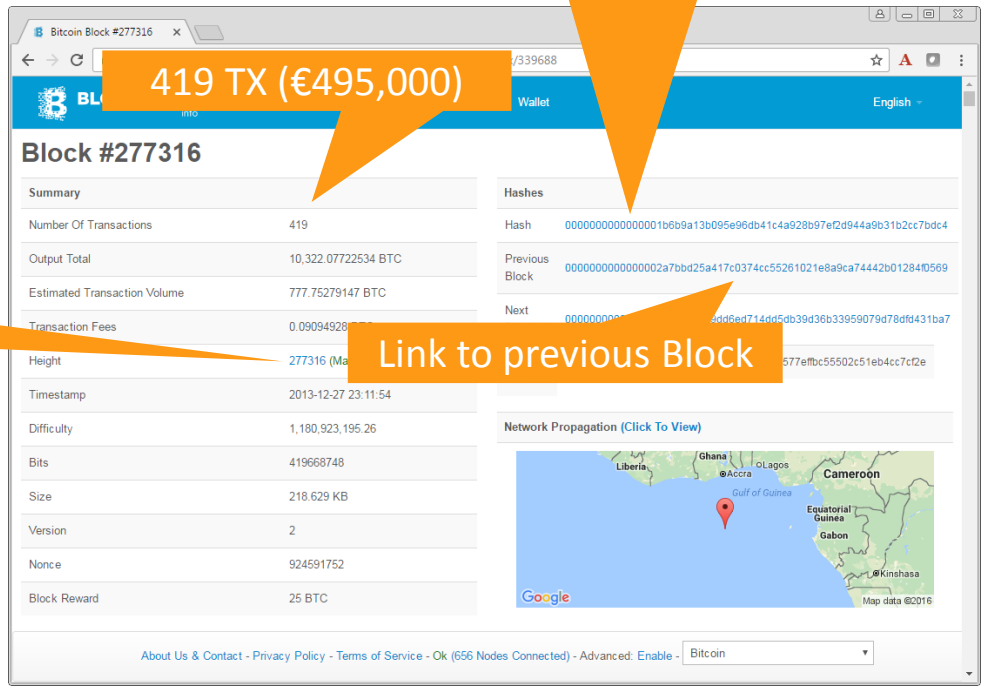


Screenshot: blockchain.info

TX Blocks and the Blockchain

- **Block** #277316
  includes coffee TX





Screenshot: blockchain.info

From Transactions to Blocks (Mining)

1. New TX are propagated through Bitcoin **peer-to-peer network**
2. Bitcoin client receive new TX and add it to local **«mempool»**
3. Client starts to **«mine»** transactions:
   - Assemble TX from mempool to **block candidate**
   - Starts to solve the block candidate's **crypto challenge**
   - Client solving the challenge first, gets **block reward** and all **TX fees**
3. Winning client sends the new block to its peers
4. Arrival of new block triggers the next challenge

Block Hashes and Crypto Challenge

```
mzi@BSI ~/Desktop/oss/events/2017/jug_blockchain_2017

$ java DummyBitcoinMiner 1
…
B37060F28617A5DFA3DB9A3D547663B3:I am Satoshi Nakamoto:lubf -> CF6BB3C636DF380E357E28271D948BBC
B37060F28617A5DFA3DB9A3D547663B3:I am Satoshi Nakamoto:jauj -> E6F1EB09AEF0BF331261B64E1C798EAB
B37060F28617A5DFA3DB9A3D547663B3:I am Satoshi Nakamoto:dwpt -> 0CEE0B104F133062073BDD810D3DB6CF
Success with nonce 'dwpt' for difficulty '0'. Hashes calculated: 29

$ java DummyBitcoinMiner 4
…
B37060F28617A5DFA3DB9A3D547663B3:I am Satoshi Nakamoto:quyc -> 89BD526A2DF7EBF41ACD227BFC6B78FE
B37060F28617A5DFA3DB9A3D547663B3:I am Satoshi Nakamoto:ceaw -> 0000AD30B2DDD8A773B8E5AABB5282AD
Success with nonce 'ceaw' for difficulty '0000'. Hashes calculated: 11584
```

Difficulty Oct’ 17: 18 leading zeros

Bitcoin Recap

Bitcoin Success

- ➔ Completely decentral currency (no need for banks)
- ➔ Open Source (GitHub) and Open Data (complete TX history)
- ➔ First successful implementation of any crypto currency
- ➔ «Gold Standard» since 2009
- ➔ Record price levels in 2017

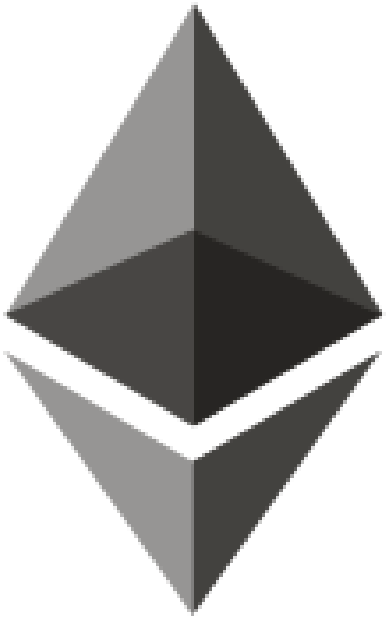
Bitcoin Challenges

- ➔ Scaling debate/war
- ➔ Declining market share (Ethereum, …)

Bitcoin Resources

https://github.com/bitcoin/bitcoin https://github.com/bitcoinbook/bitcoinbook

Ethereum



Currency and Smart Contracts

- 2014 by Vitalik Buterin
- Distributed VM (Turing complete)
- Open source software

Ethereum vs Bitcoin

Common Traits

- ➔ Virtual currency
- ➔ Peer-to-peer network/nodes with local blockchain
- ➔ Concepts of addresses, transactions, mining

Main Differences

- ➔ **Specification** with different implementations (Bitcoin reference client)
- ➔ **Smart contracts** and Ethereum virtual machine
- ➔ **Gas** to execute smart contracts and TX

Gas

What is gas?

- ➔ Unit to pay mining nodes
- ➔ Unit of gas has price in Ethers

What can we buy with gas?

- ➔ Pay TX fees
- ➔ Execute smart contracts
- ➔ Computations performed by clients: **Ethereum Virtual Machine** (EVM)
- ➔ EVM is working as long as there is gas
- ➔ **Example 1**: **SHA3** computation costs 30 gas
- ➔ **Example 2**: EVM always terminates (stays in **infinite loop** until gas runs out)

Ethereum Smart Contracts

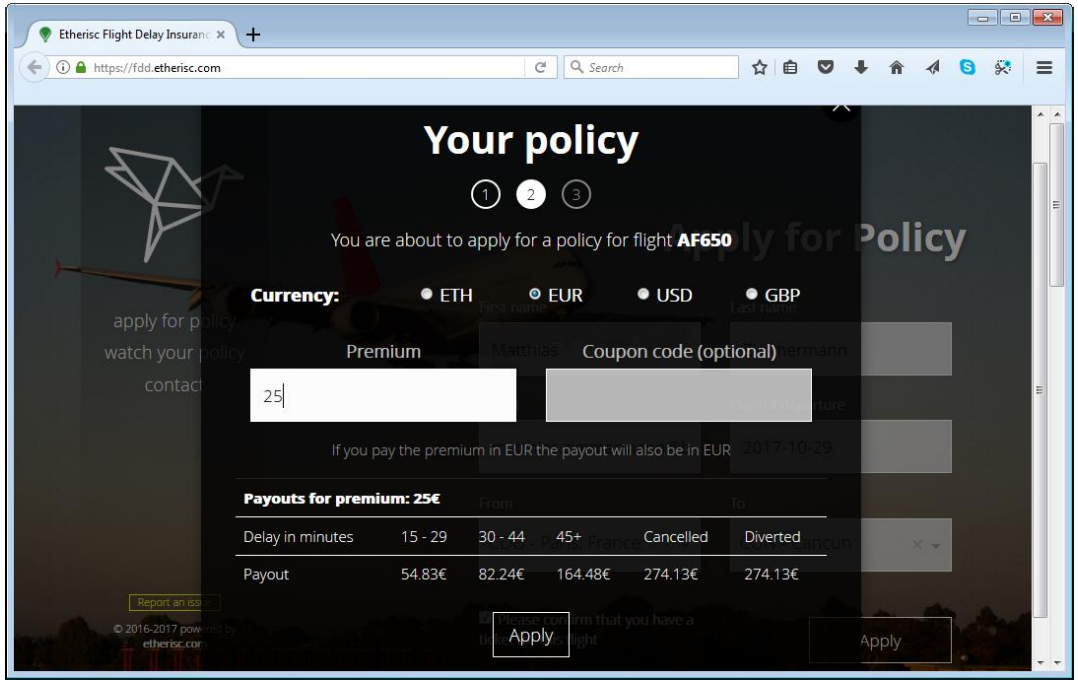
What is a Smart Contract?

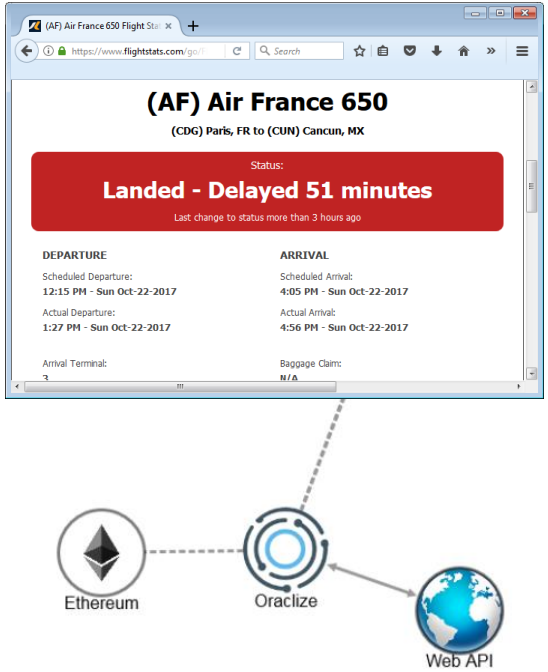
- ➔ Code written in high level language «Solidity»
- ➔ Code is compiled into byte code
- ➔ Byte code executed on client by EVM
- ➔ Has owner
- ➔ Has address
- ➔ Can hold currency

Examples

1. Flight delay insurance
2. «Truly» autonomous cars

Flight Delay App





https://fdd.etherisc.com http://oraclize.it http://www.flightstats.com

«Truly» Autonomous Cars

Uber's self-driving cars are now picking up passengers in Arizona

Tempe or bust

by Andrew J. Hawkins | @andyjayhawk | Feb 21, 2017, 1:55pm EST

SHARE TWEET LINKEDIN

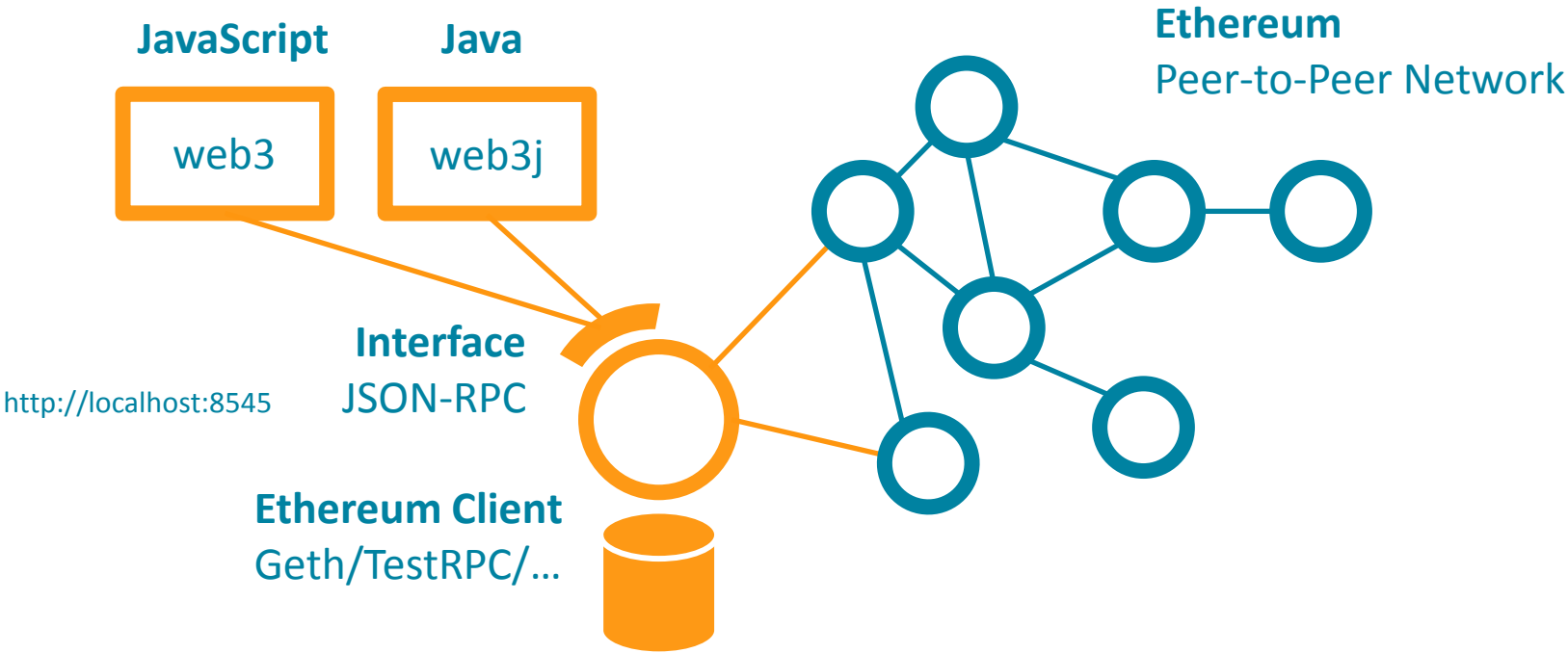
In 2017 RWE introduces charging stations connected to Ethereum blockchain

- ➔ **Smart contract**: Order car to transport people (fees go to car contract)
- ➔ **Smart contract**: Car pays for energy/services (car pays with it's own funds)

http://www.trustnodes.com/2017/04/29/germanys-energy-giant-launches-100s-ethereum-based-electric-cars-charging-stations
https://www.theverge.com/2017/2/21/14687346/uber-self-driving-car-arizona-pilot-ducey-california

«Greeter» with web3
Smart Contract Hello World

Ethereum and Applications



«Hello World» (greeter.sol)

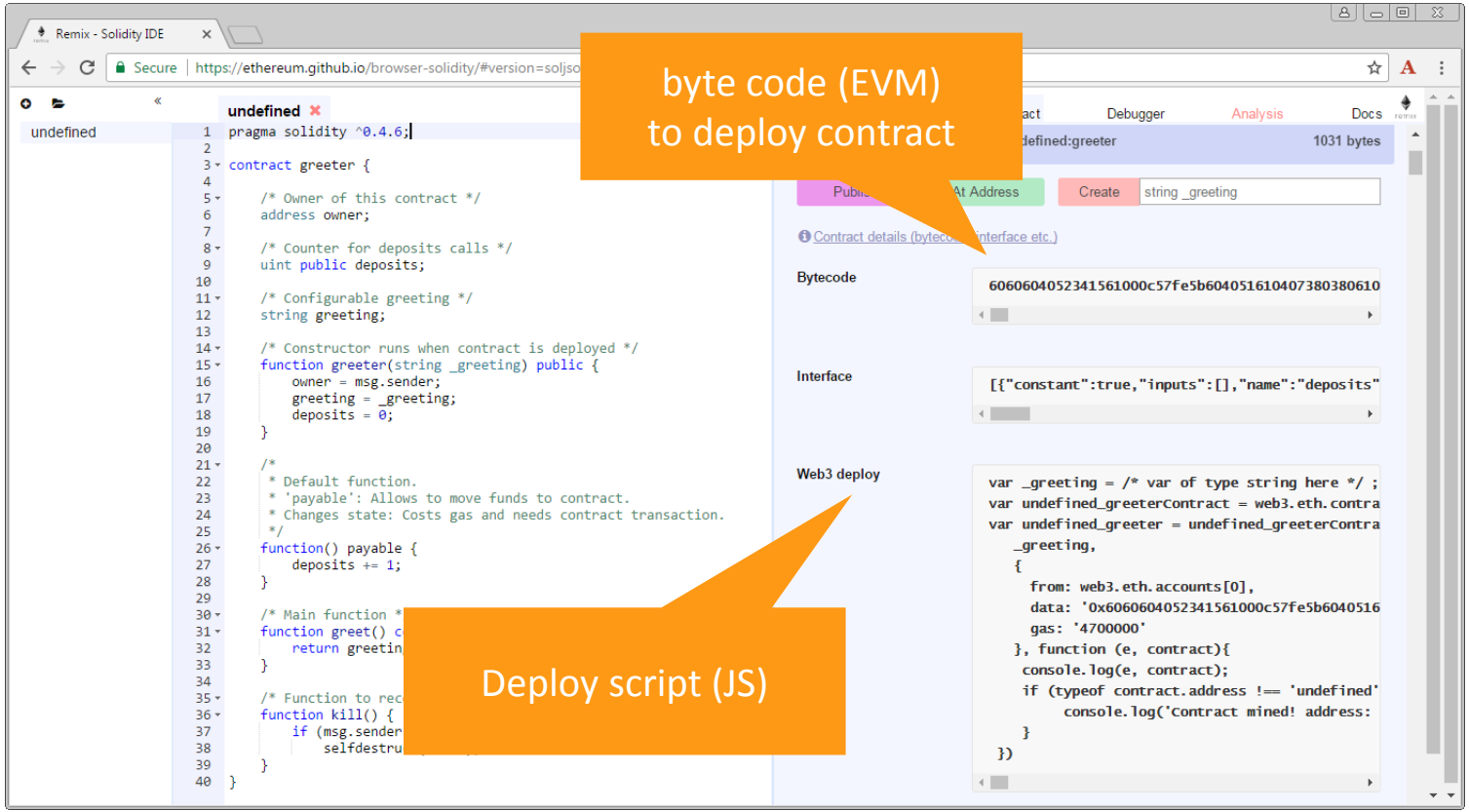
```
contract greeter {

    /* Owner of this contract */
    address owner;

    /* Configurable greeting */
    string greeting;

    /* Constructor runs when contract is deployed */
    function greeter(string _greeting) public {
        owner = msg.sender;
        greeting = _greeting;
    }

    /* Main function */
    function greet() constant returns (string) {
        return greeting;
    }

    /* Function to recover the funds on the contract */
    function kill() {
        if (msg.sender == owner)
            selfdestruct(owner);
    }
}
```

```
contract greeter {

    /* Counter for deposits calls */
    uint public deposits;

    /*
     * Default function.
     * 'payable': Allows to move funds to contract.
     * Changes state: Costs gas and needs contract transaction.
     */
    function() payable {
        deposits += 1;
    }

    /*
     * Returns number of deposits.
     * 'const': This function does not change contract state.
     * Does not change state and does not cost gas/fees.
     * No contract transaction needed.
     */
    function deposits() constant returns (uint) {
        return deposits
    }

    address owner;
    string greeting;

    function greeter(string _greeting) public { deposits = 0; ... }
    function greet() constant returns (string) { ... }
    function kill() { ... }
}
```

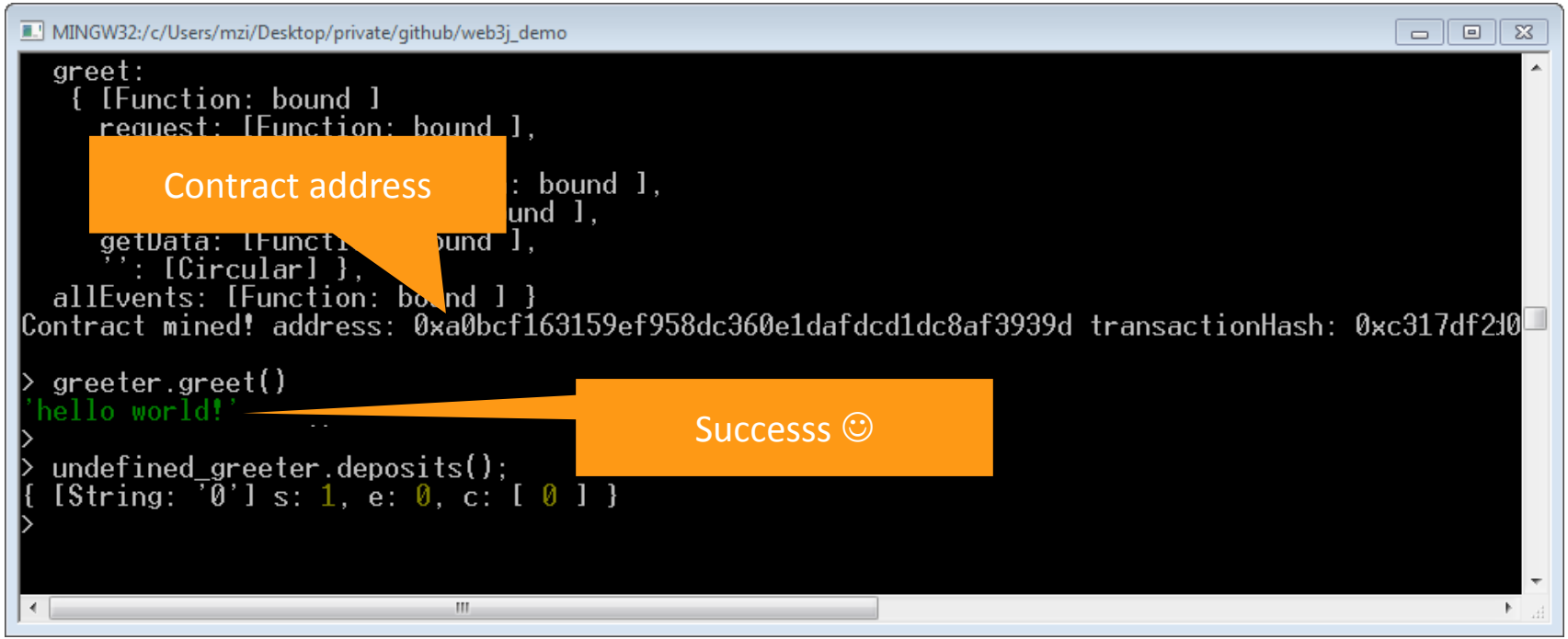
greeter.sol

+ additional state
+ ‘payable’

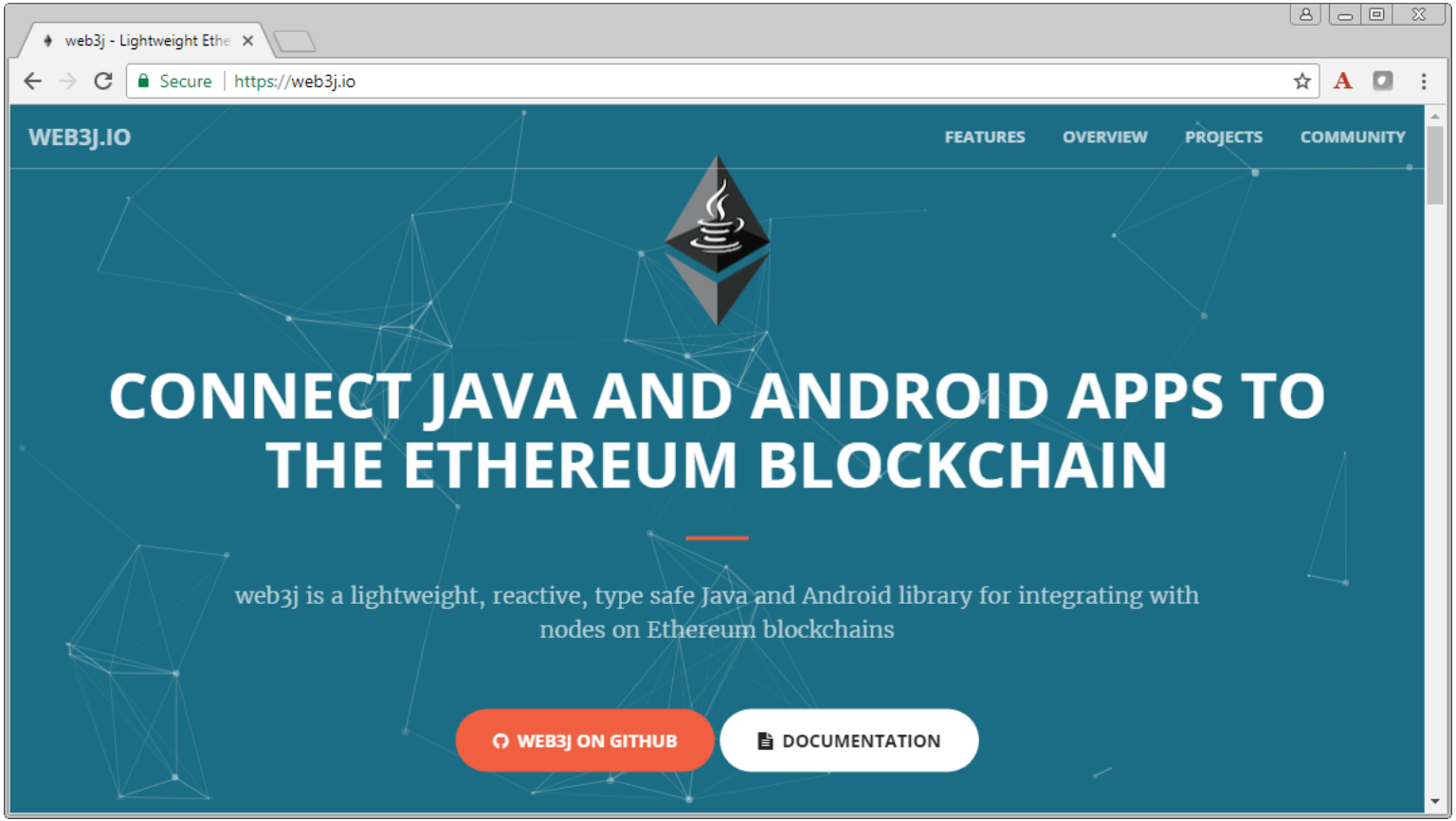
Solidity Compiler (online)



Deploy (Console)

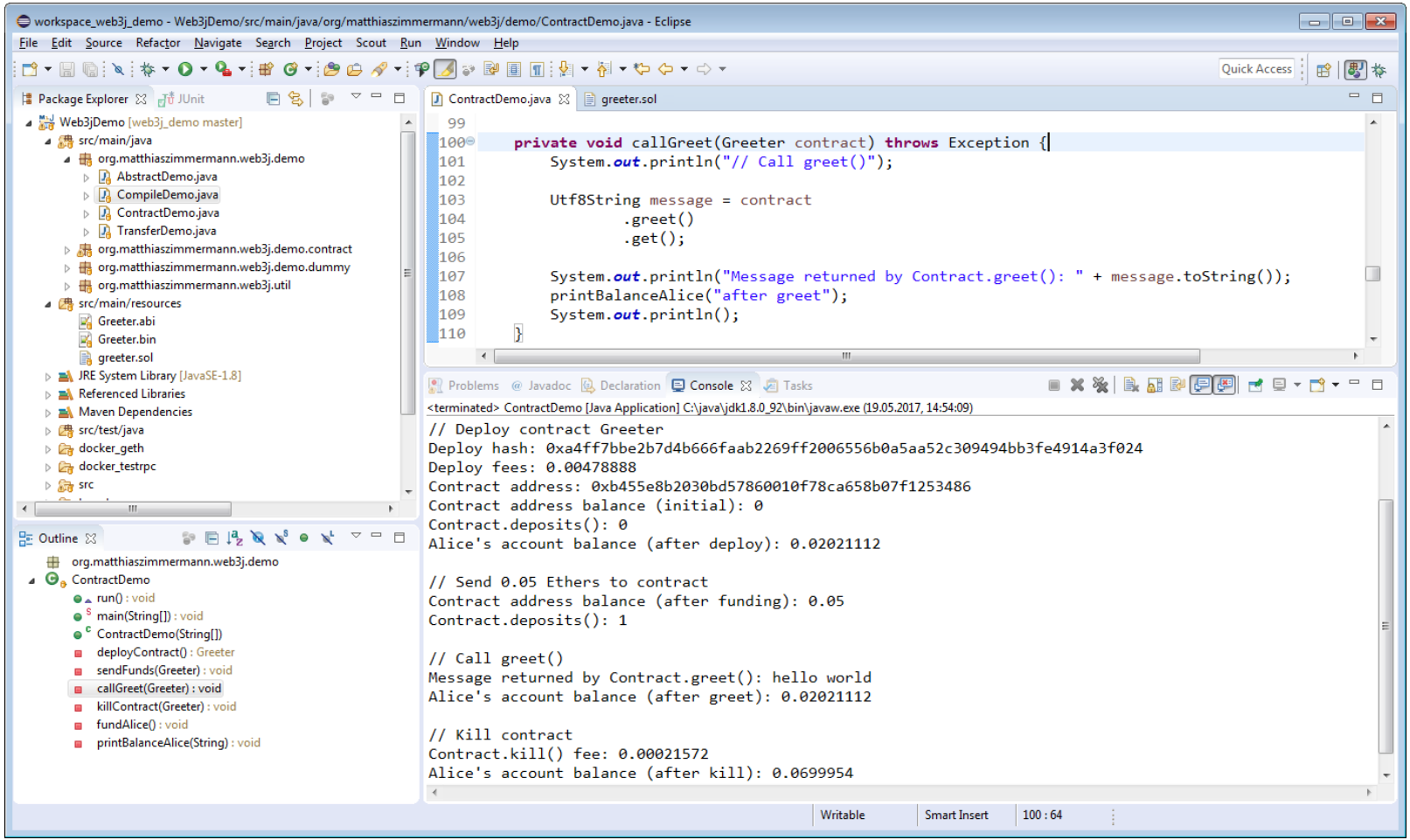


«Greeter» with web3j


web3j - Lightweight Ethe
Secure
https://web3j.io
WEB3J.IO
FEATURES
OVERVIEW
PROJECTS
COMMUNITY
CONNECT JAVA AND ANDROID APPS TO THE ETHEREUM BLOCKCHAIN
web3j is a lightweight, reactive, type safe Java and Android library for integrating with nodes on Ethereum blockchains
WEB3J ON GITHUB
DOCUMENTATION

greeter.sol → Greeter.java

1. Compile `greeter.sol`
   - → `greeter.bin`
   - → `greeter.abi`
2. Create wrapper class (use Web3j command line tool)
   - → `Greeter.java`



https://github.com/matthiaszimmermann/web3j_demo

Trading-Network Demo

Ethereum, web3j, Eclipse Scout

Trading Network Demo

Use Case

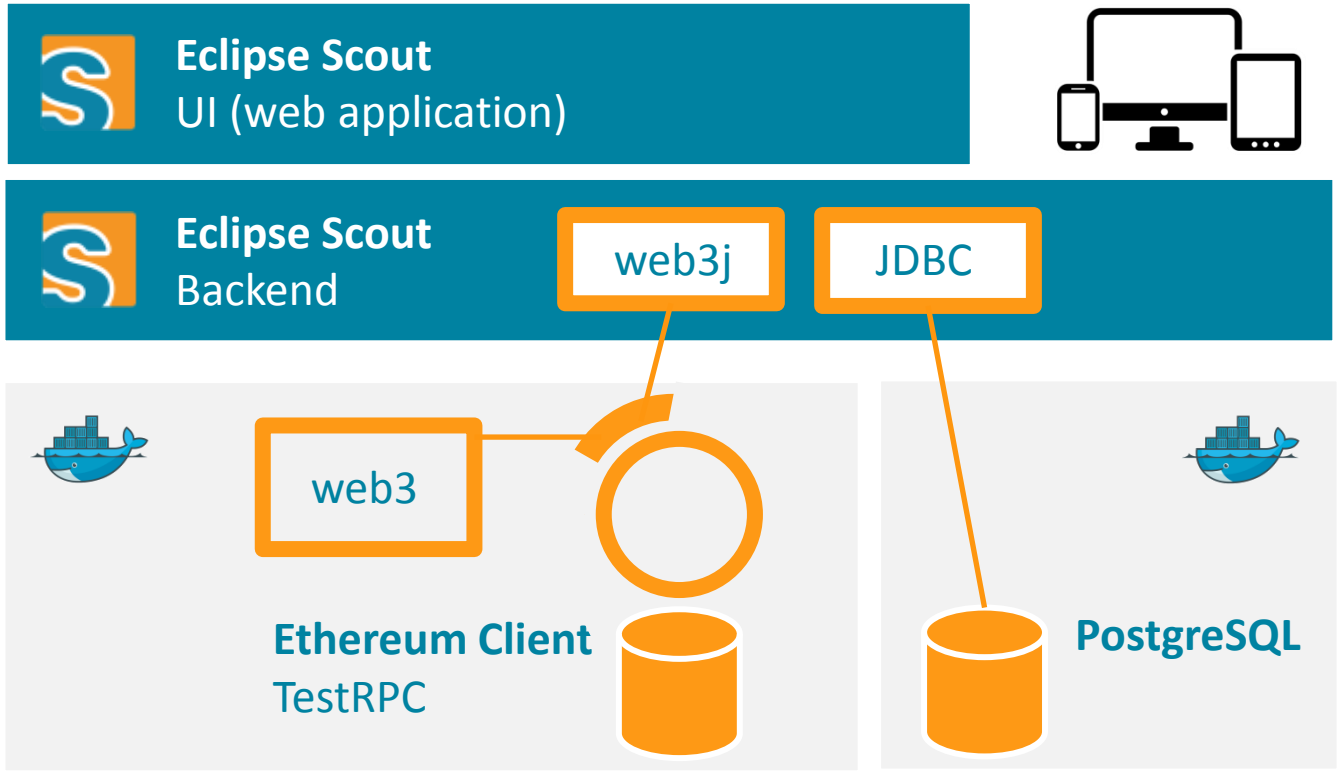
➔ **Currency Hedging**: Manage buy and sell orders for € / US$

➔ **Classical Business App**

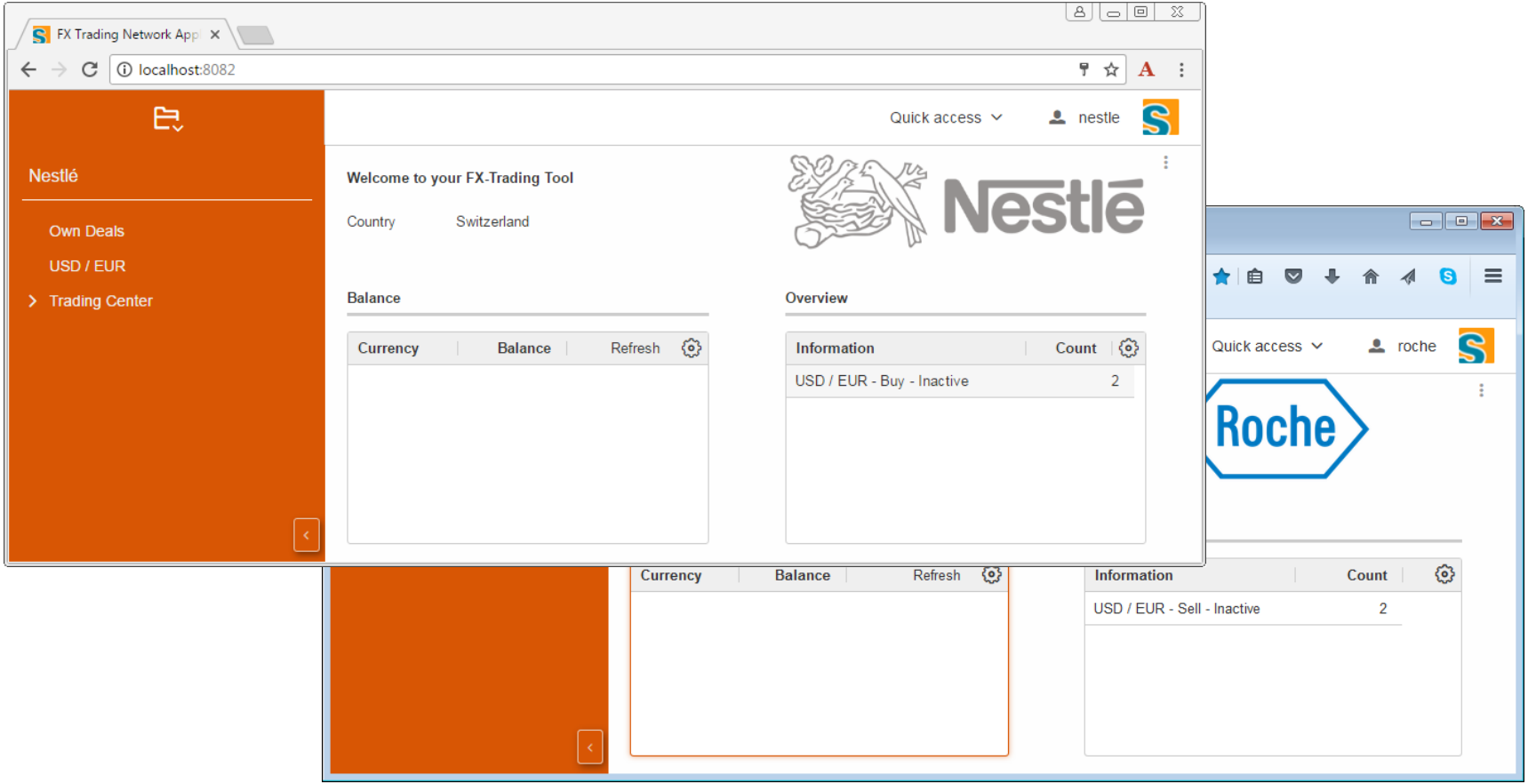
- **Idendity management:** Map users with Ethereum addresses
- **web3j** library to access Ethereum client
- **Eclipse Scout** to build application

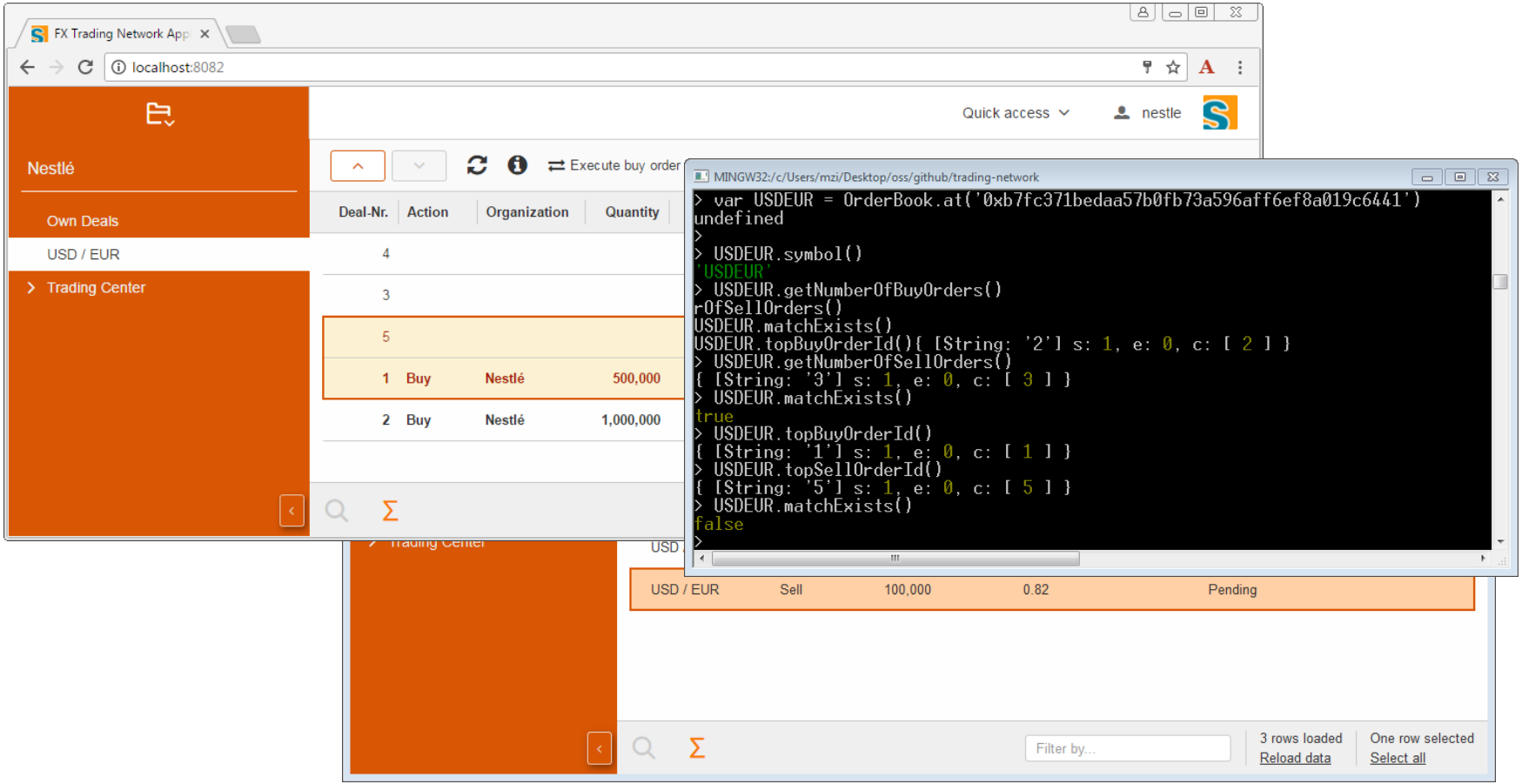
➔ **Blockchain Benefits**

- **Efficiency**: No central organization/infrastructure
- **Trust**: Tampering-proof ledger, trust by blockchain

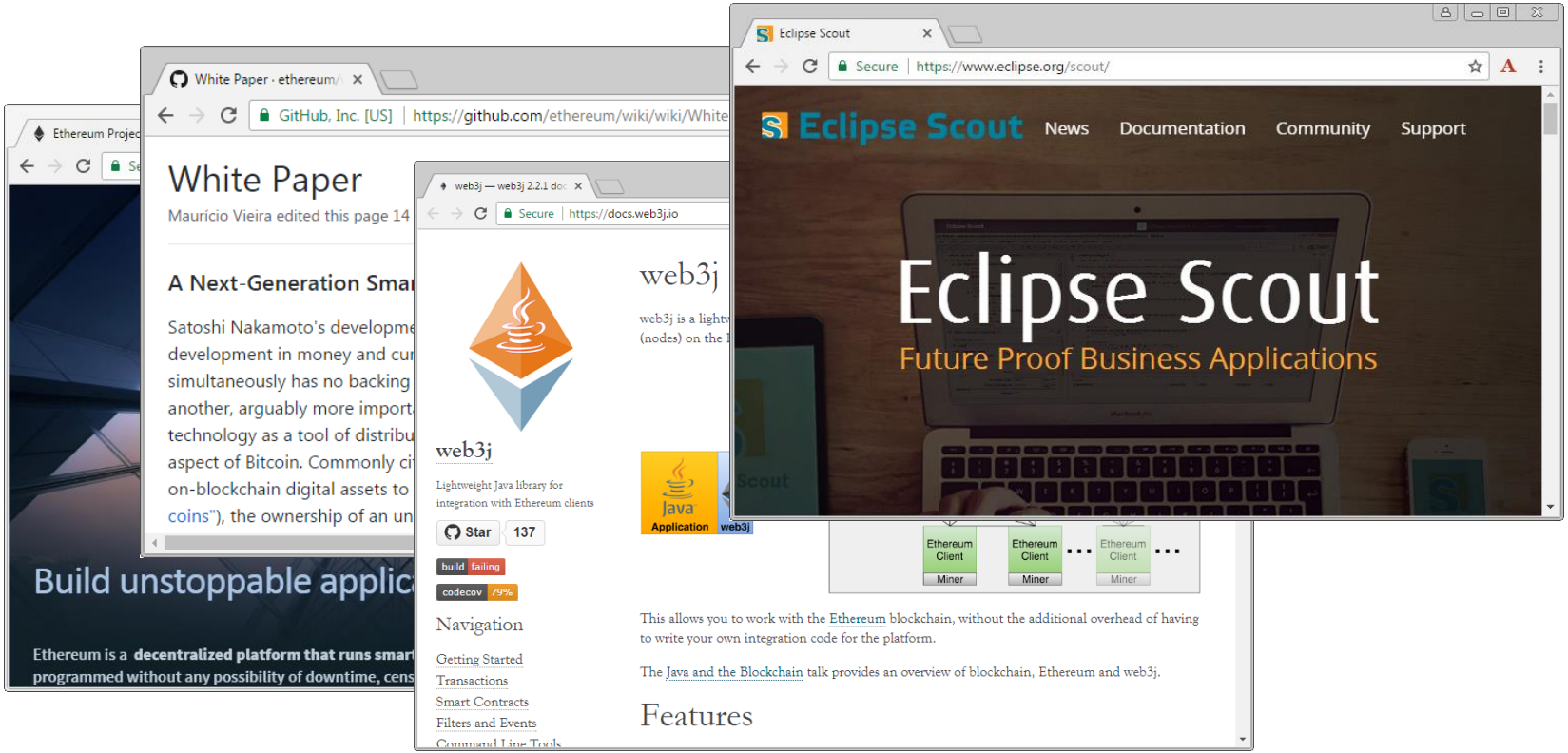


https://github.com/BSI-Business-Systems-Integration-AG/trading-network/tree/features/matthiaszimmermann/jugch_talk_2017


FX Trading Network App
localhost:8082
Quick access
nestle
Nestlé
Own Deals
USD / EUR
Trading Center
Welcome to your FX-Trading Tool
Country
Switzerland
Nestlé
Balance
Currency
Balance
Refresh
Overview
Information
Count
USD / EUR - Buy - Inactive
2
Quick access
roche
Roche
Currency
Balance
Refresh
Information
Count
USD / EUR - Sell - Inactive
2


FX Trading Network App
localhost:8082
Quick access
nestle
Nestlé
Own Deals
USD / EUR
Trading Center
Execute buy order
Deal-Nr.
Action
Organization
Quantity
4
3
5
1 Buy Nestlé 500,000
2 Buy Nestlé 1,000,000
MINGW32:/c/Users/mzi/Desktop/oss/github/trading-network
> var USDEUR = OrderBook.at('0xb7fc371bedaa57b0fb73a596aff6ef8a019c6441')
undefined
> USDEUR.symbol()
'USDEUR'
> USDEUR.getNumberOfBuyOrders()
rOfSellOrders()
USDEUR.matchExists()
USDEUR.topBuyOrderId(){ [String: '2'] s: 1, e: 0, c: [2] }
> USDEUR.getNumberOfSellOrders()
{ [String: '3'] s: 1, e: 0, c: [3] }
> USDEUR.matchExists()
true
> USDEUR.topBuyOrderId()
{ [String: '1'] s: 1, e: 0, c: [1] }
> USDEUR.topSellOrderId()
{ [String: '5'] s: 1, e: 0, c: [5] }
> USDEUR.matchExists()
false
>
USD / EUR Sell 100,000 0.82 Pending
Filter by...
3 rows loaded
Reload data
One row selected
Select all

Resources



https://www.ethereum.org/ https://github.com/ethereum/ https://docs.web3j.io/ https://www.eclipse.org/scout/

Summary

Wrap-up

Blockchain

- Internet of decentralized trust
- Cool new technology

Technology is great for

- «unbanked»: Machines AND people
- Efficient trustless global exchange for values (and information)
- Distributed business models

Challenges

- Privacy
- Scalability (Bitcoin can do 7 tx/s)
- Energy consuption (Bitcoin power consumption ~ Ecuador)
- Maturity (blockchain still in it's infancy)
- Regulatory (it's a mess …)

Thanks!

«Blockchain, Ethereum and Business Applications»

Additional Material

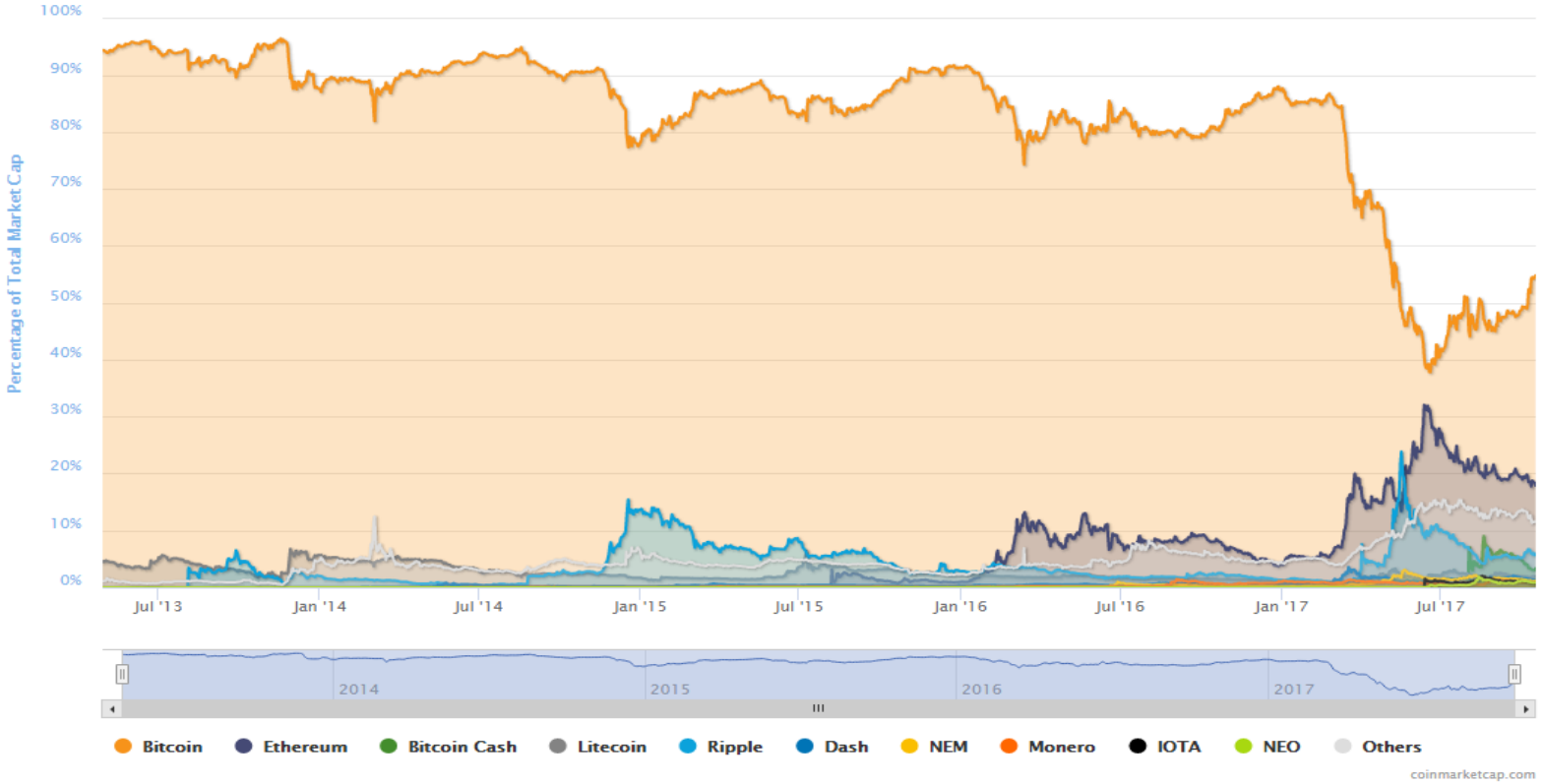
Bitcoin · $5,554.90 Ethereum · $298.16 Litecoin · $55.19

1H 1D 1W 1M 1Y ALL

$5,554.90

BITCOIN PRICE

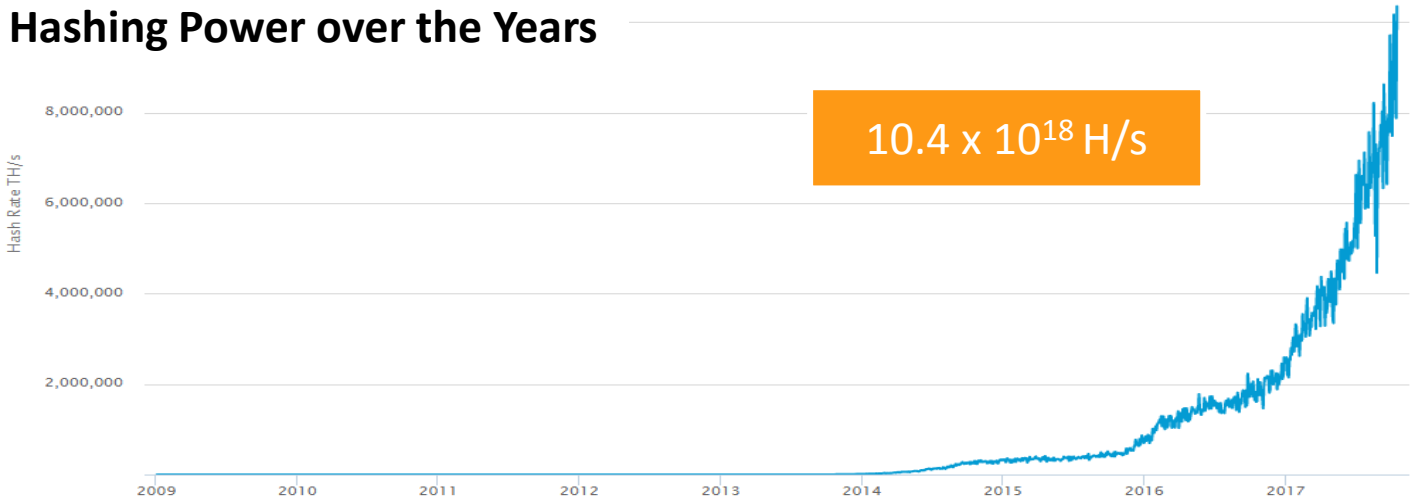
Bitcoin Market Share



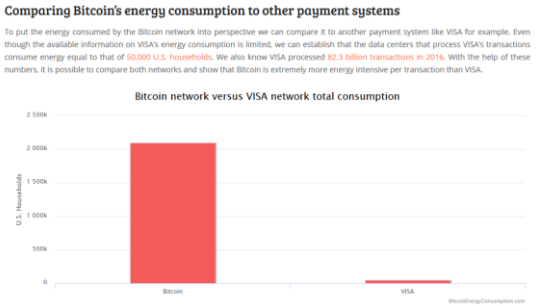
Bitcoin Mining Today

- **Mining-pools**: Include many ASIC computers (PC way too slow)
- **AntMiner**: 10,000x faster than PC, burns 10x more electricity
- **Energy Costs**: # of hashes per KWh is central criteria + cooling(!)

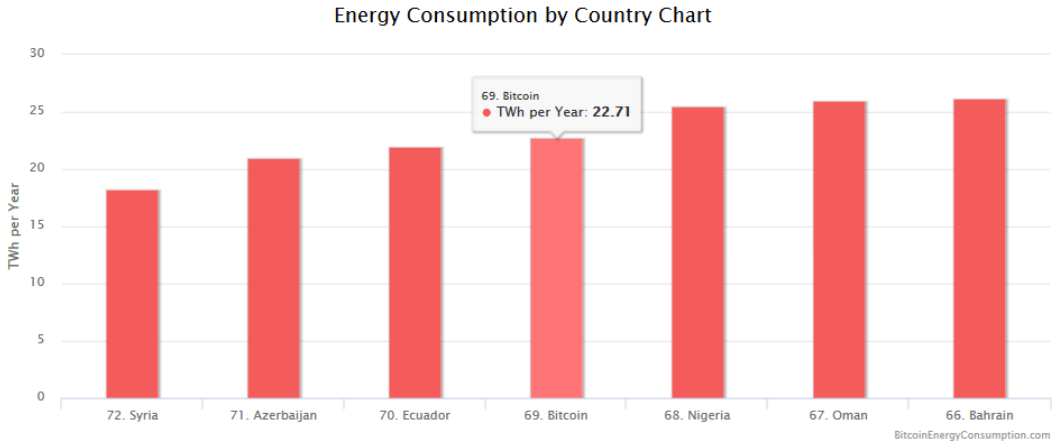
Hashing Power over the Years



Bitcoin Energy Consumption Index

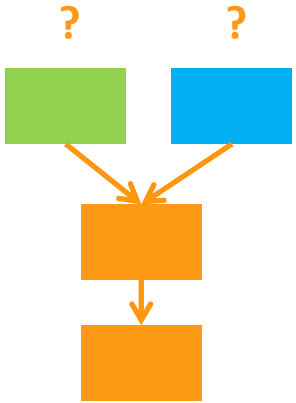


Bitcoin vs VISA



Bitcoin compared to countries

Consensus Mechanism
«Preventing Forks»



The Challenge

- ➔ Mining clients build block candidates independently
- ➔ **Several new blocks** might be found **at the «same» time**
- ➔ Clients may receive new blocks that are inconsistent
- ➔ The local copy of the blockchain may have forks

The Solution

- ➔ The «true» blockchain is defined by the **highest cumulative PoW** (difficulty)
- ➔ By selecting the greatest-difficulty chain, **eventual consensus** is achieved
- ➔ Miner **majority vote** defines the true chain
- ➔ Miners «vote» for the true chain by deciding which block/fork to extend

Financial Industry getting ne