Blockchain Technology in Healthcare

Alexander Schönhuth

UNIVERSITÄT BIELEFELD
Faculty of Technology

Bielefeld University
April 27, 2022

Organization

Blockchains
–
Motivation

Bitcoin
–
Motivation

Bitcoin
&
Blockchains

Basic Information

- *Organization:*
  - How do lectures, tutorials etc work
  - What tools will be used
- What is the basic motivation behind *Blockchains*? What is the meaning of
  - Immutability
  - Transparency and Anonymity
  - Decentralization
- Why is there *Bitcoin*? What/Who is
  - Electronic cash
  - Double spending
  - Satoshi Nakamoto
- *Bitcoin and Blockchains:* What are
  - Preserving value
  - Having a ledger
  - Blocks of transactions
  - Proof of Work

Organization

Blockchains
–
Motivation

Bitcoin
–
Motivation

Bitcoin
&
Blockchains

PREREQUISITES, LECTURES, EXERCISES

- Lectures: Wednesdays, 12-14; hybrid or online meetings
- Lectures will be recorded
- Edited videos and slides will be posted
- Exercises: 5 assignments + 1 exam preparation session

Assignments, Exam

- *Tutorials / Assignments:*
  - New exercise sheets provided on Wednesdays May 4, May 18, June 1, June 15, June 29, after the lecture
  - Exam preparation: July 6
  - Exercises to be submitted by Tuesday, **23:59** twelve days thereafter; Discussion on Thursday, 10-12 same week
  - Submission of exercises in groups of 2-3 people possible
  - Everyone is supposed to present at least one exercise in the tutorials
  - Upload to corresponding folder in the "Lernraum Plus"
  - First exercise sheet uploaded on 4th of May (next week)
- *Exam:*
  - Presence exam planned for **Wednesday, July 13, 2022 between 10:00 and 14:00** (may be subject to changes due to situation; we will communicate changes as timely as possible)
  - Admitted: everyone exceeding 50% of total exercise points

Tutorials

- Every **Thursday, 10-12**
- Tutor: Johann Verolet
- Tutorials will be in English
- Presence or Zoom meetings: yet TBD (links will be provided in time)
- Presentation of solutions during the online meeting individually

COURSE MATERIAL

- … available on course website: `https://gds.techfak.uni-bielefeld.de/teaching/2022summer/dsh`
  - Slides and pointers to literature
  - Excercise sheets
- Lernraum Plus: `https://lernraumplus.uni-bielefeld.de/course/view.php?id=13387`
  - Submission of exercise solutions
  - Self-managed forum

LITERATURE AND LINKS

- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder (2016). *Mining of Massive Datasets*. 3rd Edition, Cambridge University Press.
- *Download:* `https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf`
- *Further materials:* `https://bitcoinbook.cs.princeton.edu/`
- *Other literature:* See Lernraum Plus, course website and lecture slides

COURSE CURRICULUM

Part 1: Foundations / Bitcoin

- Introduction / Motivation
- Cryptography / Cryptocurrencies
- Decentralization
- Cryptocurrency Mechanics
- Application I: Griggs Paper

Part 2: Extensions / Applications

- Smart Contracts: Motivation
- Ethereum Blockchains
- Solidity Tutorial
- Applications II, III, IV: MedRec, FHIR, Maslove Paper

Organization

Blockchains
–
Motivation

Bitcoin
–
Motivation

Bitcoins
&
Blockchains

Major Applications

- Management of individual medical records
- Insurance claim processes
- Clinical / biomedical research / studies
- Biomedical / health care data ledger

Central Benefits

- Immutability: once deposited, data cannot be changed
- Transparency: every participant can see data
- Anonymity / Security: real identities not revealed
- Robustness: Data resistant to blackouts / technical failurs
- Decentralization: Nobody ”owns” the data

Example
–
Electronic health records (EHR)

EHRs - Immutability

Use case - Bob visits a doctor

- Bob has a stomach ache and visits doctor Alice
- Alice assumes Bob ate too much and isn't really sick
- Alice prescribes chamomile tea and puts the case to her files

EHRs - Immutability

Use case - Bob gets misdiagnosed

- However, Bob has a severe infection and has to go to the hospital
- Alice is afraid that she is going to face repercussions because of her mistake
- Alice would like to access Bob's file to fake the evidence and change Bob's diagnosis

Databased management systems (DBMSs) versus Blockchains

- *Database management systems (DBMSs)* have ”delete” and ”modify” functionalities, so that's possible
- *Blockchains support immutability:* no record can be altered retroactively

EHRs - Privacy / Transparency

Use case - Accessing Bob's files

- Independent authorities
  - get access to Bob's files to evaluate the situation
  - should not be able to identify Bob's identity
  - should nevertheless be sure it's from the right patient
  - should be able to make sure that records are consistent

DBMSs vs Blockchains

- *DBMSs:* Records contain names, addresses etc, to identify ownership of records; records could not be approved by patients
- *Blockchains:*
  - Privacy through anonymized identifiers, while still assignable to real people when necessary
  - Enhanced transparency, everyone can check validity of records without discovering Bob's real identity

EHRs - Decentralization

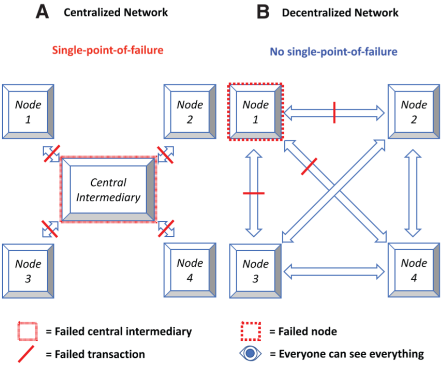
Use case - Bob goes to the hospital

- Bob does not trust Alice any longer and goes to the hospital instead
- At the hospital, he receives treatment against the infection
- However, the hospital was subject to a hack and all data got lost, which prevents Walter, the new doctor, to treat Bob
- Bob has to undergo a series of test, so that the doctors can continue his treatment

DBMSs vs blockchains

- *DBMSs:* Centralized storage, so no remote backups available
- *Blockchains:* Build on decentralized network.
  - Records are stored ”everywhere in the network”
  - This avoids ”single points of failure”

Motivation - Decentralization



A: Central authority (e.g. running a DBMS), single point of failure

B: Cluster / cloud: no single point of failure. However, no transparency, anonymity, immutability

☞ We'll get to all of that!

Other Prominent Applications

Insurance Claim Processes

- *Immutability:* No party involved can tamper with relevant records / evidence; audits facilitation and fraud detection
- *Transparency:* All records that support decisions verifiable by anyone involved
- *Anonymity / Security:* No hacking of medical / financial information
- *Robustness:* Patient data accessible from multiple silos
- *Decentralization:* No intermediaries who could have own interestes necessary

Clinical/Biomedical Studies/Research

- *Immutability:* Trackable, timestamped patient-generated data
- *Transparency:* Continuous access to real-time data and information on provenance, overall verifiability. Relevant cross-study insights can be gained
- *Anonymity / Security:* No real-world identities to be maintained other than with the participating patients themselves
- *Robustness:* No broken real-time data records.
- *Decentralization:* Each institution keeps control of their own resources, while allowing for full collaboration on shared data

Health Care Data Ledger

Internet of Things, Mobile Devices

- *Immutability:* Providing ordered (timestamped), continuously updated data
- *Transparency:* Forged, poor quality or stolen data easily identified
- *Anonymity / Security:* Patients can provide access to data using cryptographic protocols
- *Robustness:* Drug counterfeiting in drug supply chains impossible
- *Decentralization:* Data ”pooled”, so central authorities do not prevent individual usage

Organization

Blockchains
–
Motivation

**Bitcoin
–
Motivation**

Bitcoin
&
Blockchains

Bitcoin

–

Online Cash

Offline Cash

Disadvantages

- Needs to be ”bootstrapped”: initial distribution of cash to participants necessary
- Physical presence required for transactions

Advantages

- Full anonymity: no spending records, no identities
- Offline transactions, no involvement of third parties

Electronic Banking

Credit Cards

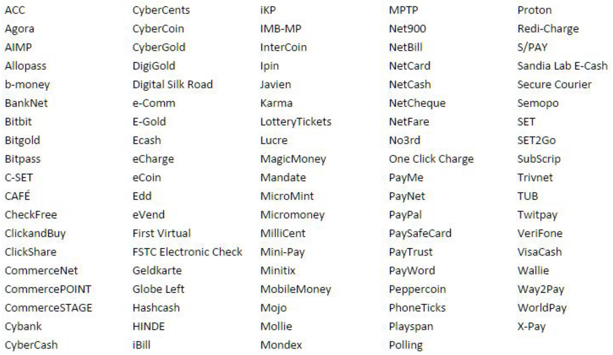
- Buyer sends credit card details to seller; seller contacts ”system”
- The ”system” involves various third parties: banks, processors, credit card intermediaries, and so on
- *Disadvantages:*
  - Seller has credit card details
  - Third parties, even if trustworthy, can exploit records for legal things

PayPal

- Buyer and seller communicate via PayPal
- Seller does not receive credit card details
- *Disadvantages:*
  - PayPal has access to personal data
  - Buyer and seller need account with PayPal

Online Buying / Selling

Situation before Bitcoin



ACC
Agora
AIMP
Allopass
b-money
BankNet
Bitbit
Bitgold
Bitpass
C-SET
CAFÉ
CheckFree
ClickandBuy
ClickShare
CommerceNet
CommercePOINT
CommerceSTAGE
Cybank
CyberCash
CyberCents
CyberCoin
CyberGold
DigiGold
Digital Silk Road
e-Comm
E-Gold
Ecash
eCharge
eCoin
Edd
eVend
First Virtual
FSTC Electronic Check
Geldkarte
Globe Left
Hashcash
HINDE
iBill
iKP
IMB-MP
InterCoin
Ipin
Javien
Karma
LotteryTickets
Lucre
MagicMoney
Mandate
MicroMint
Micromoney
MilliCent
Mini-Pay
Minitix
MobileMoney
Mojo
Mollie
Mondex
MPTP
Net900
NetBill
NetCard
NetCash
NetCheque
NetFare
No3rd
One Click Charge
PayMe
PayNet
PayPal
PaySafeCard
PayTrust
PayWord
Peppercoin
PhoneTicks
Playspan
Polling
Proton
Redi-Charge
S/PAY
Sandia Lab E-Cash
Secure Courier
Semopo
SET
SET2Go
SubScrip
Trivnet
TUB
Twitpay
VeriFone
VisaCash
Wallie
Way2Pay
WorldPay
X-Pay

Many more have tried without success

From `https://bitcoinbook.cs.princeton.edu`

BITCOIN ELECTRONIC CASH

Bitcoins versus Cash

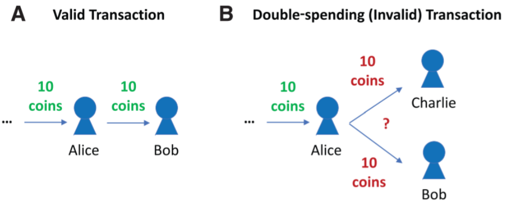
- Bitcoin does not reach full anonymity
- Bitcoin does not reach no involvement of third parties
- *However:* Bitcoin comes very close using cryptographic principles

Bitcoins: Principle and Major Issue

- Money is a piece of data
- *Caveat:* Copy piece of data, and spend it twice

"Double Spending"

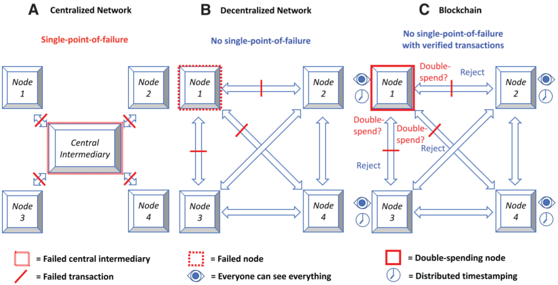
Double Spending



From Kuo et al., 2018

- As of today, no solution without central authority conceivable
- *Issue:* Adding unique identifiers to pieces of data (= coins!) requires central server to keep track of identities of coins
- *Bitcoin:* Don't worry – let double spending happen, detect it afterwards, and reverse it in the shortest amount of time possible

DECENTRALIZATION



From Kuo et al., 2018

Advantages of Blockchains

- No single ”point of failure”
- No central authority
- Everyone observing everything suppresses ”double spending”

Creating Bitcoin I

- The *creator of Bitcoin* adopted the pseudonym *Satoshi Nakamoto*.
- Female or male, one or several people? Nobody knows.
- Started coding in May 2007; claimed domain `bitcoin.org` in August 2008
- Released white paper in October 2008; soon thereafter released the code
- By December 2010, others had taken over maintenance

Creating Bitcoin II

- *Fun fact:* Wikipedia planned to dismiss Bitcoin mid 2010 because of missing relevance
- Bitcoin was the first decentralized platform to work; many concepts were entirely new, circumventing various patents for electronic cash systems released by others
- Reasons for anonymity:
    - Just for fun...
    - Legal worries: founders of ”Liberty” and ”e-Gold” accused for money laundering, guilty plea shortly before spring 2008
    - Satoshi, likely, is stinking rich, as possessing lots of bitcoins...

MATERIALS / OUTLOOK

- See *Bitcoin and Cryptocurrency Technologies*, Preface
- See `https://bitcoinbook.cs.princeton.edu/` for further resources
- Further: T. Kuo, H.Kim and L. Ohno-Machado (2017): *Blockchain ditributed ledger technologies for biomedical and health care applications*
- Next lecture: “Cryptography I”
  - See *Bitcoin and Cryptocurrency Technologies* 1.2–1.4, 2.1
  - The Internet Society (2006). `https://www.rfc-editor.org/rfc/rfc4634`, page 6