OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

DS1 part 2

Thomas Bocek

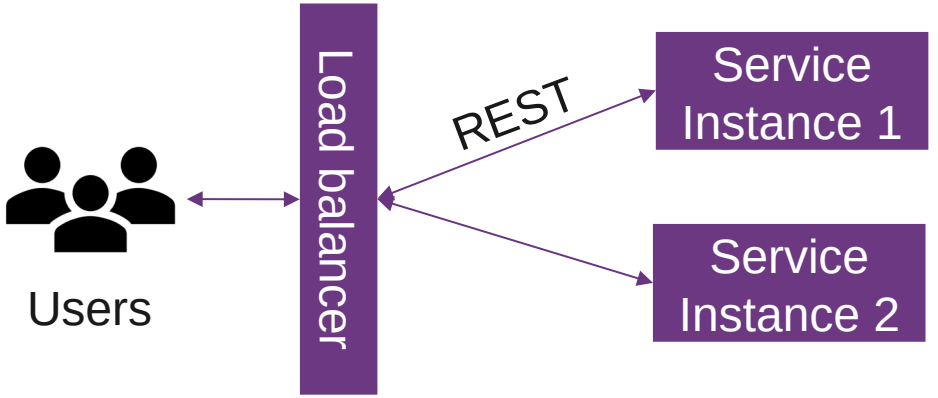
30.09.2021

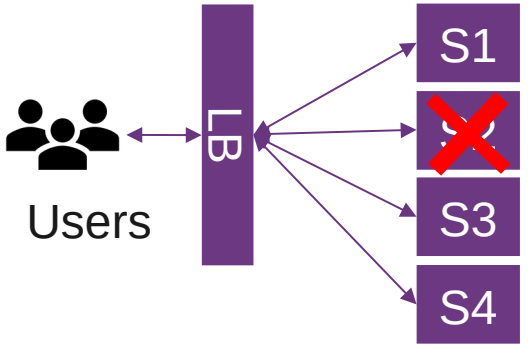
Lecture 4

Load balancing

- What is load balancing
  - Distribution of workloads across multiple computing resources
    - Workloads (requests)
    - Computing resources (machines)
  - Distributes client requests or network load efficiently across multiple servers
    - E.g., service get popular, high load on service

    → horizontal scaling
- Why load balancing
  - Ensures high availability and reliability by sending requests only to servers that are online
  - Provides the flexibility to add or subtract servers as demand dictates





Software-based load balancing

- Layer 7: HTTP(S), layer 7: DNS
- DNS Load balancing
  - Round-robin DNS, very easy to setup, static, caching with no fast changes
  - Split horizon DNS - different DNS information, depending on source of the DNS request
    - Your ISP, you if you do recursive DNS
    - But 1.1.1.1, 4.4.4.4, 8.8.8.8
  - Anycast (you need an AS for that, difficult and time consuming) – return the IP with lowest latency, e.g., anycast as a service, Global Accelerator
- Reduced Downtime, Scalable, Redundancy
  - Client can decide what to do
  - Negative caching impact!
  - Used in bitcoin: dig dnsseed.emzy.de

```
$TTL 3D
$ORIGIN tomp2p.net.
@ SOA ns.nope.ch. root.nope.ch. (2018030404 8H
2H 4W 3H)
                NS              ns.nope.ch.
                NS              ns.jos.li.
                MX      10      mail.nope.ch.
                A               188.40.119.115
                TXT             "v=spf1 mx -
all“
www             A               188.40.119.115
bootstrap       A               188.40.119.115
bootstrap       A               152.96.80.48
```

```
--- bootstrap.tomp2p.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.025/0.035/0.046/0.012 ms
draft@gserver:~$ ping bootstrap.tomp2p.net
PING bootstrap.tomp2p.net (188.40.119.115) 56(84) bytes of
data.
64 bytes from jos.li (188.40.119.115): icmp_seq=1 ttl=64
time=0.026 ms
--- bootstrap.tomp2p.net ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.026/0.026/0.026/0.000 ms
draft@gserver:~$ ping bootstrap.tomp2p.net
PING bootstrap.tomp2p.net (152.96.80.48) 56(84) bytes of
data.
64 bytes from dsl.hsr.ch (152.96.80.48): icmp_seq=1 ttl=53
time=23.1 ms
```

CORS

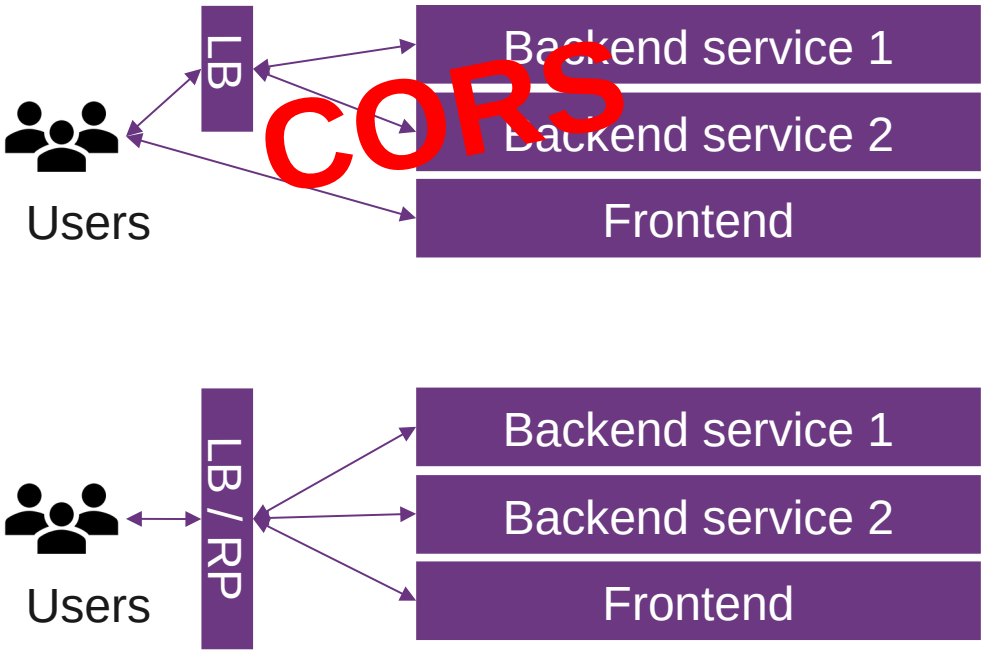
- CORS = Cross-Origin Resource Sharing
  - For security reasons, browsers restrict cross-origin HTTP requests initiated from scripts (among others)
  - Mechanism to instruct browsers that runs a resource from origin A to run resources from origin B
- Solution
  1. Use reverse proxy with builtin webserver, e.g., nginx, or user reverse proxy with external webserver.

     → The client only sees the same origin for the API and the frontend assets

  1. Access-Control-Allow-Origin: https://foo.example

     → For dev: Access-Control-Allow-Origin: *

- Reverse proxy



OST

Lecture 5

Authentication

- Authentication
  - Single-factor authentication
    - E.g. password
  - Multi-factor authentication / 2FA
    - E.g. password and software token, SMS (15.03.2021)
- Password rules
- Don’t use:
  - The name of a pet, child, family member, or significant other
  - Anniversary dates and birthdays
  - Birthplace
  - Name of a favorite holiday
  - Something related to a favorite sports team
  - The word "password“
- Don’t’ reuse passwords, use password managers

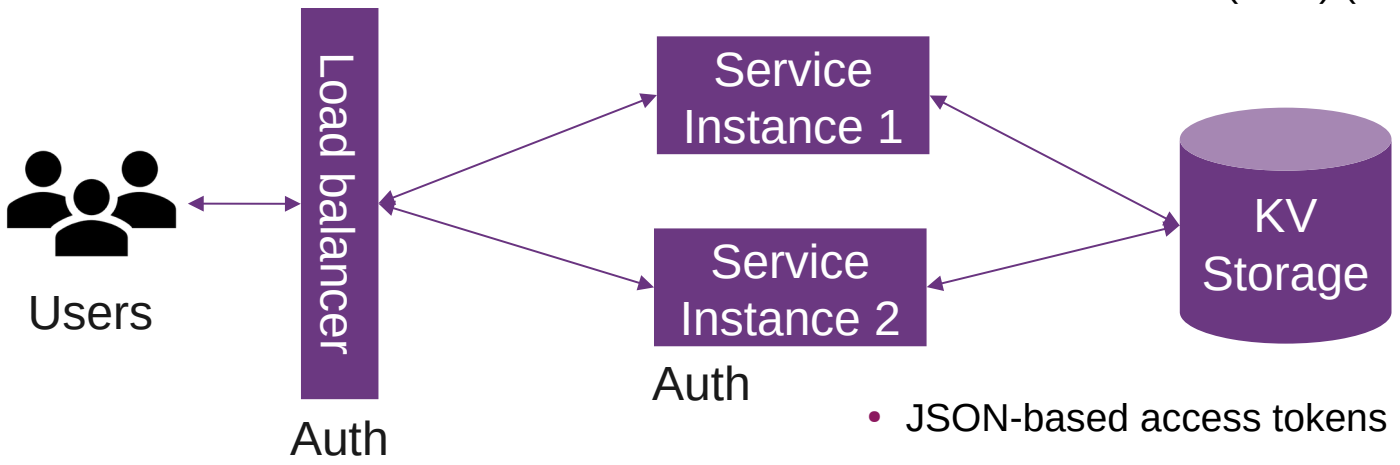
- Don’t enter passwords on unencrypted sites
- Password length:
  password cracking with 5000$ in 2018 with hashcat
  - Hashtype: WPA/WPA2: 1190.5 kH/s
- Combinations depend on PW complexity

Pw length	Combinations	Time
6	11m	9s
7	656m	9m
8	38b	8h
9	$7 * 10^{15}$	186y
10	$4 * 10^{17}$	11ky
11	$2 * 10^{19}$	665ky
12	$1 * 10^{21}$	38my

OST

Authentication

- Session-based authentication (stateful)
  - Sticky session
    - org.apache.catalina.session.StandardManager based on ConcurrentHashMap
  - JSON Web Token (JWT) (stateless)

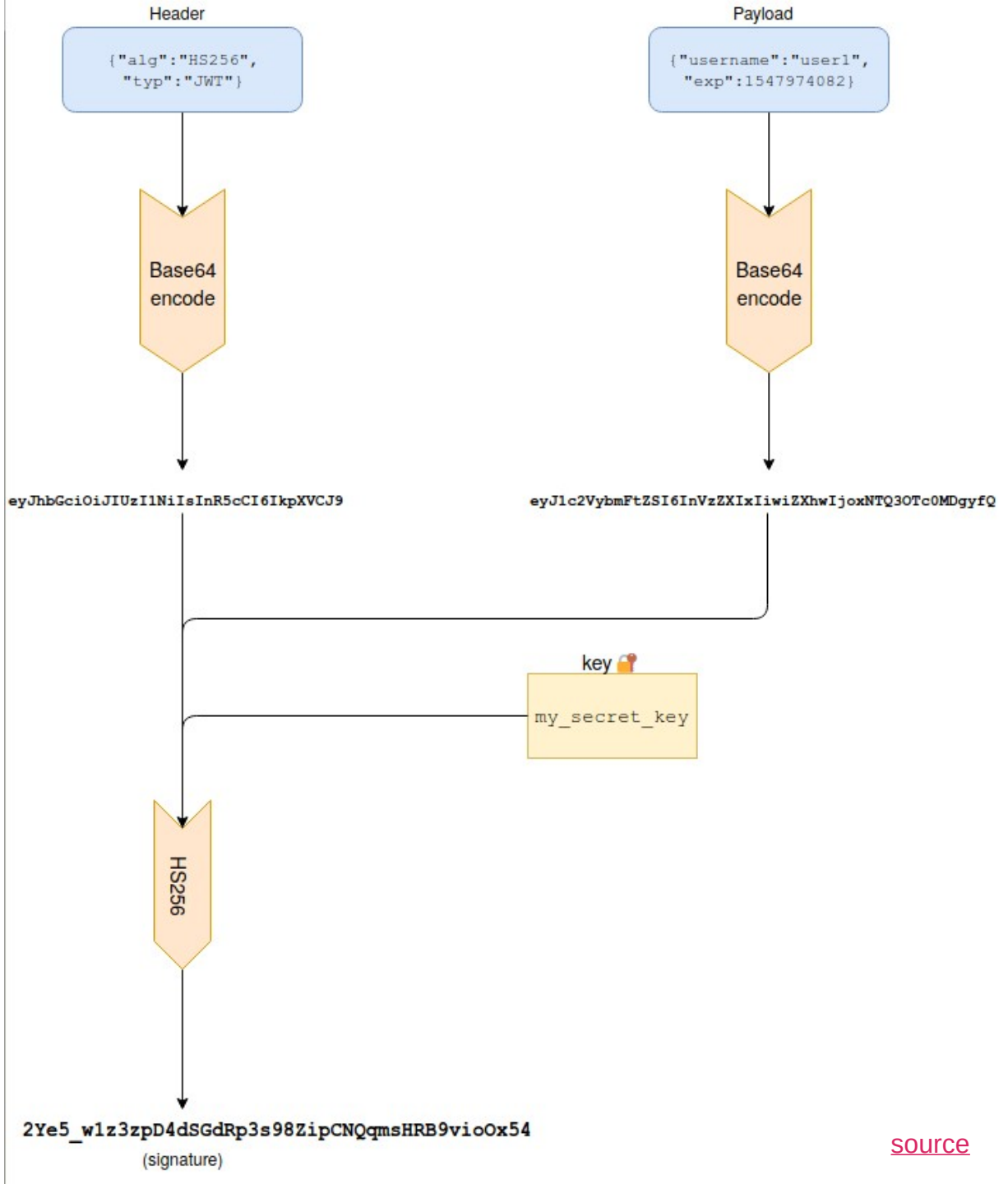


- E.g., spring-boot
  - Simple login app
  - JSESSIONID, Session information, that user was successfully authenticated: memory
  - JSON-based access tokens (jwt.io)
    - All server instances know a secret token / public key
    - When user logs in, server send back token
    - Client sends: Authorization: Bearer <token>
    - const user_token = base64urlEncoding(header) + '.' + base64urlEncoding(payload) + '.' + base64urlEncoding(signature)

OST

Authentication

- JSON-based access tokens
  - Header: {"alg" : "HS256"}
  - Payload: {“sub" : "tom", "role" : "admin", “exp" : 1422779638}
- Signature (simple): keyed-hash message
  - ~hash(base64(header)+base64(payload) + secret token)
- Client can store user_token in
  - localStorage.setItem(“token", userToken);
- Example in golang with JWT
  - Tutorial: here and here
- OAuth - protocol for authorization 3rd party integration
  - Grant access on other websites without giving them the passwords



source

Access Token / Refresh Token

- Access Token only short lifetime, e.g., 10min.
  - If public key / secret is known, the content in the token can be trusted, e.g., in the serivce
  - Can have userId, role, etc.
    - No need to query DB for those information, e.g.:

```
type TokenClaims struct {
     MailFrom string `json:"mail_from,omitempty"`
     MailTo   string `json:"mail_to,omitempty"`
     jwt.Claims
}
```

- Refresh Token longer lifetime, e.g., 6 month
  - A refresh token is used to get a new access token
  - IAM / Auth server creates access tokens
- Only access token, with long lifetime
  - If a user credential is revoked – how to inform every service?
- Only refresh token
  - Tightly coupled Service/Auth, every request to Service, Auth needs to be involved for every access
- Access + Refresh token
  - If a user credential is revoked, user has max. 10min more to access service
  - Auth only involved if access token is expired
- Authorization Code Flow with Proof Key for Code Exchange (PKCE)

OST

Lecture 6

Protocols

- Protocols, lecture 2: layer 4
  - TCP, UDP, (QUIC)
- Designing custom protocols (e.g. Kafka)

  - Needs more time to develop / test

  + Can be more efficient (space/performance)
- Protocol generators (binary): Thrift / Avro / Protocol Buffers / (ASN1)

  + IDL (interface description language) generates code

  + Standard

  - Has more overhead
  - e.g, Avro IDL - higher-level language for authoring Avro schemata → generates Avro schema

```
//Avro IDL
@namespace("ch.hsr.dsl")

protocol MyProtocol{
  record AMessage {
     string request;
     int code;
  }
  record BMessage {
     string reply;
  }

  BMessage GetMessage(AMessage msg);
}
```


OST

JSON example

- JSON + REST
  - Human-readable text to transmit data
  - Often used for web apps
- 187 bytes

```
func main() {
  fmt.Println("Connecting...")
  req, _ := http.NewRequest("POST",
"http://localhost:7000",
    strings.NewReader(`{"code": 5,"message": "Anybody
there?"}`))
  req.Header.Set("Content-Type", "application/json")
  client := &http.Client{}
  resp, err := client.Do(req)
  if err != nil {
    panic(err)
  }
  defer resp.Body.Close()
  fmt.Printf("wrote request")
}
```

- Parsing overhead, JSON slower than binary protocol - benchmarks

```
[
    {
        "id": "bitcoin",
        "name": "Bitcoin",
        "symbol": "BTC",
        "rank": "1",
        "price_usd": "9324.08",
        "price_btc": "1.0",
        "24h_volume_usd": "9039300000.0",
        "market_cap_usd": "158560288125",
        "available_supply": "17005462.0",
        "total_supply": "17005462.0",
        "max_supply": "21000000.0",
        "percent_change_1h": "0.46",
        "percent_change_24h": "-0.27",
        "percent_change_7d": "4.5",
        "last_updated": "1525011874“
    }, ...
]
```


OST

Application Protocol: HTTP

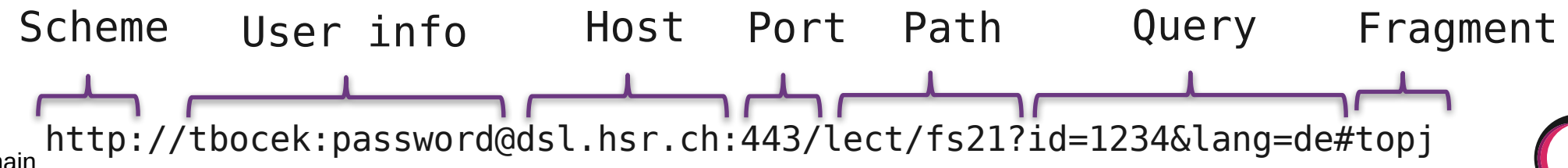
- HTTP (HyperText Transfer Protocol): foundation of data communication for www
- Started in 1989 by Tim Berners-Lee
  - HTTP/1.1 published in 1997
  - HTTP/2 published in 2015
    - More efficient, header compression, multiplexing
  - HTTP/3 wip
- Request / response (resource)
- HTTP resources identified by URL
  - https://dsl.hsr.ch/design/hsr_logo.svg

- Text-based protocol

```
openssl s_client -connect dsl.hsr.ch:443
… TLS handshake …
GET /
```

Request Headers (359 B)

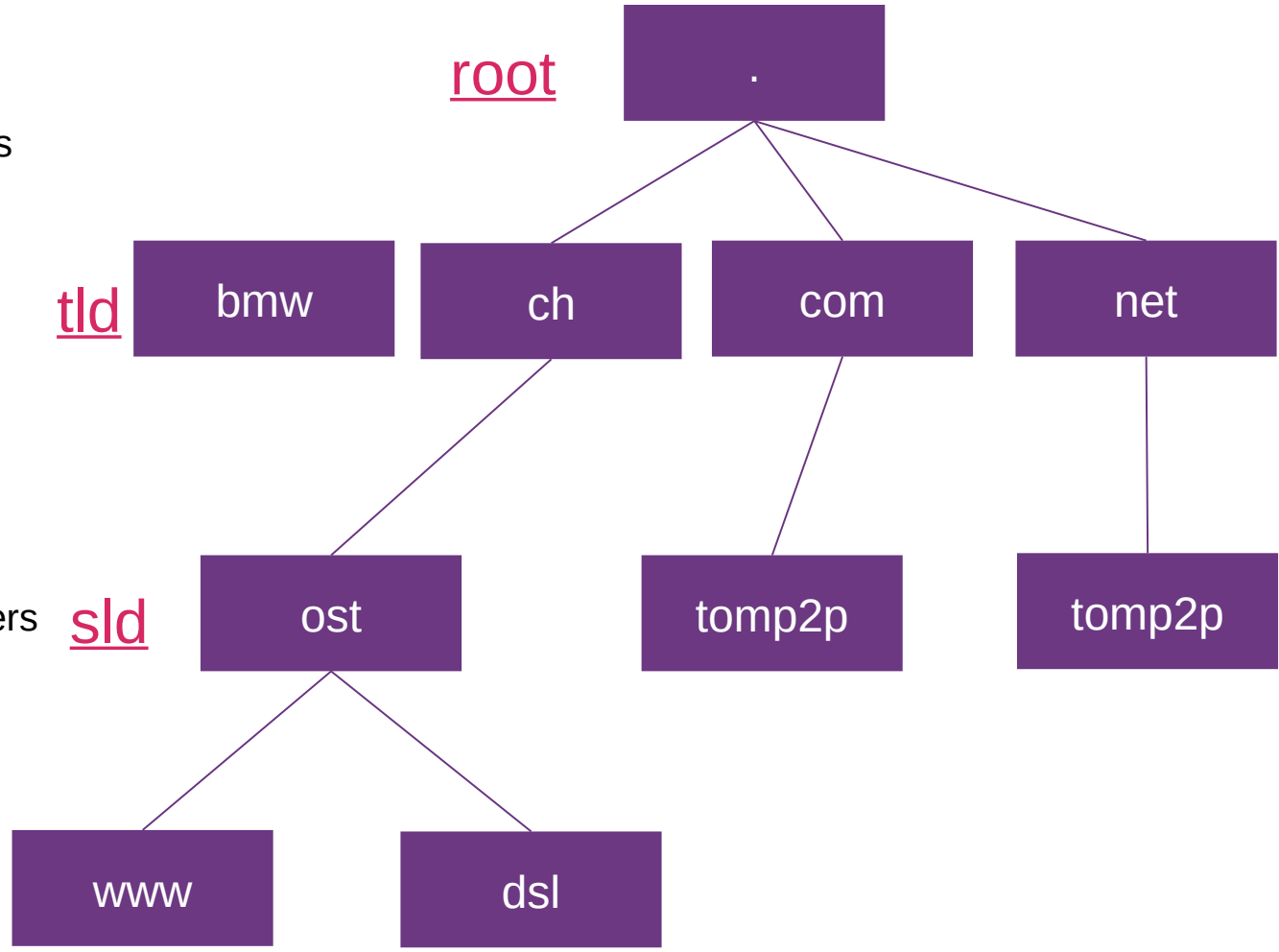
```
Host: dsl.hsr.ch
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
TE: Trailers
```



OST

Application Protocol: DNS

- Translates human readable domain names to IP addresses
  “phonebook of the Internet”
  - Delegate authority over sub-domains to other name servers
- Lots of new TLD
  : .zuerich, .bmw, .americanexpress, .youtube, .ϑϑ (application fee 185k USD)
  - No special characters: ASCII (no UTF)
  - Punycode: bücher.tld → xn--bcher-kva.tld
- Hierarchical and decentralized naming system for computers
  - E.g., dsl.hsr.ch
  - Uses UDP, port 53
  - Designed in 1983: unencrypted, unsigned
- Before DNS: exchange of hosts.txt
  - Does not scale



The DNS war

DoH

- provides confidentiality of lookups in transit
- Uses standard HTTP/2, on the standard port (443)
- Cannot distinguish between traffic/DNS
- Trivially deployed , DNS response are served like simple web pages
- Performance: TCP+TLS handshake → 2/3 RTT
- But: Cloudflare is close to you
- Difficult upgrade path for clients: per-application installation
- Browsers can perform DNS queries using Javascript

DoT

- provides confidentiality of lookups in transit
- DNS over TLS, separate port (853)
- Can be blocked
- Widely supported by serving software (Bind, PowerDNS, Unbound) and public resolvers (Cloudflare, Quad9, Google)
- Performance: TCP+TLS handshake → 2/3 RTT
- But: ISP is close to you
- Easy upgrade path for clients: clients can test if the configured resolver supports DoT on port 853, fall back to DoU53 otherwise)

OST

Lecture 9

Introduction

- Bitcoin is an experimental digital currency
  - Bitcoin is fully decentralized (no central entity)
  - Smallest unit: 0.00000001 BTC (1 satoshi)
- Key characteristics
  - Maximum of ~21 million BTC
  - Every transaction broadcast to all peers
    - Every peers knows all transactions (~366 GByte)
  - 1st Bitcoin issued on January 3, 2009
- The initiator is unknown so far

https://www.thedailysatoshi.com/

OST

WIRED SUBSCRIBE » SECTIONS » BLOGS » REVIEWS » VIDEO » HOW

Sign In | RSS Feeds

FEATURES
For *John Carter*, Director Andrew Stanton Leaps From Animation to Live-Action Sci-Fi

START
MIT's Sebastian Seung Wants Computers to Map the Brain

PLAY
The Five-Year Engagement Takes Director Nick Stoller Off the Grid

/ MAGAZINE

FEATURES 19.12

The Rise and Fall of Bitcoin

759 348 123 Tweet +1 Share

By Benjamin Wallace | November 23, 2011 | 2:52 pm | Categories: Wired December 2011

The Economist

Log in | Register | Subscribe

Digital & mobile | Events | Topics A-Z | Newsletters | Jobs

Tuesday May 8th 2012

Search

World politics | Business & finance | Economics | Science & technology | Culture | Blogs | Debate | The World in 2012 | Multimedia | Print edition

Babbage
Science and technology

Previous | Next | Latest Babbage

Latest from all our blogs

Comment (45) Print

E-mail Permalink

Reprints & permissions

Virtual currency

Bits and bob

Jun 13th 2011, 20:30 by J.P. | LONDON

Like Tweet 625

About Babbage

In this blog, our correspondents report on the inters between science, technology, culture and policy. T takes its name from Charles Babbage, a Victorian mathematician and engineer who designed a mec computer.

Follow @EconSciTech 22.8K followers

RSS feed

From 2011

de fr it

Ihr Ort: Zürich 19° Mi 20° Do 26° Über Schweiz

Registrieren Login

20 minuten ONLINE

Video TV Infografik Games E-Prospekte RSS

Inhalt A-Z Suchen

Schweiz Ausland Panorama Wirtschaft Sport Blockbuster People Entertainment Digital Mehr

News SMI Alle Indices Ratgeber Geld Trading Anlageprodukte Finanzrechner Dossiers

Ihre Story, Ihre Informationen, Ihr Hinweis? feedback@20minuten.ch

BITCOIN, DIE DEVISE IM WEB

07. Juni 2011 07:15; *Akt: 07.06.2011 09:11*

Der gefährliche Cyber-Dollar

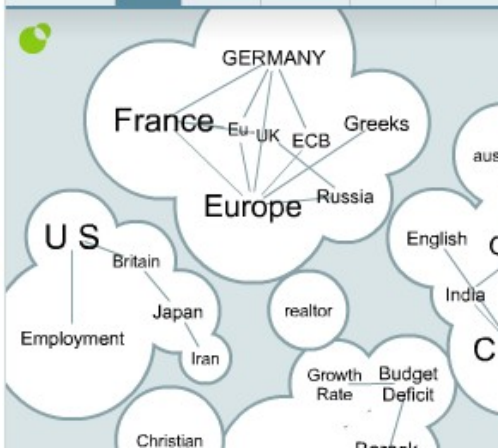
von Gérard Moinat - Die Online-Währung Bitcoin wirft hohe Wellen. Es sei das «gefährlichste Open-Source-Projekt aller Zeiten» und «gefährde

ought ought
ly,
stment
y a

Trending topics

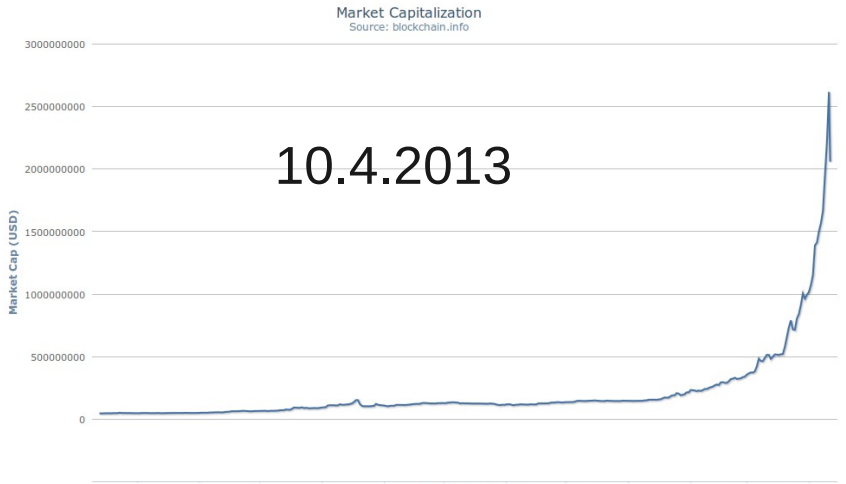
Read comments on the site's most popular topics

Period: 1 day | 1 week | 2 weeks | 30 days



Bitcoin‘s Market Capitalization in USD

- Bitcoin boom, started in 2013 – current price



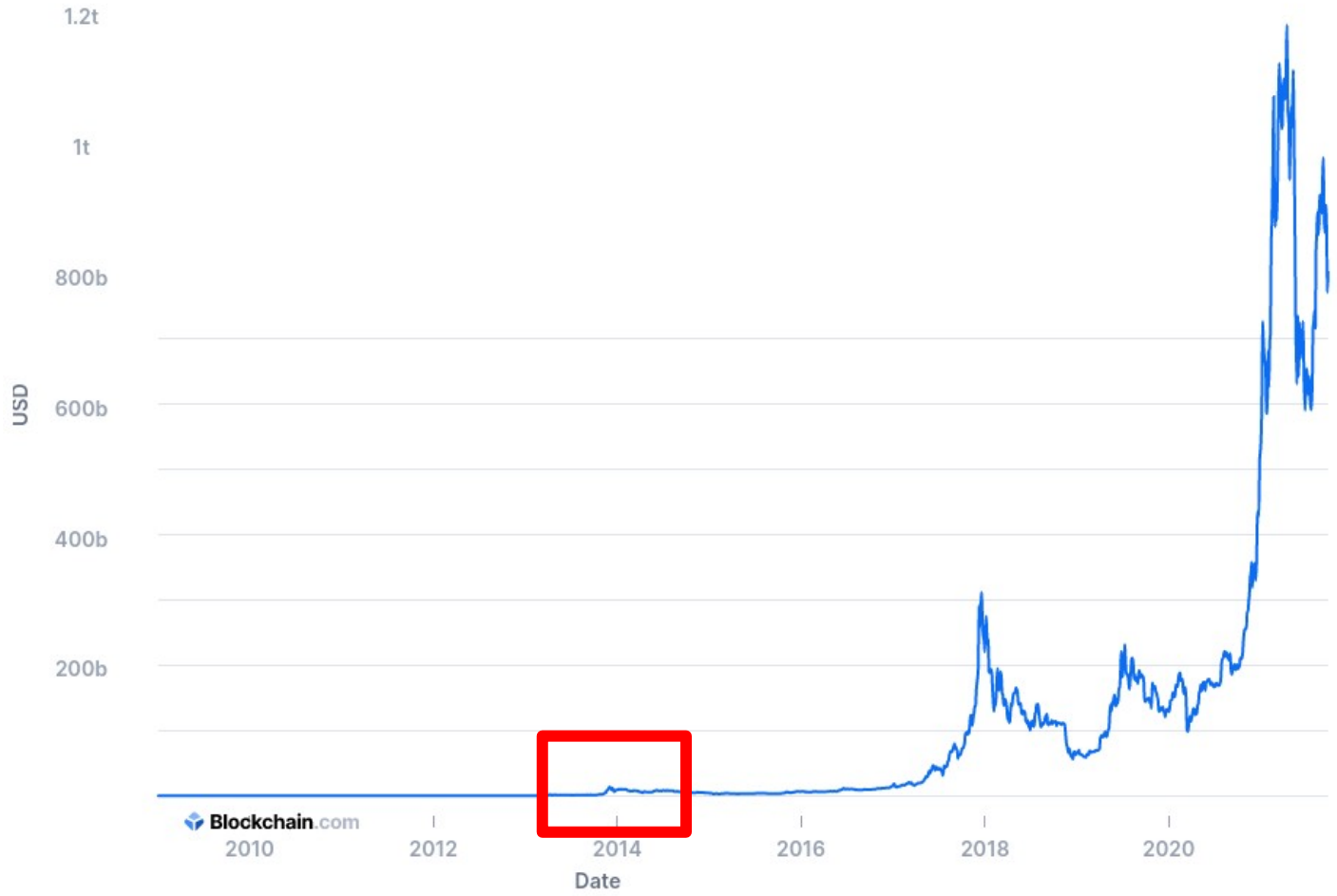
10.4.2013

24.4.2013

26.4.2014

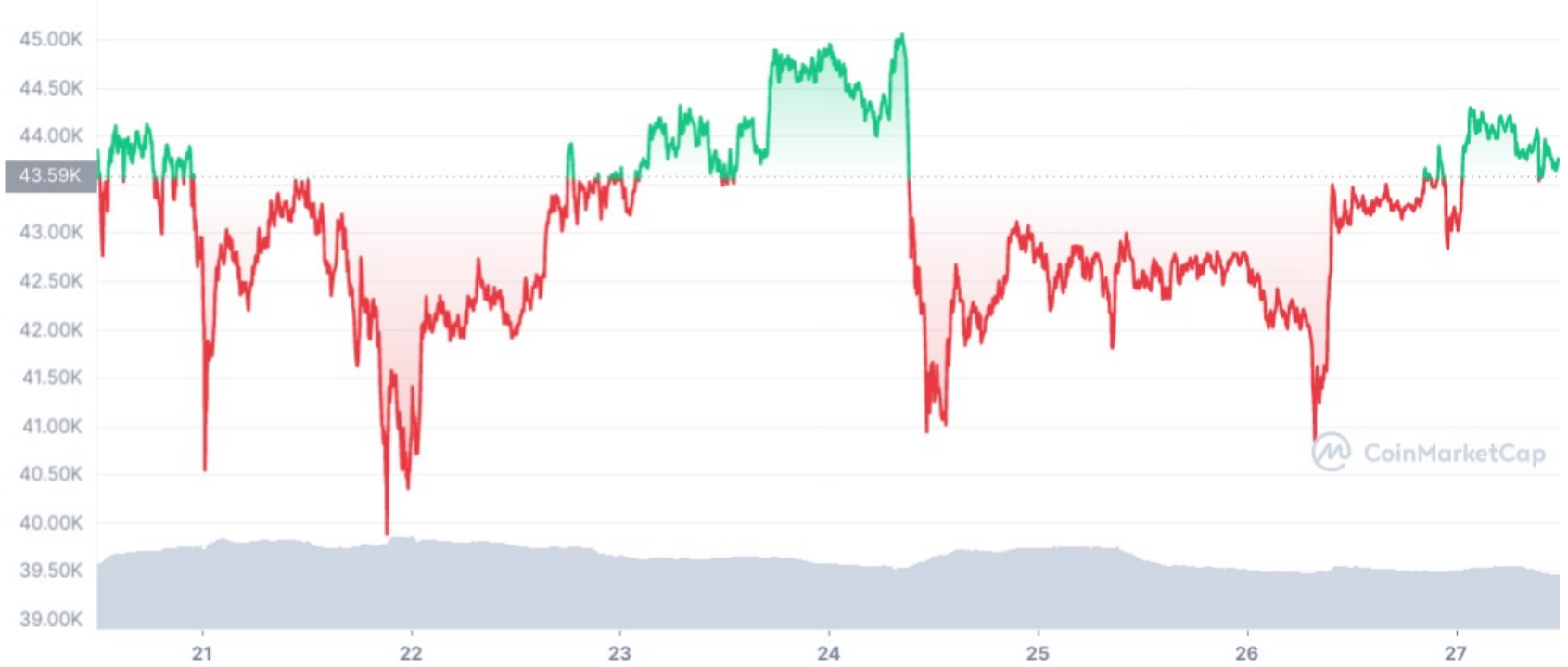
22.4.2015

Bitcoin‘s Price USD 2021



Bitcoin‘s Price USD 2021

- What happened on the 24.9.2021?
- 24.9.2021: China declared that cryptocurrency transactions and mining are illegal



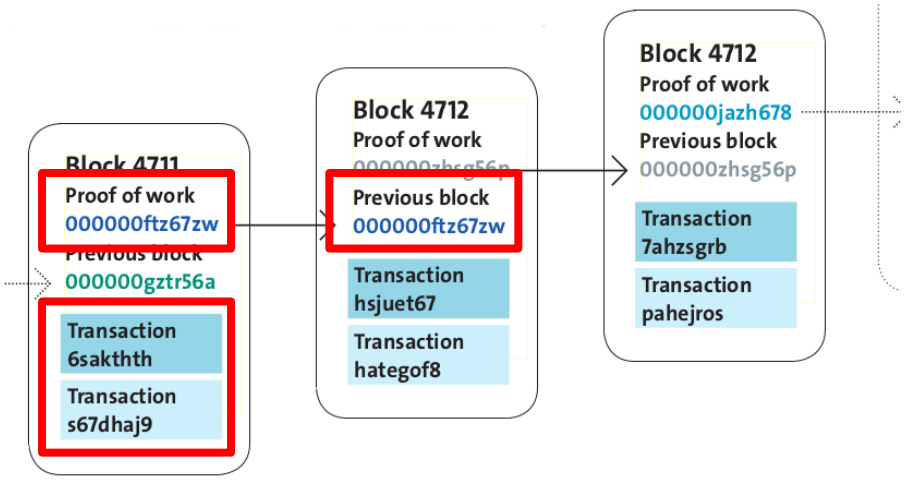
Timeline of China vs. Crypto [source]

- Fall 2013
  - China bans banks from handling bitcoin transactions, calling it a “virtual good” and not legal tender.
  - BTC China, the country’s largest bitcoin exchange, stops taking deposits in yuan under pressure from payment processors and the government.
- Fall / Winter 2017
  - Amid a crypto boom, China says it is investigating market manipulation and money laundering through bitcoin.
  - China bans initial coin offerings (ICOs).
  - Crypto exchanges are banned in China. Citizens largely get around the ban by using offshore exchanges and peer-to-peer trading.
- Fall 2019
  - China considers eliminating crypto mining but eventually declines to act.
- Spring 2021
  - China cracks down on crypto mining, as mining activities start to threaten the country’s environmental goals.
  - The government bans financial institutions and payment companies from providing crypto-related services.

OST

Blockchain (e.g., Bitcoin)

- Alice sends Bob 1 BTC
  - Transactions are collected in blocks
  - New block created approximately every 10 min
- A block has a pointer to previous block
- Blocks contain solved crypto puzzles
  - Creation of blocks is called mining (reward)
  - In the form of partial hash collisions (SHA256)



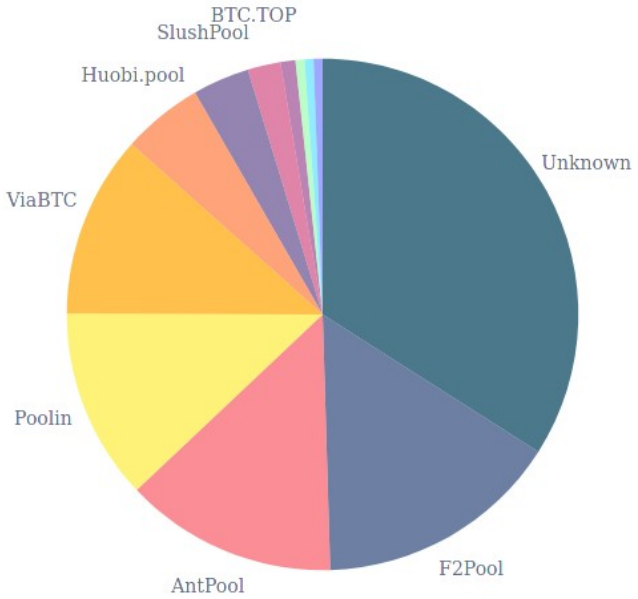
Cryptographic Hash Function

- One-way function
  - Easy to calculate hash (949bd2f7a173661b1b87efff86b2b20b8c5d07c067698c58ad98887396faccb3) if “Hello OST” is known
  - Difficult to calculate “Hello OST”, if only 949bd2f7a173661b1b87efff86b2b20b8c5d07c067698c58ad98887396faccb3 is known
  - Example

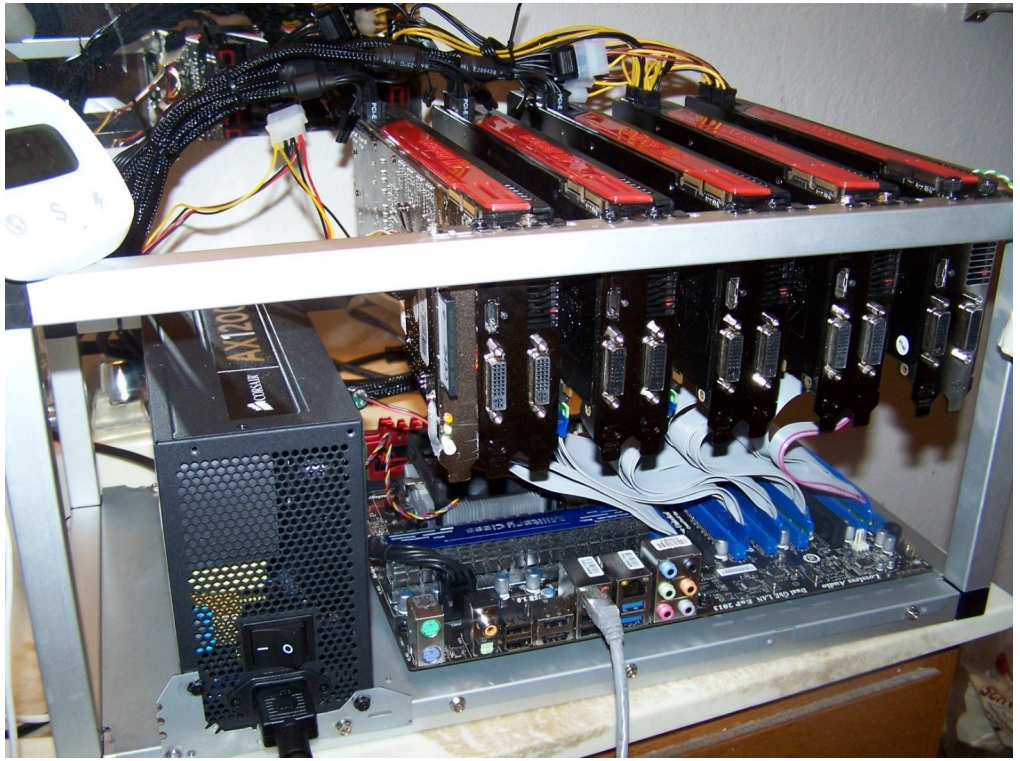
OST

Mining

- Miners specialized, AMD GPUs, ASIC (application-specific integrated circuit) [1][2][3]
- Mining = finding solution to crypto puzzle



http://blockchain.info/pools



https://bitcointalk.org/index.php?topic=7216.560

OST

Mining

- Mining farms: [1], [2], [3], [4], [5], [6], [7]

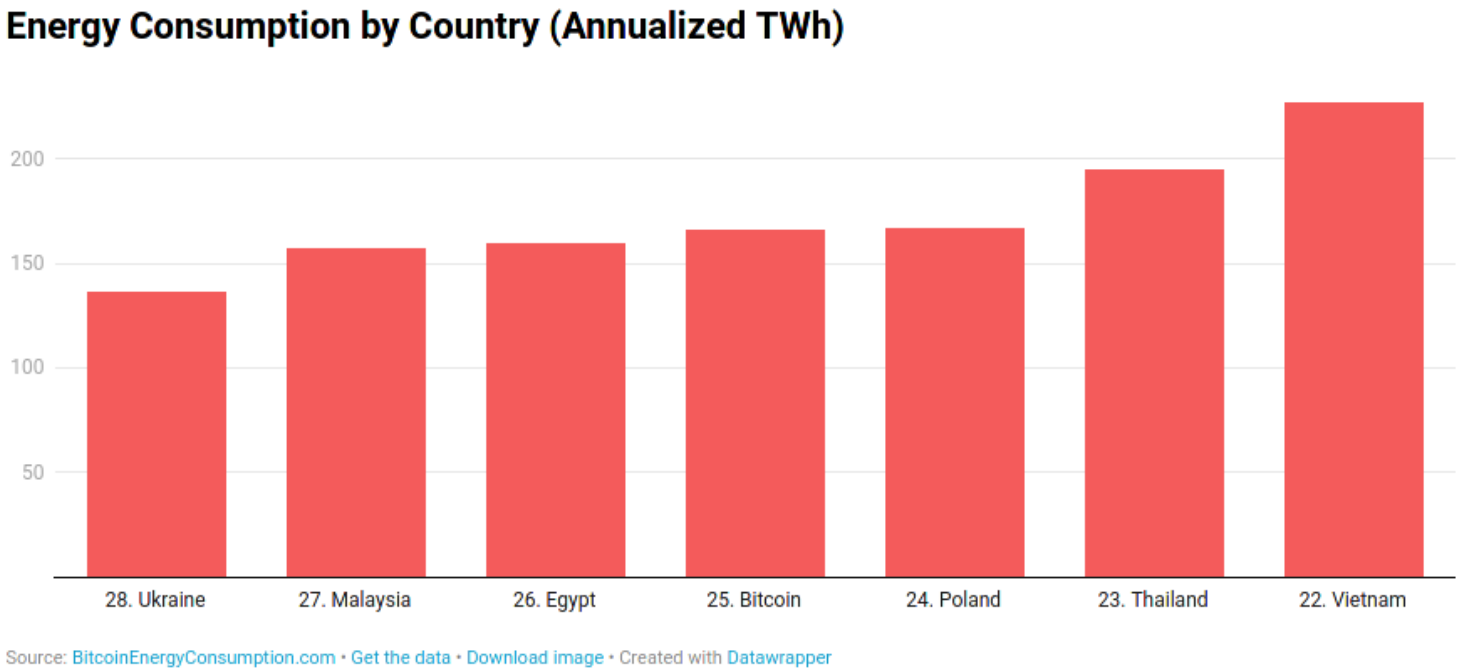
http://www.openmobilefree.net/?p=1308

Source: https://www.datacenterdynamics.com/en/news/knc-miner-to-build-second-facility-in-the-node-pole/

OST

Electricity

- High energy consumption [source], Switzerland ~60TWh
- Visualized
  - Ethereum? ~75TWh



OST

Ethereum

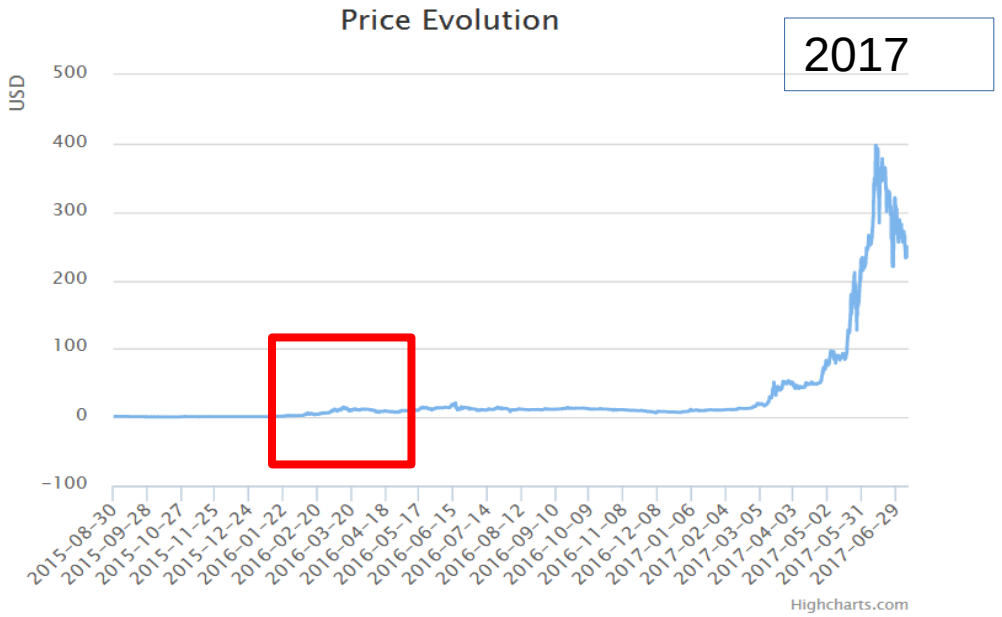
- Ethereum (1 ETH ~3000$)
- White paper released in December 2013
- Protocols designed from scratch (not a Bitcoin clone)
- Ethereum foundation located in Zug (initiator known) - non-profit foundation
- Mining reward ~2 ETH (“always”, unlike Bitcoin)
- Blockchain with smart contracts (loops, arithemitcs, etc.)
  - Smart contract programming

Vitalik Buterin

OST

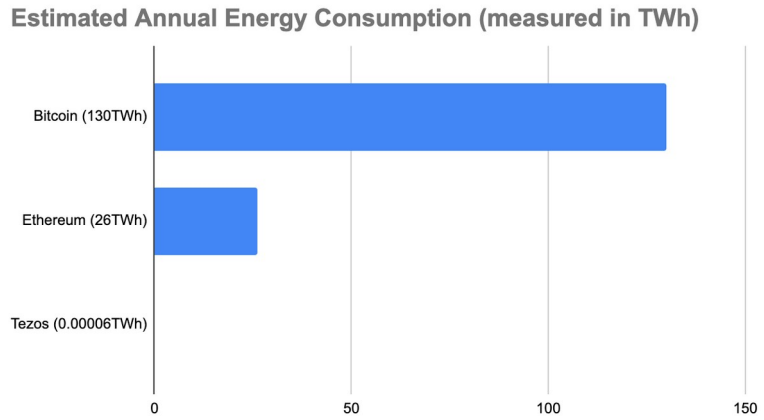
Ethereum in Numbers

- 2nd in market cap ~ 352b USD
- Block every ~14s
- Crytpo puzzle memory hard (difficult for ASICs)
  - Avoid miner centralization
  - ~75TWh



Ethereum 2.0

- Current problem: crypto puzzles need a lot of energy
  - ETH 2.0 – change from proof-of-work to proof-of-stake (research started 2013, still ongoing)
  - Tezos has proof-of-stake ~60 MWh
- Why not use a energy friendly blockchain?
  - Cardano (13.9.2021) - Cardano launches smart contracts after successful hard fork
  - Binance Coin (not considered decentralized)
  - Ethereum has (in my opinion) the best developer tooling and ecosystem
  - Bitcoin? well...
- The future (my opinion): energy friendly blockchains with e.g., proof-of-stake or other alternatives)

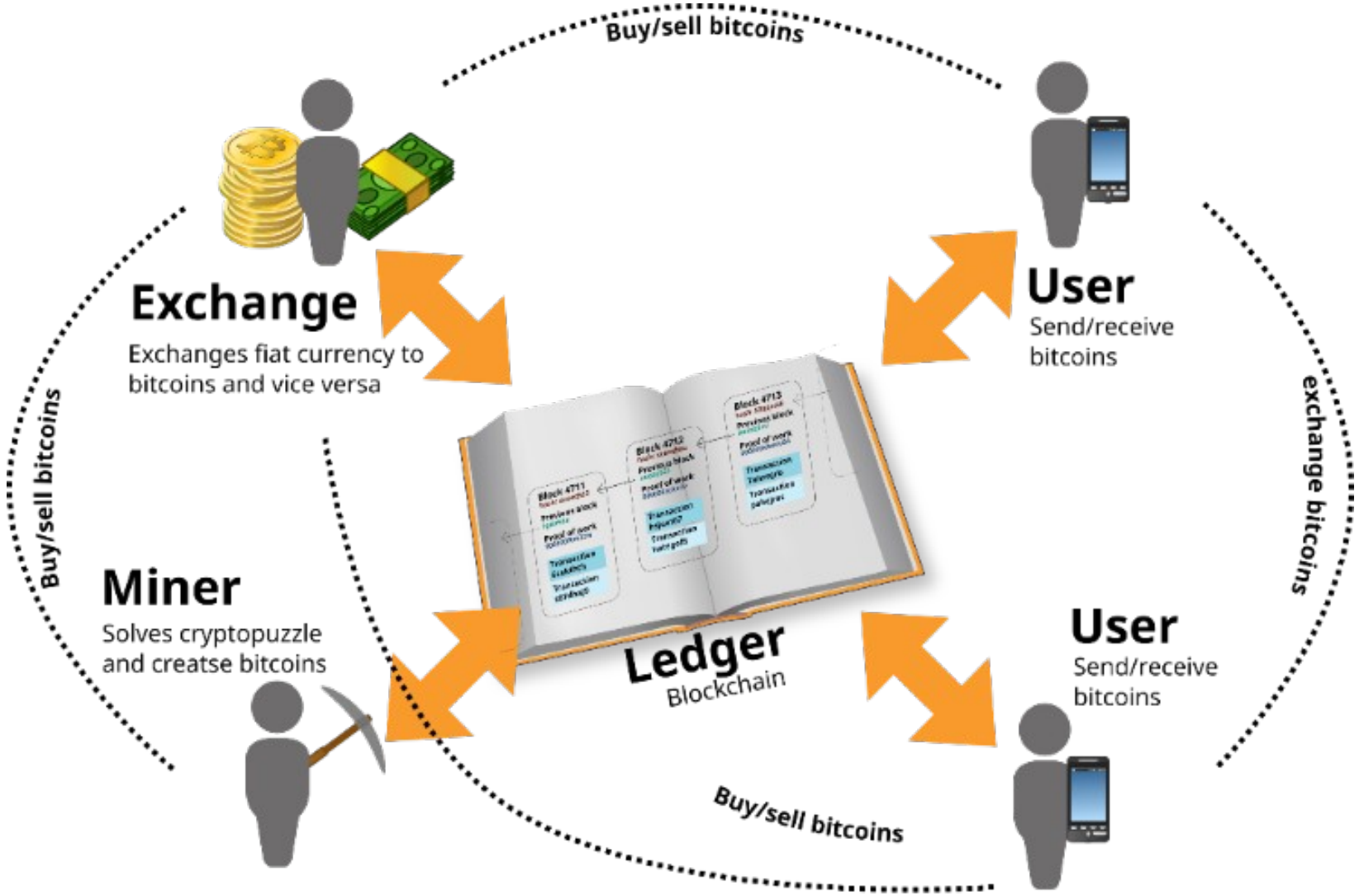


https://medium.com/tqtezos/proof-of-work-vs-proof-of-stake-the-ecological-footprint-c58029faee44

OST

Lecture 10

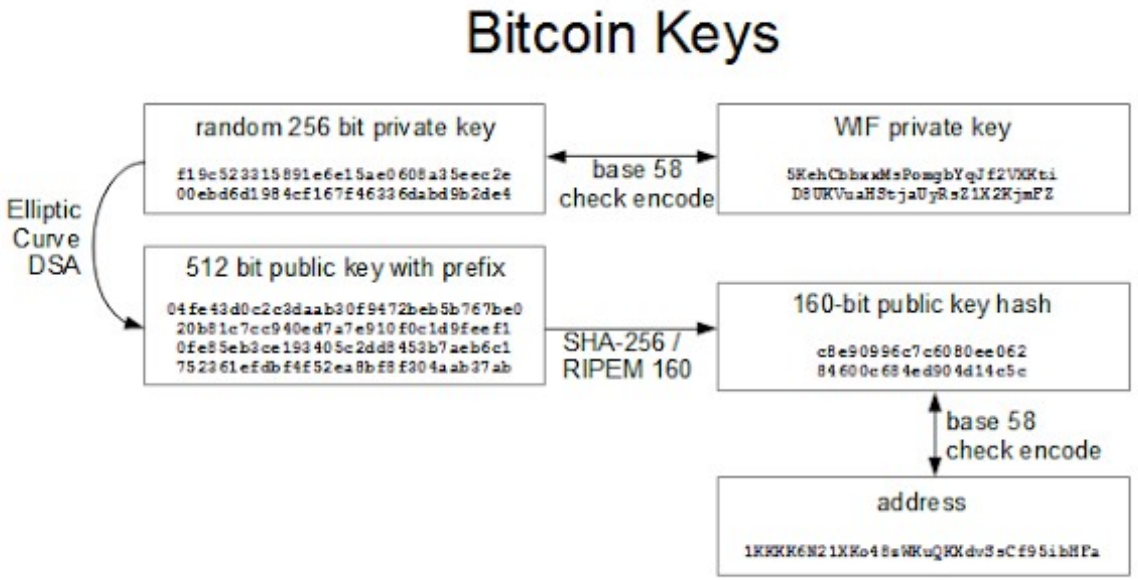
Summary: Bitcoin Stakeholders

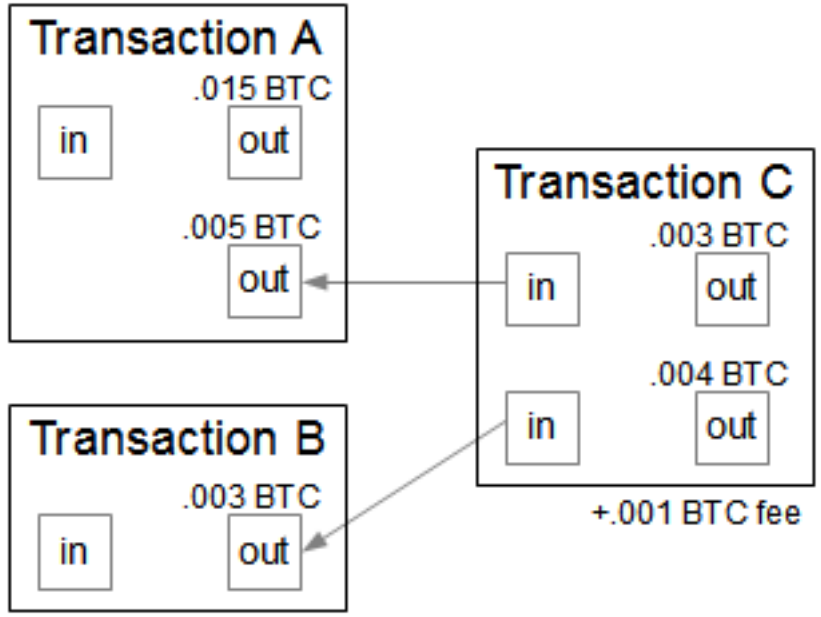


OST

Bitcoin in Detail

- Good information: http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html





OST

51% Attack

- “If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.”
  - https://bitcoin.org/bitcoin.pdf
- PoW: majority of hashing power, PoS: majority of coins
- How expensive is a 51% attack?
  - Buy an attack?
- Double spend, or rollback transactions
  - X is an exchange
  - Mine secretly, Y is your address
  - X arrived – payout (1 block conf.)
  - You mine faster, broadcast secret chain
  - Tx F→X: 15 never happened, goes to Y
- 04.08.2021: Bitcoin SV Faces a 51% Attack [link]