Blockchain Technology

Beyond the Hype

BlockchainHub Graz & lab10 collective ■ Thomas Zeinzinger & Didi Hofer ■ April 29th, 2017

Blockchain technology is currently one of the most hyped topics and you will find scams just as well as real business value propositions.
Knowing what can be done and what is not feasible is likely determining the success of any business proposal.
We also believe that we have a chance to use it for a re-decentralization of the web as proposed by Tim Burners-Lee. Privacy is another highly underrepresented value caused by monopolies and various surveillance tactics by governments and private companies.

Overview | Under the Hood | Examples | Outlook


LEHMAN BROTHERS
THE TIMES
Eat Out from £5
Chancellor on brink of second bailout for banks

… a little bit of history

1997: Adam Back proposed “hashcash“ incorporating proof-of-work to limit e-mail spam and denial-of-service attacks.

1998: Wei Dai created “b-money“, Nick Szabo created “Bit Gold“ and Hal Finney developed “RPOW”. All these cryptocurrencies used hashcash as their proof-of-work algorithm.

2004: BitTorrent emerged – it is the most used Peer-2-Peer file sharing communication protocol with approx. 250 million users per month.

2008: Bitcoin was introduced by Satoshi Nakamoto (identity unknown) with a paper called “*bitcoin: A Peer-to-Peer Electronic Cash System”.*

2009: The first open source bitcoin client went live and mining of bitcoins started. By definition there are only 21 million Bitcoin (BTC) possible.

2013: Ethereum was first described by Vitalik Buterin: *“Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform”*

Blockchain Demo

Blockchain 101 - A Visual Demo

Hash | Block | Blockchain | Distributed | Tokens | Coinba

Blockchain

3

37

012fa9b916eb9078f8d98a7864e697ae83

0b9015ce2a08b61216ba5a0778545bf4d

Block: # 4

Nonce: 35990

Data:

Prev: 0000b9015ce2a08b61216ba5a0778545bf4d

Hash: 0000ae8bbc96cf89c68be6e10a865cc47c6c4

Mine

Block: # 5

Nonce: 56265

Data:

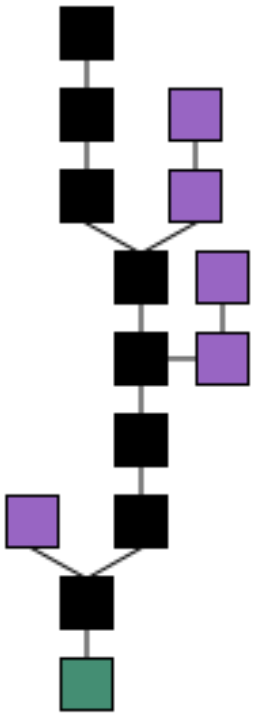
Prev: 0000ae8bbc96cf89c68be6e10a865cc47c6c4

Hash: 0000e4b9052fd8aae92a8afda42e2ea0f1797

Mine

Source: https://anders.com/blockchain/

The Bitcoin - Blockchain



Wikipedia, CC-BY-3.0

- Start: Jan. 3rd 2009
- Blockchain stores all transactions
- >5000 full-nodes and 22 mining pools
- Full-nodes store the 110 GB Blockchain
- No central governance (just like TCP/IP or Linux)
- Miners compete over the mining reward (PoW)
- 12.5 BTC are generated every 10 minutes
- Block reward halving every 210.000 blocks (~4 years)
- Difficulty adjustment every 2016 blocks
- 21 Million BTC will be generated
- The longest Blockchain is the truth

Top 10 – Alt-Coins

Ranking in line with market capitalisation

Based on free trading

All ▾ Currencies ▾ Assets ▾ EUR ▾ Next 100 → View All

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	€19 373 230 955	€1188.78	16,296,687 BTC	€357 645 403	1.54%	
2	Ethereum	€4 849 895 678	€53.24	91,095,988 ETH	€161 265 800	12.08%	
3	Ripple	€1 128 396 183	€0.029785	37,884,925,434 XRP *	€11 981 439	-1.30%	
4	Litecoin	€678 899 233	€13.35	50,835,707 LTC	€68 230 606	-5.84%	
5	Dash	€484 030 994	€66.71	7,255,850 DASH	€10 172 018	1.25%	
6	NEM	€426 463 793	€0.047385	8,999,999,999 XEM *	€22 451 891	16.35%	
7	Ethereum Classic	€425 063 032	€4.67	91,077,393 ETC	€73 041 168	28.13%	
8	Monero	€259 436 970	€18.06	14,364,565 XMR	€7 048 089	1.09%	
9	Augur	€134 341 701	€12.21	11,000,000 REP *	€2 573 844	-0.97%	
10	MaidSafeCoin	€99 219 400	€0.219244	452,552,412 MAID *	€1 074 007	1.16%	

April 29, 2017

Source: http://coinmarketcap.com/currencies/

Bitcoin

“Depending on your point of view, you could see some problems with Bitcoin.”

- **Block Time**
  high variation, 10 min. average
- **Finality**
  very long lead time, 6 blocks
- **Consensus - PoW**
  security vs. waste of energy
- **Governance**
  long consensus time, e.g. Segwit vs. BU
- **Extensibility**
  very tough, scripting language
- **Scalability**
  limited by protocol, ~ 280 kTx per day

Bitcoin – Ethereum Comparison

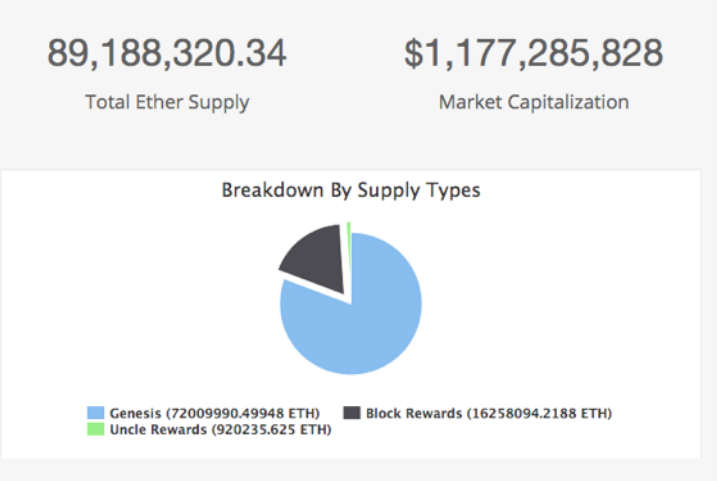
Block Time	High variation, average 10 min.	High variation, average 15 sec.
Finality	6 block confirmations, ≈ 60 min.	12 (25) block confirmations, ≈ 3 (6) min.
Consensus	PoW, energy waste for security	PoW for distribution, Plan: transition to PoS
Governance	slow decisions, conservative	actively developed, leadership
Extensibility	hard, simple scripting language	simple, smart contract + EVM
Scalability	3 Tx/s, Plan: payment channels	15 Tx/s, Plan: payment channels, sharding

Basic Differences Ethereum vs. Bitcoin Ether

Ether – Main purpose:

- Cryptocurrency to run the state machine of Ethereum
- Cryptocurrency traded on exchanges

Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000



Basic Differences Ethereum vs. Bitcoin Accounts

State Objects

Externally Owned Accounts (EAOs)
simple „Accounts“

State: Balance

Contract Accounts
simple „Contracts“

State: Balance & Storage

- has an ether balance,
- can send transactions (ether transfer or trigger contract code),
- is controlled by private keys,
- has no associated code.

- has an ether balance,
- has associated code,
- code execution is triggered by transactions or messages (calls) received from other contracts.
- when executed - perform operations of arbitrary complexity (Turing completeness) - manipulate its own persistent storage, i.e., can have its own permanent state - can call other contracts

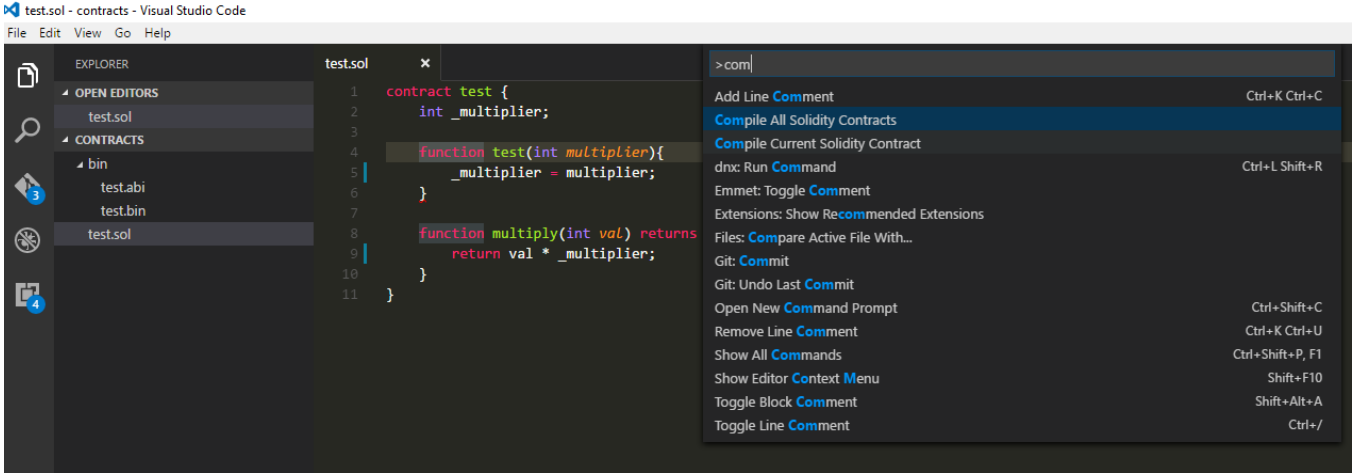
Basic Differences Ethereum vs. Bitcoin Languages for the EVM

Serpent – is a Python-like programming language. The latest version of the Serpent compiler is written in C++, allowing it to be easily included in any client.

III – is a Lisp-like low-level programming language. Serpent can be compiled to III.

Solidity – is a Java Script-like programming language and by far the most popular one. It was also used for „The DAO“.

Mutan (Discontinued) – is a C-Like language and it supports a full, statically typed higher level language.



Basic Differences Ethereum vs. Bitcoin GAS

Transactions

- Signed Message from EOA (Externaly Owned Accounts)
- Signature Sender / Address Recipient / Ether transferred
- STARTGAS - is the amount of ”GAS" that the transaction assigns itself
- GASPRICE - is the fee that the transaction pays per unit of gas

Messages

- Inter-contract communication
- Messages are triggered by Transactions (defines GASPRICE)
- STARTGAS applies for the transaction and all subsequent computations

Attention: Insufficient STARTGAS → pay miner / no state change

Basic Differences Ethereum vs. Bitcoin

- “GAS“ limit defines transactions per second
- Adjustment of “GAS“ limit with every block
- Also used to counteract DDoS attacks

Bitcoin

```
1024 * 1024 / 600 B = 1747.7 transactions per block,
```

which translates down to

```
1747.7 / 600 s = 2.9127 transactions per second.
```

Ethereum

```
4712388 / 21000 = 224.4 transactions per block
```

which translates down to

```
224.4 / 15 = 14.96 transactions per second.
```

GAS limit can increse by 1+1/1024 with every block and in the early olympic testnet it reached around 25tx/s.

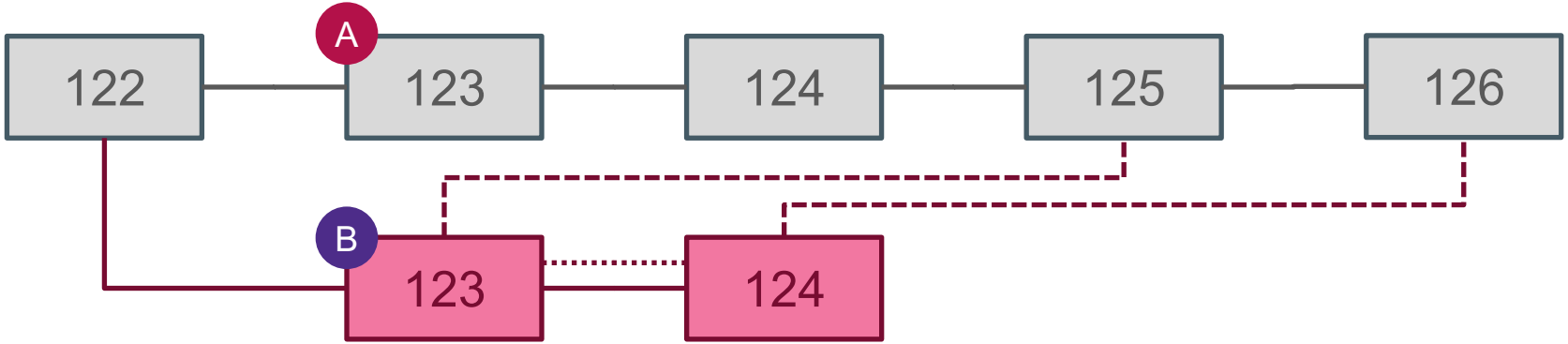
Live View: https://ethstats.net/

Source: http://ethereum.stackexchange.com/questions/3308/how-do-i-compare-the-scalability-capabilities-between-ethereum-and-bitcoin

Basic Differences Ethereum vs. Bitcoin Consensus: GHOST Protocol

The modified GHOST (Greedy Heaviest-Observed Sub-Tree) of Ethereum tackles two problems by including stale blocks:

- Network Propagation Time
- Miner Centralization



Source: https://genius.com/Ethereum-ethereum-whitepaper-annotated
GHOST Protocol: http://www.cs.huji.ac.il/~avivz/pubs/13/btc_scalability_full.pdf

Basic Differences Ethereum vs. Bitcoin Mining

Ethash (Dagger – Hashimoto)

- ASIC-resistance
- Light client verifiability

Mining Block Reward

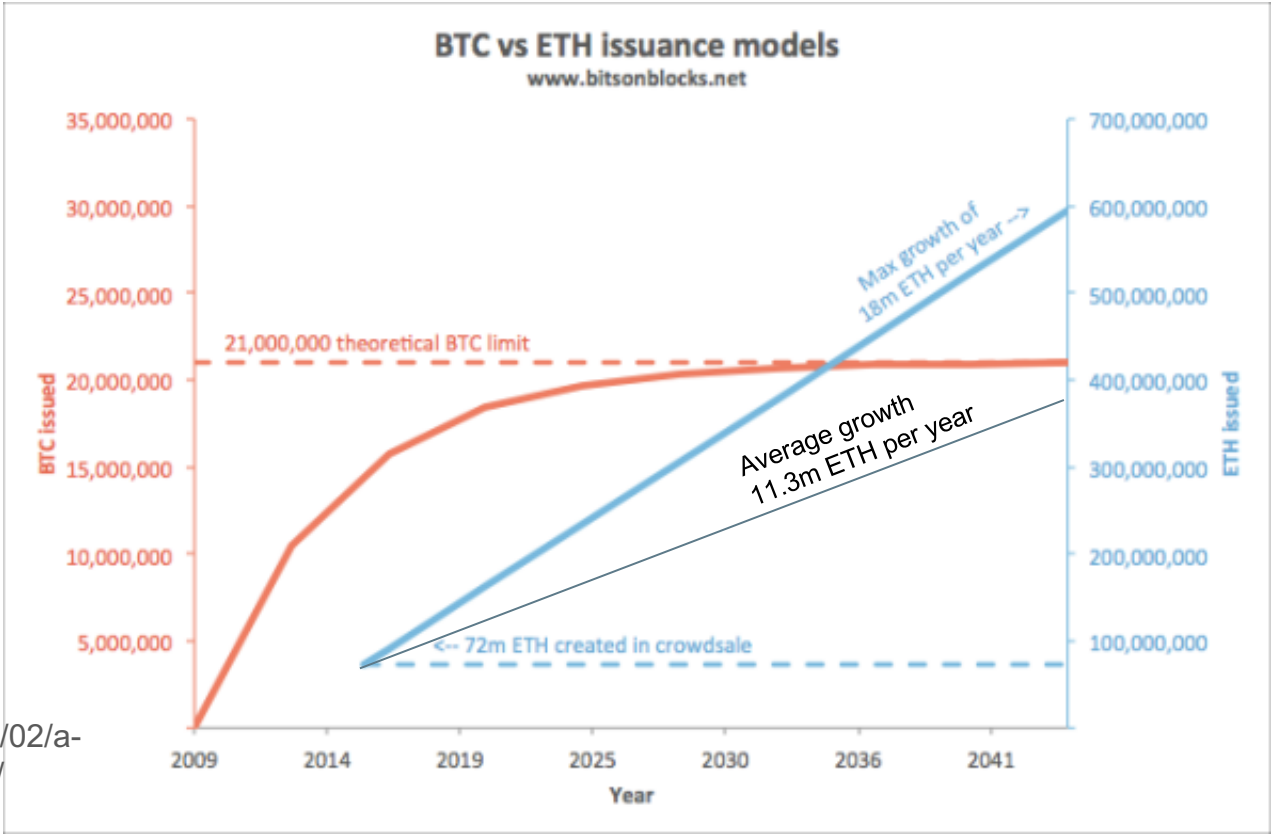
- 5 ETH/Block
- 1/32 of Block Reward for every Uncle Block (max. 2)
- All ETH for transactions and EVM computation

Uncle Block Reward

- 7/8 of Block Reward → 4.375 ETH/Block

Source: https://github.com/ethereum/wiki/blob/master/Dagger-Hashimoto.md

Basic Differences Ethereum vs. Bitcoin Inflation



Source: https://bitsonblocks.net/2016/10/02/a-gentle-introduction-to-ethereum/

Bitcoin – Ethereum Comparison

Block Time	High variation, average 10 min.	High variation, average 15 sec.
Finality	6 block confirmations, ≈ 60 min.	12 (25) block confirmations, ≈ 3 (6) min.
Consensus	PoW, energy waste for security	PoW for distribution, Plan: transition to PoS
Governance	slow decisions, conservative	actively developed, leadership
Extensibility	hard, simple scripting language	simple, smart contract + EVM
Scalability	3 Tx/s, Plan: payment channels	15 Tx/s, Plan: payment channels, sharding

Extensability: Example – ERC 20 Token

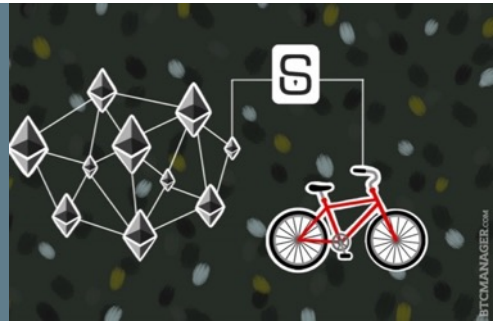
Can represent any asset, e.g.
local currency, voucher, 1 hour worth of baby sitting, promise for a crowd funded product, insurance policy, event ticket, …

Token standard ERC-20

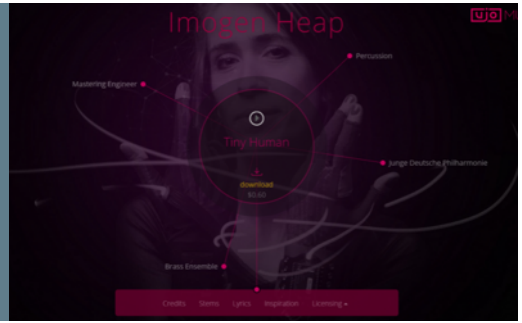
Smart contract can implement features like:
multi-party issuance control, asset freezing rules, dependency on events in the real world, ...

Use Cases – Ethereum Smart Contracts

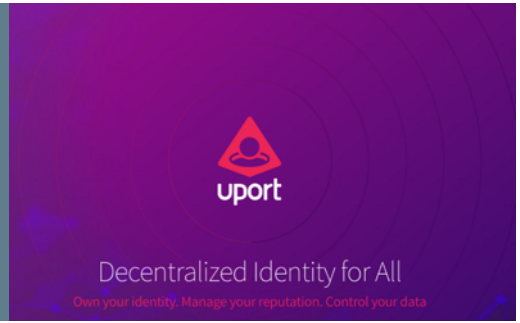
LOCKS



MUSIC



IDENTITY

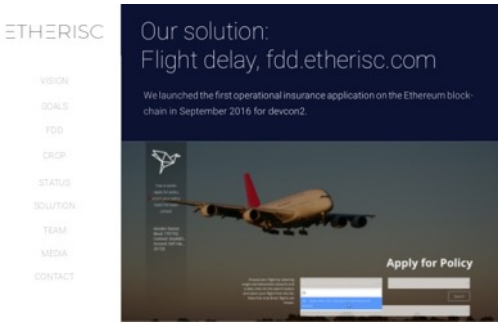


ASSETS

MICROGRID

LO3 ENERGY

INSURANCE



Use Cases – Ethereum Smart Contracts

SMITH + CROWN

HOME ICOS MARKETS RESEARCH ABOUT

Humaniq (HMQ)	Profile	A blockchain fintech service that aims to expand financial inclusion with bio-identification and mobile technology. Note: The totals listed here do not include roughly $300,000 in fiat currency raised during a brief pre-sale.		Apr 6, 2017	Apr 27, 2017	$4,698,251
TaaS (TAAS)	Profile	TaaS is a tokenized closed-end fund dedicated to blockchain markets.		Mar 27, 2017	Apr 27, 2017	$6,950,405
Gnosis (GNO)	Profile	An accessible prediction market platform enabling the free flow of useful information.		Apr 24, 2017	Apr 24, 2017	$12,250,000
Embermine (EMB)	Summary	Embermine is a platform designed to give content creators the means to protect and control their creative endeavors. Update: The sale was canceled because of a security issue.		Apr 13, 2017	Apr 20, 2017	Refunded

BlockchainHub

Blockchain Basics | Blockchain in Depth | Local Hubs

lab10 Collective


Thomas


Didi


Sandra


Mario

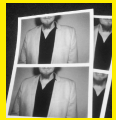

Tom


Bernhard


David


Markus


Verena


Matthias

Robert


Hagen


Andreas

Projects

IT Education

Shared Economy

Timeline

Phase 1	Phase 2	Phase 3
• Define Projects & Teams • Found lab10 collective • Involve Investors	• ICO's for lab10 token and platform token • New projects and teams • Spin-off companies	• Scale lab10 concept • Foster shared economy • Build own IT education

You want to become part of the core founding team?

Get in touch

Thomas | thomas@lab10.io | @leantom42

Questions?

blockchainhub.net/graz

blockchainhubgraz

@bchgraz

Thomas Zeinzinger

@leantom42

thomas zeinzinger