HS19

DISTRIBUTED SYSTEMS ADVANCED & BLOCKCHAIN

Exam Preparation and Brief Introduction to Elliptic Curve Cryptography

T. Bocek

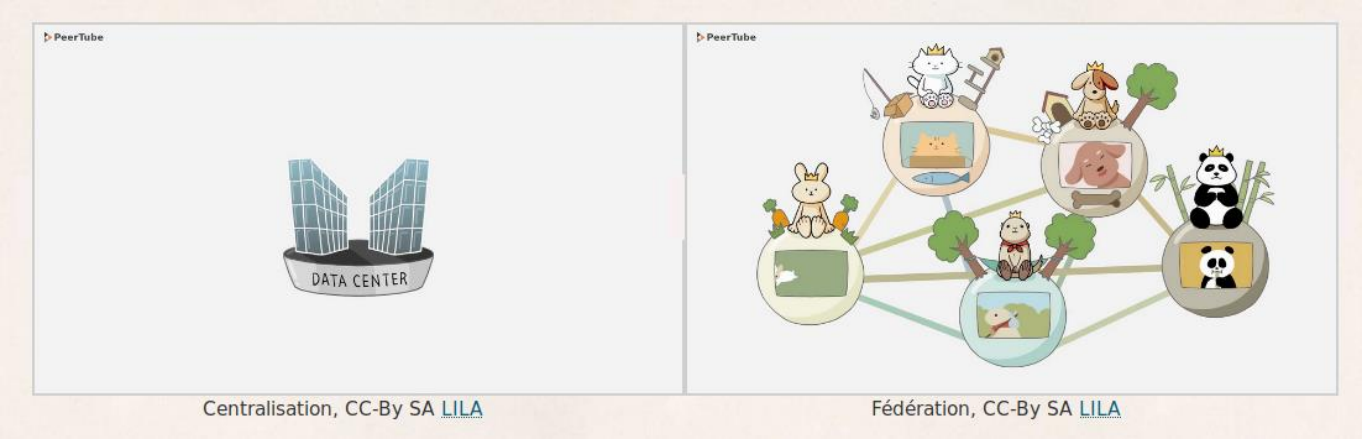
thomas.bocek@hsr.ch

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Distributed Systems - In the *News*

- **12.11.2019: Binance Exchange Is First Client for Paxos' New Dollar Gateway**
  - Paxos? What is Paxos?
  - Paxos Standard (PAX) is a US Dollar sable coin
- **12.11.2019: PeerTube has worked twice as hard to free your videos from YouTube !**
  - "Federation and instances to avoid creating a new tech giant"



Centralisation, CC-By SA LILA Fédération, CC-By SA LILA

  - Uses WebTorrent / WebRTC
  - uses the ActivityPub protocol, a W3C web standard for federation
    - A client to server protocol, or "Social API"
    - A server to server protocol, or "Federation Protocol"
- **31.10.2019: Ethereum is now unforkable, thanks to DeFi**
  - "Why there will never be another ETH Classic"
  - A thought experiment, with many ifs and whens
  - "If there can never be another ETC-like fork, then it seems that "governance-by-fork" will become a thing of the past. Welcome to the post-forkable era."

Upcoming lectures

Nr	Date	Topics	Who
10	20.11.2019	Bitcoin Advanced, Lightning	Christian Decker
11	27.11.2019	Monero	Sebastian Küng
12	04.12.2019	Crypto Mining	Tolino Nello
12	04.12.2019	NEO (technical)	Guilherme Sperb Machado

- **Upcoming 3 lectures are from various crypto projects**
  - Bitcoin, Monero, technical details of NEO
  - Tolino works at HSR and is a crypto miner

Quiz

URL:
b.socrative.com/student/

Room: HSR

b) (4P) Wieso fallen in der Regel Transaktionsgebühren für Transaktionen in einer Blockchain an?

d) (6P) Was passiert bei einer 51% Attacke? Erklären Sie das Problem mit einem Käufer und Verkäufer, der Waren mit einer Kryptowährung kauft.

Quiz

URL:
b.socrative.com/student/

Room: HSR

b) (2P) Was ist der Unterschied zwischen direkter Replikation und indirekter Replikation

c) (2P) Wozu wird eine Bootstrap Peer/Node verwendet?

d) (4P) Was für Probleme sehen sie, wenn sie eine DHT in ihrer Applikation implementieren und es auf einem mobilen Gerät laufen lassen?

CAP Theorem

- **CAP theorem: Only 2 of 3**
  - **Consistency**: Every read receives the most recent write or an error
  - **Availability**: Every request receives a (non-error) response, without the guarantee that it contains the most recent write
  - **Partition** tolerance: The system continues to operate despite an arbitrary number of messages being dropped (or delayed) by the network between nodes

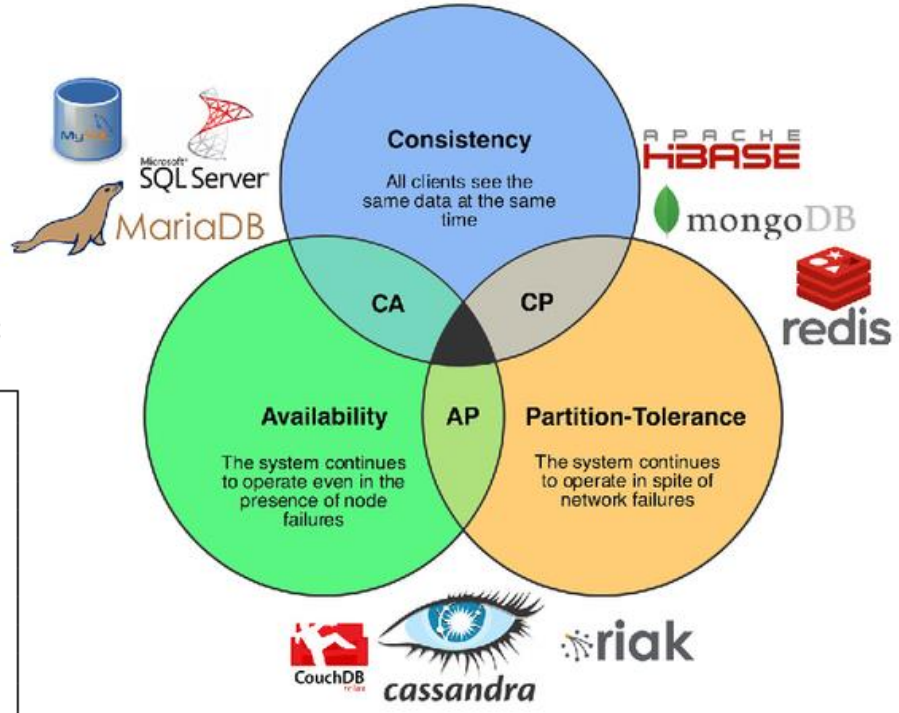
- **Difficult to categorize: depensds on the configuration**
  - “in case of a network partition (a rare occurrence) one needs to choose between availability and consistency.” (source)

g) (3P) Wofür steht beim CAP Theorem von Brewer, das C, A, und P. Erklären sie die Begriffe mit maximal je einem Satz.

C:

A:

P:



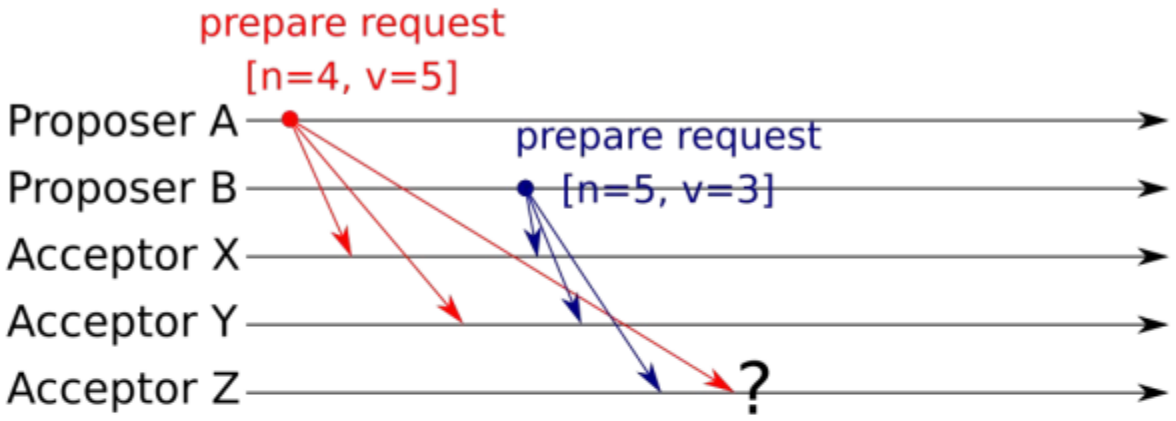
https://www.quora.com/What-Is-CAP-Theorem-1

Quiz

URL:
b.socrative.com/student/

Room: HSR

e) (3P) In der folgenden Grafik schicken beide A und B einen “prepare request”. Was macht Acceptor Z zum Zeitpunkt, welcher mit “?” markiert ist? Schickt er [n=4, v=5], [n=5,v=3], [n=4, v=3] oder gar nichts?

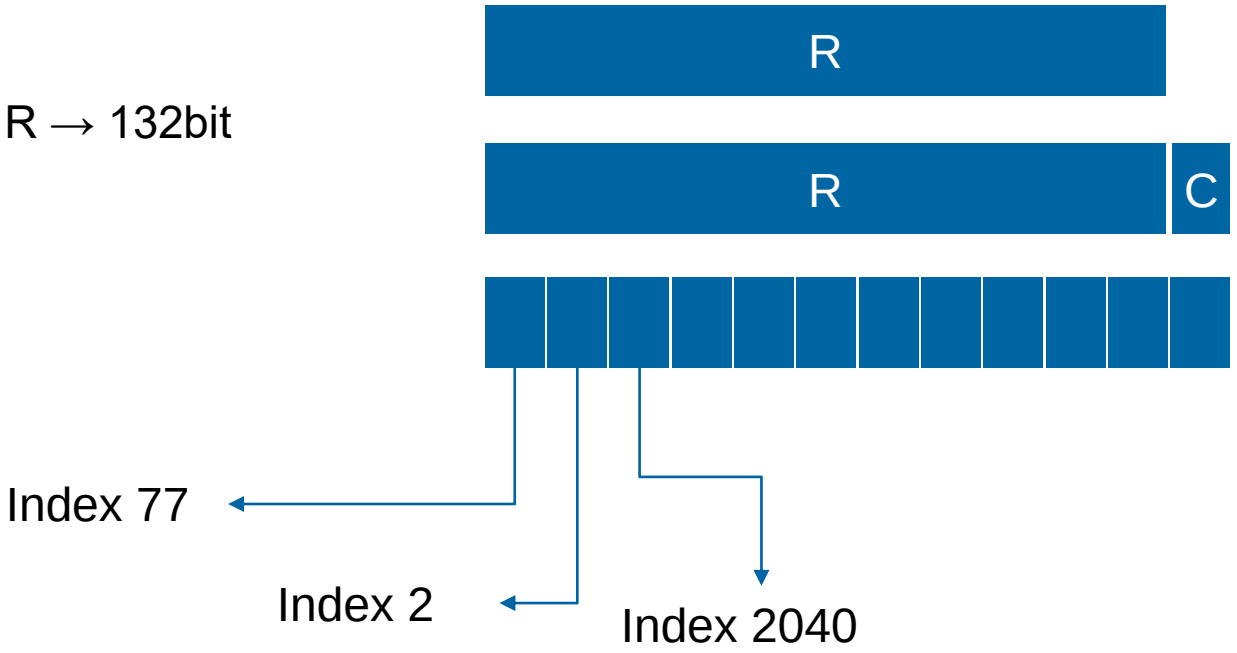


Lösung:

f) (3P) Warum ist in Raft der Heartbeat für die Leader Election wichtig?

BIP39

- **BIP39 mnemonic code words represent a number**
  - Human readable, e.g. for your challenge task
  - Mnemonic code words are a sequence of 12 to 24 words; e.g. “army van defense carry jealous true garbage claim echo media make crunch”
  - Wordlist 2048 words for various languages
- **Encoding R 128bit**
  - SHA256 (R), take first 4 bits attach it to R → 132bit
  - 2048 are represented in 11 bits
  - 132/11 = 12 → we will have 12 words
  - 77: another
  - 2: ability
  - 2040: year
  - …



URL:
b.socrative.com/student/

Room: HSR

Aufgabe 4: Praktische Aufgaben (26 Punkte)

Sie entwickeln eine verteilte Chat Applikation mit Anbindung an eine Blockchain. Um den Seed möglichst einfach dem Benutzer zugänglich zu machen speichern Sie den Seed mit einer vordefinierten List von Wörtern ab. Die 4-bit Liste besteht aus den folgenden Wörtern:

0 Apple	1 Kiwi	2 Mango	3 Banana
4 Cherry	5 Peach	6 Melon	7 Lime
8 Grape	9 Pear	10 Pineapple	11 Avocado
12 Coconut	13 Blueberry	14 Orange	15 Pear

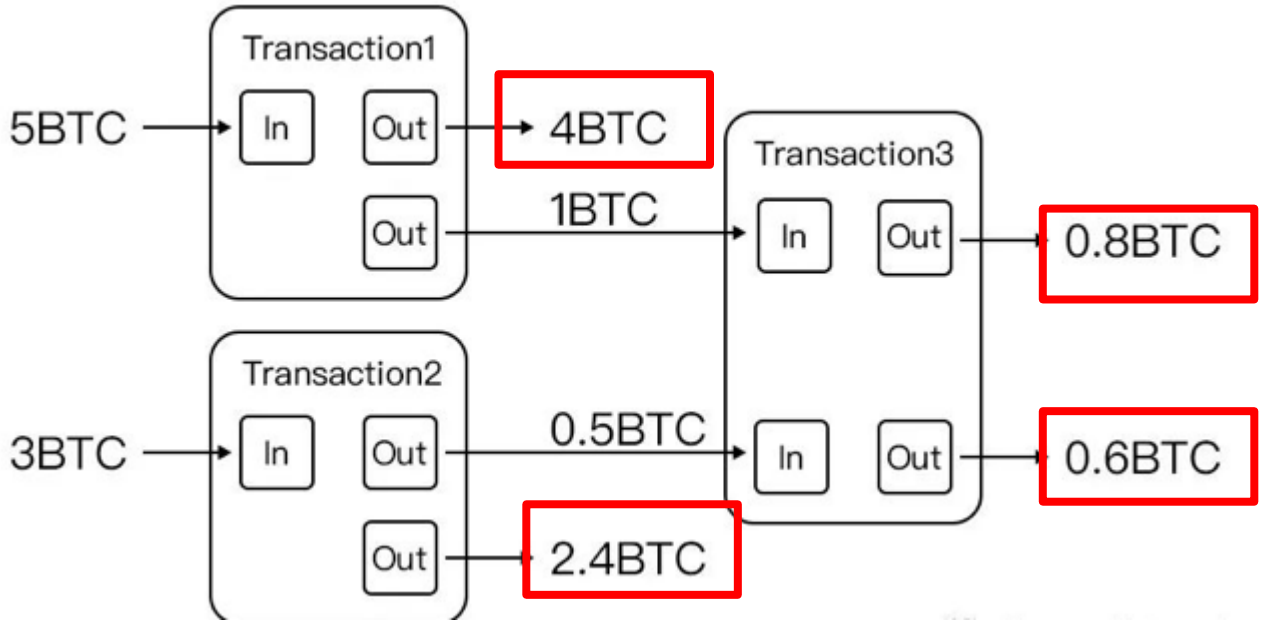
a) (2P) Welche Wörter soll der Benutzer aufschreiben, wenn der Seed 0x1a09 ist?

b) (2P) Um sicher zu gehen, dass alle Zahlen stimmen, wird eine Checksum hinzugefügt. Die Checksum addiert alle 4-bit Zahlen mit einem einfachen Overflow (Modulo 16). Der Overflow dient dazu, dass die Checksum nie grösser als 15 wird. Welches Wort wird als Checksumme verwendet?

UTXO

- **Wallet: collection of UTXO → your balance**
- **UTXO model is stateless**
- **Input of transactions is always linked to output, except “coinbase” which has no input (mining)**

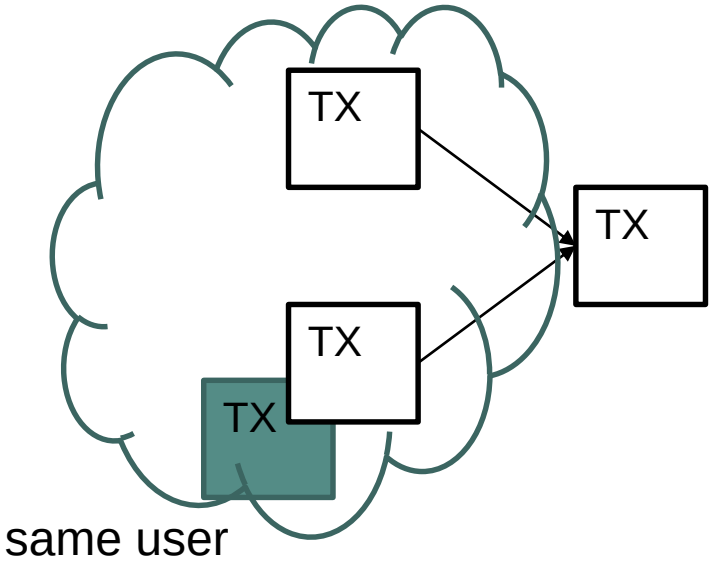
- **Is Bitcoin Anonymous?**
  - “Bitcoin is not entirely anonymous.”



https://developpaper.com/deep-dissection-of-bitcoin-and-ethernet-and-comparison-of-utxo-and-acount-models/

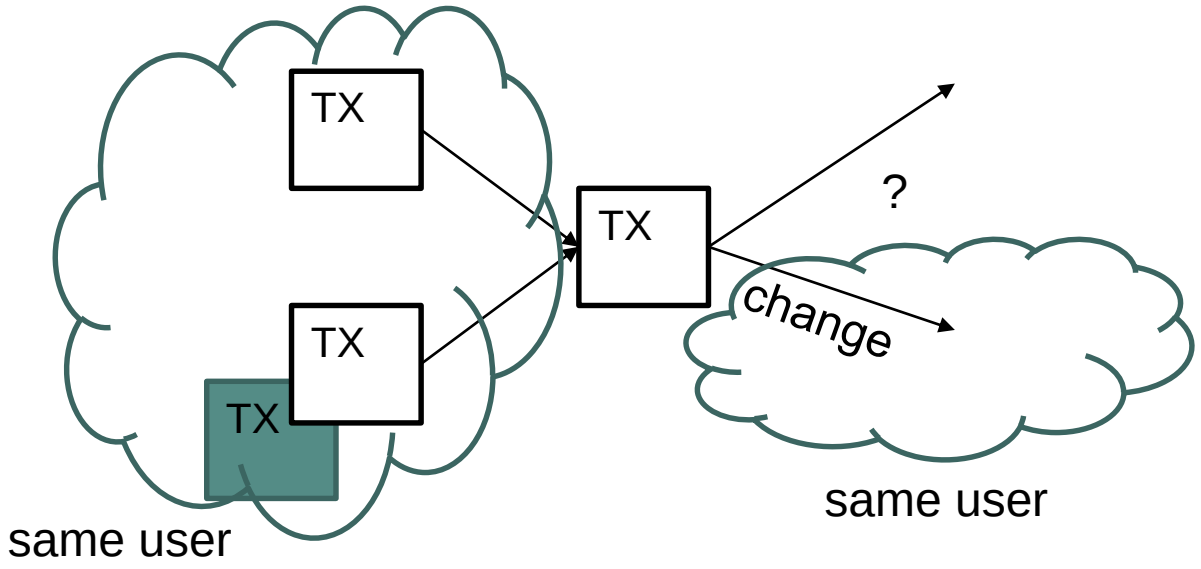
Anonymity

- **BitcoinJ: Committed bloom filters for improved wallet performance and SPV security**
- **HEURISTIC 1**
  - If two (or more) addresses are inputs to the same transaction, they are controlled by the same user; i.e., for any transaction t, all pk ∈ inputs(t) are controlled by the same user.



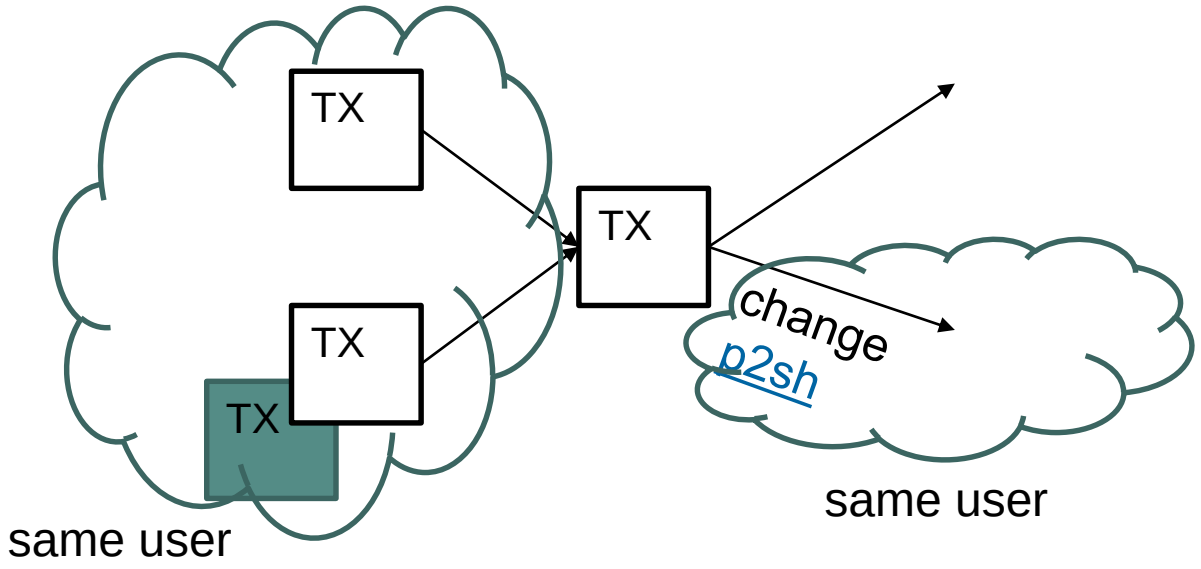
Anonymity

- **HEURISTIC 2.**
  - The one-time change address is controlled by the same user as the input addresses; i.e., for any transaction t, the controller of inputs(t) also controls the one-time change address pk ∈ outputs(t) (if such an address exists).



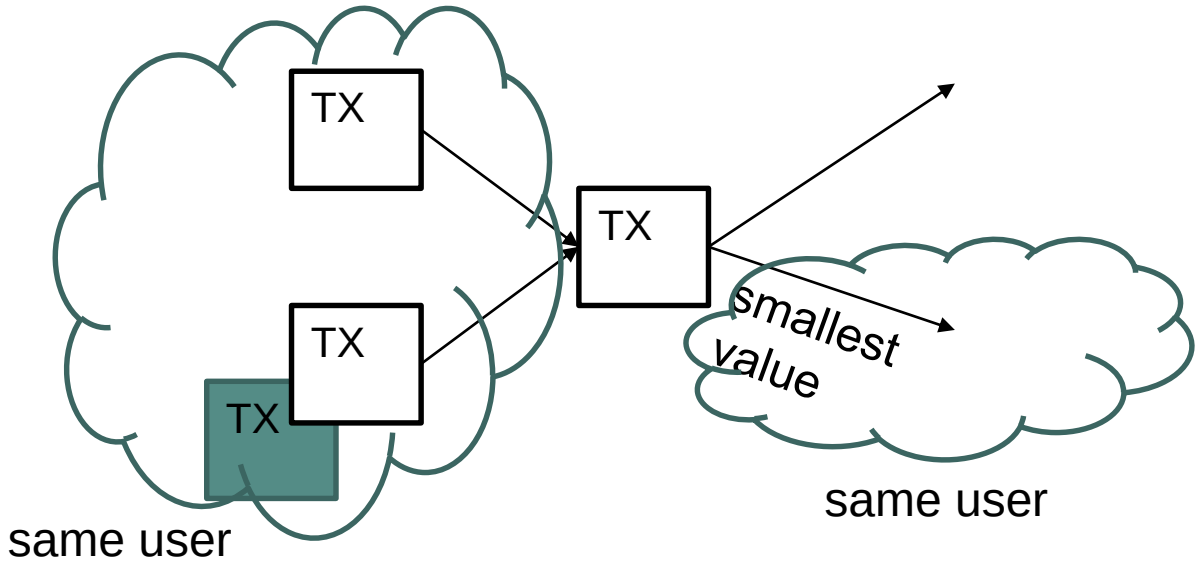
Anonymity

- **HEURISTIC 3**
  - Multisig wallets usually use p2sh change, but the recipient rarely uses p2sh, which allows to determine the correct change output with high probability.



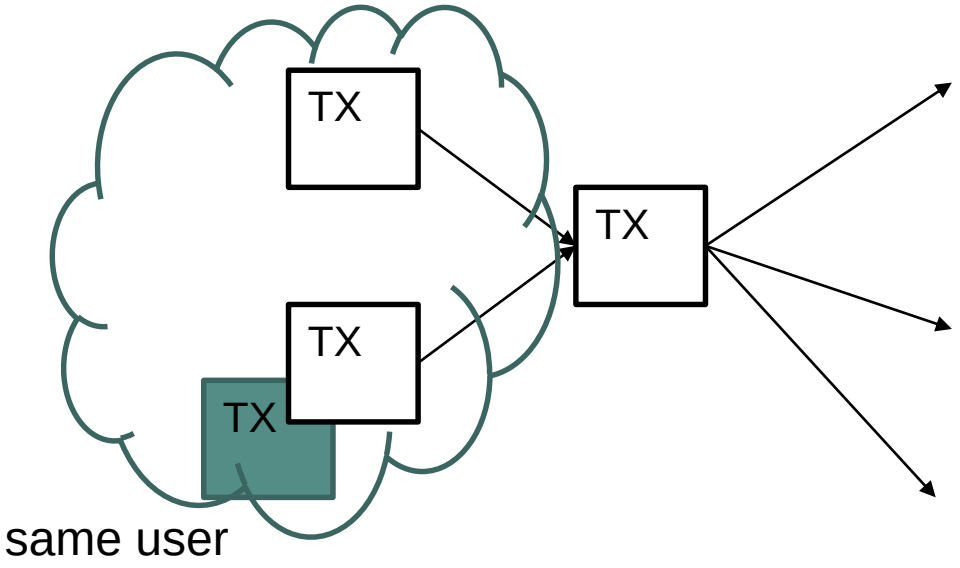
Anonymity

- **OPTIMAL CHANGE HEURISTIC**
  - The assumption is that wallet software does not spend outputs unnecessarily. Therefore the change value is smaller than any of the spent outputs. Because if the change was larger than one output then this output would be left out and the change would be reduced by the output's value.



Anonymity

- **CONSUMER HEURISTIC**
  - Consumer wallets only create transactions with two outputs. Therefore, if an output is spent by a transaction with 3 outputs it is not change.
  - WalletExplorer / Chainalysis



Quiz

URL:
b.socrative.com/student/

Room: HSR

Aufgabe 3: UTXO (15 Punkte)

Die folgende Tabelle zeigt Transaktionen in einem Block. Der Input einer Transaktion (TX) ist ein Pointer zu einer vorherigen Transaktion mit einem Index (z.B. der erste index wird mit id:0 bezeichnet) zum Output. Es fallen keine Mininggebühren an. (Hinweis: es müssen nicht alle Inputs und Outputs verwendet werden).

TX	Input	Output	Betrag (Coins)
4	1, id:0 / 1, id:1	G, H	1, 1
5	2, id:0	I	2
6	3, id:0	J, E	3, 1
7	4, id:1	K, P	4, 9
8	Coinbase	F	5

a) (4P) Alice besitzt die Schlüssel zu den folgenden Adressen F und H. Bob besitzt den Schlüssel zur Adresse M. Erstellen Sie eine Transaktion in welcher Alice 6 Coins an Bob schickt.

TX	Input	Output	Betrag (Coins)
9			

b) (4P) Transaktion 9 ist bestätigt. Bob besitzt den Schlüssel zur Adresse P. Konsolidieren sie Bobs UTXOs zum Output X (zu dem Bob ebenfalls den Schlüssel besitzt):

TX	Input	Output	Betrag (Coins)
10			

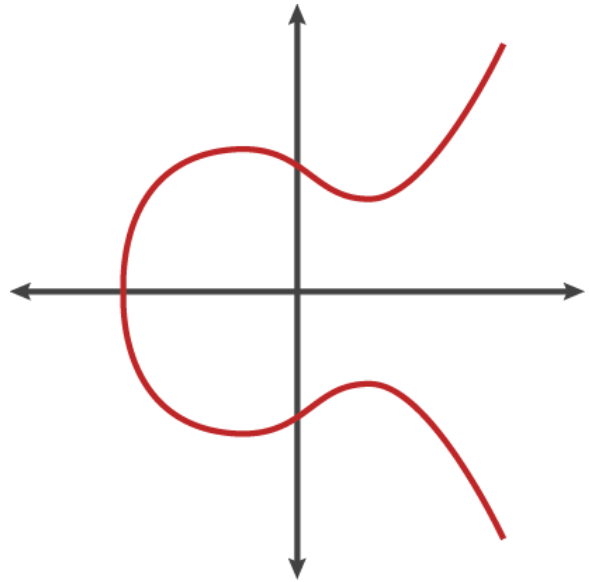
c) (4P) Transaktion 11 ist bestätigt und Charlie besitzt den Schlüssel zur Adresse N. Erstellen Sie eine Transaktion in der Bob 1 Coin an Charlie schickt:

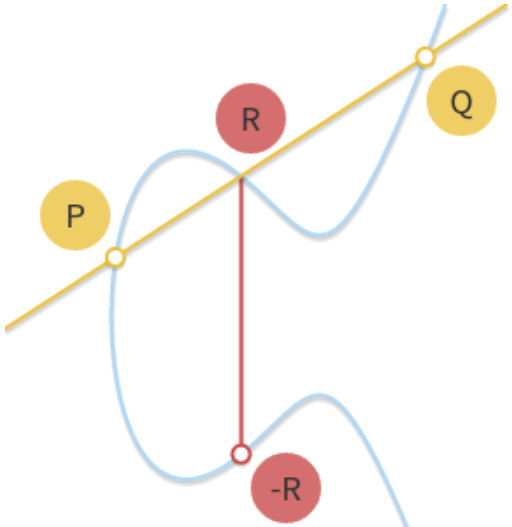
TX	Input	Output	Betrag (Coins)
11			

d) (3P) Um was für eine Wallet könnte es sich handeln, wenn eine Transaktion in einer UTXO Blockchain mehr als 3 Outputs hat?

Elliptic Curve Cryptography

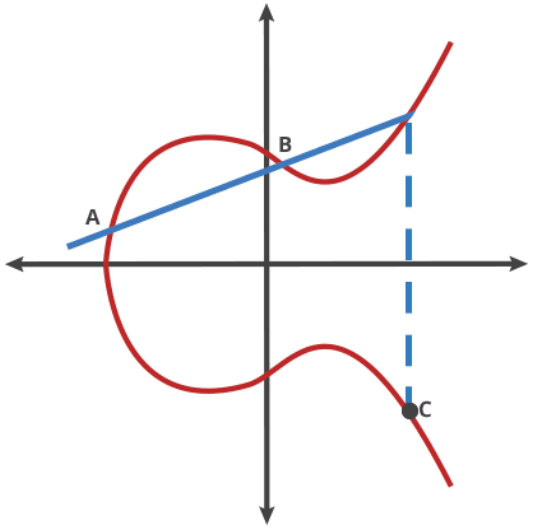
- **Elliptic Curve Cryptography from a practical point of view**
- **Set of points described by the equation:**
  - $y^2=x^3+ax+b$
  - No singular curves: $4a^3+27b^2\neq 0$
- **If a line intersects two points in the curve and not tangent it will always intersect a third**
- **Three aligned, non-zero points P, Q and R, their sum is: P+Q+R=0**
  - P+Q=-R
  - Interactive
- **P+P, tangent through P**
  - multiplication: nP = P+P+P+P+P

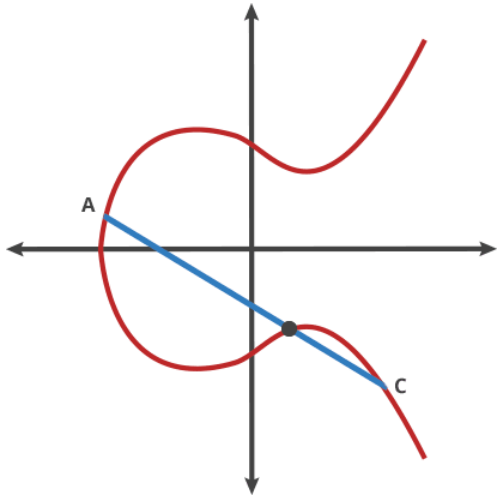


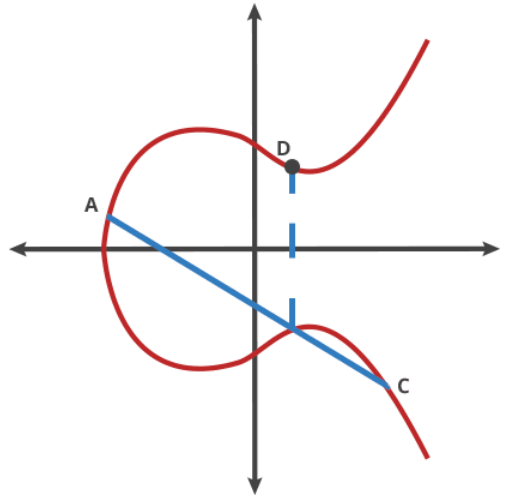


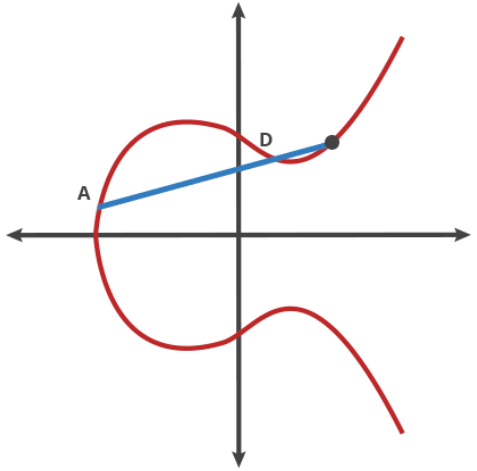
Elliptic Curve Cryptography: Multiplication

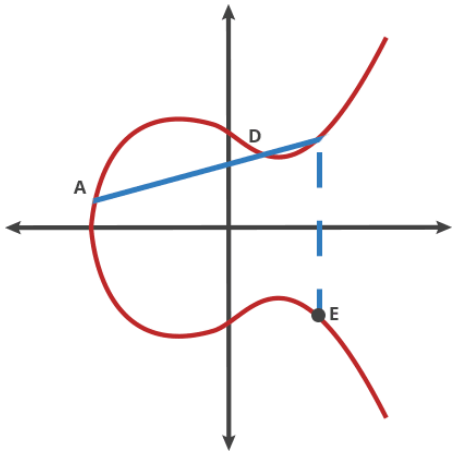
- **A + A = B**
- **A + B = C**
- **A + C = D**
- **A + D = E**
- **Point A added n times = final point. E=4A**
  - Knowing A and the final point, finding n is very hard (finite fields)
  - Trapdoor function, following the dotted lines easy, reverting it very hard







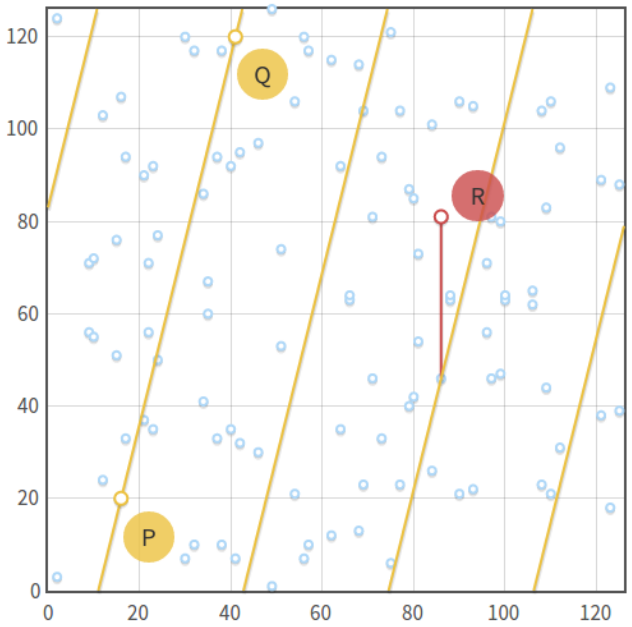




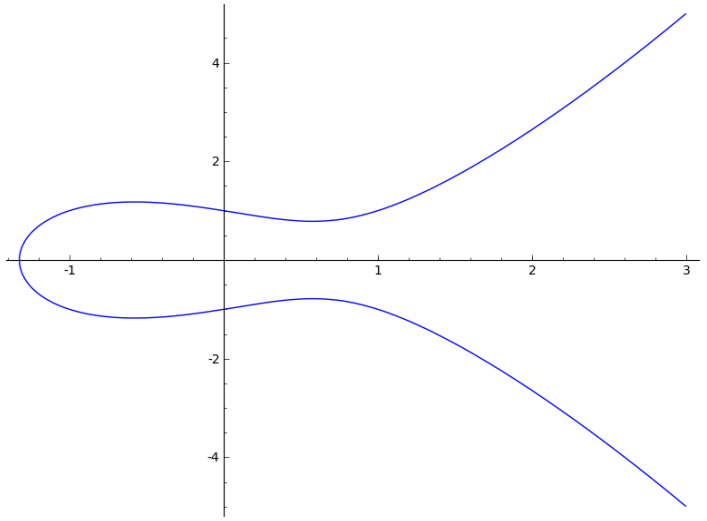
source

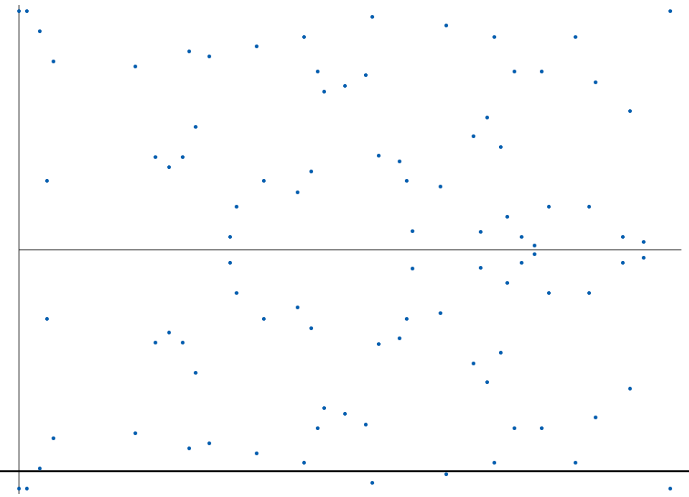
Elliptic Curve Cryptography

- **From real numbers**
  - $y^2 = x^3 - x + 1$
- **To finite fields (fixed range)**
  - $y^2 = x^3 - x + 1 \pmod{97}$
- **Same rules apply!**
- **ECC: nA = E (finding n is hard)**
- **Discrete logarithm problem**
- **$a=b^k \bmod n$**
  - $9 = 3^k \bmod 13$ (k=5, finding is hard)



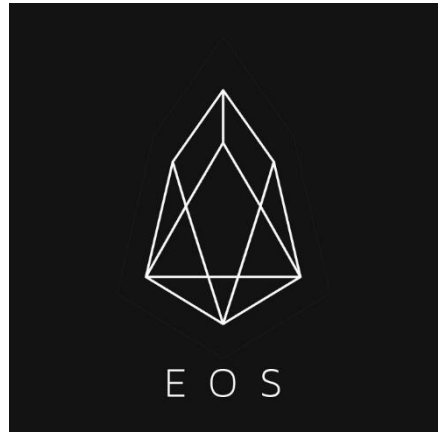
source





Elliptic Curve Cryptography: Cryptocurrencies

- **Bitcoin ECC**
  - $y^2=x^3+ax+b$
  - $a=0$
  - $b=7 \rightarrow \mathbf{y^2=x^3+7}$
  - Modulo p = $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
  - Base point G = x=55066263022773436695787188951685343262506034537775941755001873603891167292 40, y=32670510020758816978083085130507043184471273380659243275938904335757337482424
  - Also used in: Bitcoin, Ethereum, EOS, Litecoin, Dash, Zcash



ECC Key Exchange + Signature

- **Choose base curve, set base point G**
- **Private key: random number d, public key H result of dG = H**
  - Recovering p knowing only the point H and G in dG = H is very hard
- **ECDH, Alice, Bob, same G, same curve**
  - Alice: $H_A=d_AG$
  - Bob: $H_B=d_BG$
  - Alice, Bob exchanges H_A ,H_B
  - Alice: $S = d_AH_B$, Bob: $S = d_BH_A$
  - Alice: $d_A(d_BG)$, Bob: $d_B(d_AG)$ = shared secret
    - Commutative property
- **Static vs. ephemeral ECDH(E)**
  - Reuse or use key pair only once
- **Key Takeaways**
  - Elliptic curve: Point = Multiplier * Public Base Point
  - Given the point, it's impossible to get the multiplier

Questions?

Dr. Thomas Bocek thomas.bocek@hsr.ch