Blockchain, Ethereum and Business Applications

@ZimMatthias  Matthias Zimmermann
BSI Business Systems Integration AG
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»
## Blockchain Market

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
<th>Volume (24h)</th>
<th>Circulating Supply</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$96,108,095,012</td>
<td>$5779.73</td>
<td>$1,920,760,000</td>
<td>16,628,475 BTC</td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>$31,326,302,991</td>
<td>$329.24</td>
<td>$92,471,000</td>
<td>95,147,607 ETH</td>
</tr>
<tr>
<td>3</td>
<td>Ripple</td>
<td>$9,936,069,410</td>
<td>$0.257869</td>
<td>$366,836,000</td>
<td>92,531,538,922 XRP *</td>
</tr>
<tr>
<td>4</td>
<td>Bitcoin Cash</td>
<td>$5,864,609,962</td>
<td>$351.12</td>
<td>$346,000,000</td>
<td>16,702,436 BCH</td>
</tr>
<tr>
<td>5</td>
<td>Litecoin</td>
<td>$3,358,412,504</td>
<td>$62.88</td>
<td>$188,348,000</td>
<td>53,412,558 LTC</td>
</tr>
<tr>
<td>6</td>
<td>Dash</td>
<td>$2,307,274,645</td>
<td>$302.54</td>
<td>$38,470,400</td>
<td>7,620,321 DASH</td>
</tr>
<tr>
<td>7</td>
<td>NEM</td>
<td>$2,025,387,000</td>
<td>$0.225043</td>
<td>$8,065,810</td>
<td>8,999,999,999 XEM *</td>
</tr>
<tr>
<td>8</td>
<td>Monero</td>
<td>$1,451,708,799</td>
<td>$95.32</td>
<td>$31,838,500</td>
<td>15,229,142 XMR</td>
</tr>
</tbody>
</table>

### List by the *International Monetary Fund* (Partial forecasted estimates for 2017)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>GDP (millions of int$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>China</td>
<td>126,687,917</td>
</tr>
<tr>
<td>2</td>
<td>United States</td>
<td>19,417,144</td>
</tr>
<tr>
<td>3</td>
<td>World</td>
<td>23,194,411</td>
</tr>
<tr>
<td>4</td>
<td>European Union</td>
<td>20,852,702</td>
</tr>
<tr>
<td>5</td>
<td>Croatia</td>
<td>100,006</td>
</tr>
<tr>
<td>6</td>
<td>Côte d’Ivoire</td>
<td>95,887</td>
</tr>
<tr>
<td>7</td>
<td>Macedonia</td>
<td>31,924</td>
</tr>
<tr>
<td>8</td>
<td>Cyprus</td>
<td>31,093</td>
</tr>
</tbody>
</table>
Neil Woodfine 聂尔 @nwoodfine · 9 Std.
Understanding bitcoin VS. when to buy and when to sell
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

Peer-to-Peer Network
Distribution of unconfirmed TX

<table>
<thead>
<tr>
<th>Hash</th>
<th>Amount</th>
<th>Confirmations</th>
</tr>
</thead>
<tbody>
<tr>
<td>eb78fd5e6f397eb6b7d9d4d54f5b3d9df0a25f5ed417eaa4a75df</td>
<td>0.05965 BTC</td>
<td>0.1515 BTC</td>
</tr>
<tr>
<td>1NyyltqF0xyp0Luw4tcPANE9ja93h6v8u</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3QKc579cJLb4xO09etUjyKYne4wZvYzK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>184705ab578e28e23d2744d77eb3411d225b3259e1e1d567c21a5242c</td>
<td>2.53205 BTC</td>
<td></td>
</tr>
<tr>
<td>195kWQSMUWRAJ7mvGN65QHeegC39qd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1DEytcP65Wdmz9lw4wZyucYycZMySp7Xj</td>
<td></td>
<td>2 BTC</td>
</tr>
<tr>
<td>1K1ATEVPf9dRTfuMaMSzynT4gntD4T8DA9</td>
<td></td>
<td>0.53554 BTC</td>
</tr>
<tr>
<td>657738810e39824c6367b23ac544ab1249257a344d8d5d885300ed228942eb</td>
<td>0.05987 BTC</td>
<td></td>
</tr>
<tr>
<td>14JksBE833RbE8E9iqFpJ84LHEZ22Neu3U8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>169W8GEPzPtdT9p2MaYRW8px4TEKgND</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 ...

[Image of Blockchain transaction with labels: Bob's Address, Coffee Price, My Address, Link to TX Block, TX Fee]
TX Blocks and the Blockchain

- **Block #277316** includes coffee TX

  - Link to previous Block
  - Block Hash
  - do you see the leading zeros?

  **419 TX (€495,000)**

  Screenshot: blockchain.info

Genesis Block

- #1
- #2
- #277315
- #277316
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
4. Winning client sends the new block to its peers
5. 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 -> E6F1EB09A9EF0BF331261B64E1C798EAB
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 -> 0000AD30B2DDDB8A773B85AABB5282AD
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

Introduction

What Is Bitcoin?

Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem. Units of currency called bitcoins are issued and transferred through a network of participating nodes using an open-source protocol. The bitcoin protocol is similar to those underlying electronic banking systems, but it is decentralized, has no central bank, and runs entirely on a network of computers. A bitcoin node communicates with other nodes using JSON-RPC requests. The bitcoin protocol is open-source software, allowing anyone to inspect its source code. The source code is distributed over the internet, so anyone can run a bitcoin node on their computer.
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)
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

«Truly» Autonomous Cars

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

Tempe or bust
by Andrew J. Hawkins | @andyjhayward | Feb 21, 2017, 1:13 pm EST

Smart contract: Order car to transport people (fees go to car contract)
Smart contract: Car pays for energy/services (car pays with its own funds)

In 2017 RWE introduces charging stations connected to Ethereum blockchain

«Greeter» with web3
Smart Contract Hello World
Ethereum and Applications

Ethereum Client
Geth/TestRPC/…

JavaScript
web3

Java
web3j

Interface
JSON-RPC

http://localhost:8545

Ethereum Peer-to-Peer Network
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.
  * 'constant': 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() {
    ... }
}
Solidity Compiler (online)

byte code (EVM) to deploy contract

Deploy script (JS)
Deploy (Console)

Deploy

Contract address

Successs 😊
«Greeter» with web3j
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
greeter.sol ➔ Greeter.java

1. Compile greeter.sol
   ➔ greeter.bin
   ➔ greeter.abi

2. Create wrapper class (use Web3j command line tool)
   ➔ Greeter.java
private void callGreet(Greeter contract) throws Exception {
    System.out.println("// Call greet()");
    Utf8String message = contract
        .get();
    System.out.println("Message returned by Contract.greet(): " + message.toString());
    printBalanceAlice("after greet");
    System.out.println();
}

// Deploy contract Greeter
Deploy hash: 0xda4ff7b2b7d4b66f6aab2269ff2e086556b0a5a52c309494bb3fa4914a3f024
Deploy fees: 0.0047888
Contract address: 0xb455e8b2b03bd57860018f77ca658b7f1253486
Contract address balance (initial): 0
Contract.deposits(): 0
Alice’s account balance (after deploy): 0.02021112

// Send 0.05 Eths to contract
Contract address balance (after funding): 0.05
Contract.deposits(): 1

// Call greet()
Message returned by Contract.greet(): hello world
Alice’s account balance (after greet): 0.02021112

// Kill contract
Contract.kill() fee: 0.00021572
Alice’s account balance (after kill): 0.0699954

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**
  - **Identity 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
Welcome to your FX Trading Tool
Country: Switzerland

## Balance

<table>
<thead>
<tr>
<th>Currency</th>
<th>Balance</th>
<th>Refresh</th>
</tr>
</thead>
</table>

## Overview

<table>
<thead>
<tr>
<th>Information</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>USD / EUR - Buy - Inactive</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>USD / EUR - Sell - Inactive</td>
<td>2</td>
</tr>
</tbody>
</table>
```javascript
var USDEUR = OrderBook.at('0x8c679a376c9e2e3c7f8e68f941e64e19c6441')
undefined
> USDEUR.symbol()
undefined
> USDEUR.getNumberofBuyOrders()
0
> USDEUR.getNumberofSellOrders()
0
> USDEUR.matchExists()
true
> USDEUR.topBuyOrder Tổng()
[ { String: '5' } ]
> USDEUR.topSellOrder Tổng()
[ { String: '5' } ]
> USDEUR.importExists()
false
```
Resources

Summary
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 consumption (Bitcoin power consumption ~ Ecuador)
- Maturity (blockchain still in it’s infancy)
- Regulatory (it’s a mess ...)

Wrap-up
Thanks!

«Blockchain, Ethereum and Business Applications»

Evaluate the Sessions
Sign in and vote at eclipsecon.org

-1 0 +1
Additional Material
$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

- 10.4 x 10^{18} H/s
Bitcoin Energy Consumption Index

Comparing Bitcoin's energy consumption to other payment systems

To put the energy consumed by the Bitcoin network into perspective, we can compare it to another payment system like Visa, for example. Even though the available information on Visa's energy consumption is limited, we can establish that the data centers that process Visa transactions consume energy equal to that of 1.5% of U.S. households. We also know Visa processed 83 billion transactions in 2016. With the help of these numbers, it is possible to compare both networks and show that Bitcoin is extremely more energy intensive per transaction than Visa.

Energy Consumption by Country Chart

Bitcoin compared to countries


Bitcoin TWh per Year: 22.71
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 nervous…

Captains of Finance Dismiss Bitcoin at Their Peril and the pace of gains has accelerated in the past few weeks, reaching $6,000 on Friday. That’s sparked a new round of criticism from financial luminaries. Jamie Dimon, CEO of JP Morgan Chase, called Bitcoin a “fraud” and said that he would fire anyone who traded it for being “stupid.” After some pointed out that Chase is actively pursuing blockchain solutions and digital payments akin to Bitcoin, Dimon said he was only talking about it, only to repeat his critique a few days later. Larry Fink, CEO of Blackrock, called Bitcoin “an index of money laundering.” Global investment bank UBS just issued a lengthy report...