OST
Eastern Switzerland
University of Applied Sciences

Distributed Systems Advanced & Blockchain

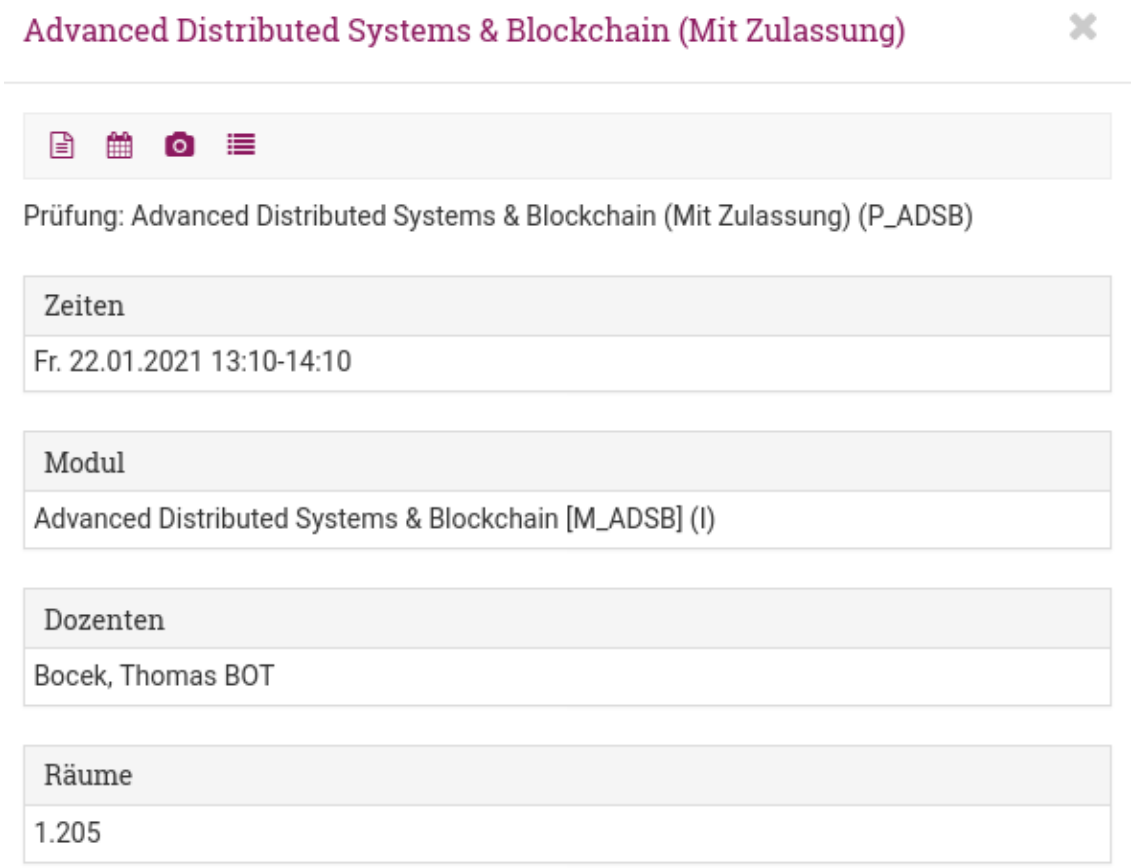
Exam Preparation

Thomas Bocek

21 November 2020

Exam DSA – HS19

- DSA exam time 120m
  - 90 points, 1 point ~ 1minute
- ADSB exam time 60m
  - 22.01.2021 13:10 – 14:10
  - Come earlier
  - 45 points, 1 point ~ 1minute
  - 1.205 ~ lets see…



OST

Hinweise

- Hinweise allgemein
  - Zeit: 60 min.
  - Zuerst diese Hinweise, dann die Prüfungsteile ganz durchlesen.
  - Diese Prüfung ist "Closed Book".
  - Taschenrechner ist nicht erlaubt.
  - Sonst sind keine Hilfsmittel zugelassen; auch kein Handy oder Smart Watch.
  - Alle Antworten und Lösungen in diese Aufgabenblätter schreiben.
  - Keinen Bleistift und keine rote Farbe verwenden.
  - Die Antworten und Lösungen müssen nachvollziehbar sein. Bitte alles in leserlicher Schrift!
  - Keine Fragen während der Prüfung. Bei Unklarheiten sind sinnvolle Annahmen zu treffen und diese klar zu dokumentieren.
  - Die Bewertungspunkte der Aufgaben können nach der Korrektur noch etwas variieren.
- Hinweise zum Prüfungsbeginn
  - Versehen Sie das Titelblatt mit Ihrem Namen.
  - Den OST-Badge sichtbar auf den Tisch legen.
  - Allfällig bereitliegende Prüfung nicht umdrehen oder umblättern, bis die Aufsichtsperson explizit das OK dazu gegeben hat.
- Hinweise zur Prüfungsabgabe
  - Kontrollieren Sie nochmals, ob die Prüfung mit Ihrem Namen versehen ist. Geben Sie alle Blätter – auch von nicht gelösten Aufgaben – geordnet und geheftet ab.
  - Nach Prüfungsende: Drehen Sie Ihre Prüfung um und warten Sie, bis die Prüfung eingesammelt wird. Bleiben Sie dann sitzen bis die/eine Aufsichtsperson die Prüfungen gezählt hat und ein Zeichen zum Verlassen des Raums gegeben hat.

Aufgabe 1: Blockchain Basics (17 Punkte)

	Statement	True	False
1	Transaktionsdaten in Neo werden so verschlüsselt, dass nicht jeder die Transaktionen mitlesen kann.		
2	Transaktionsdaten in Ethereum werden nicht verschlüsselt, und jeder kann die Transaktionen mitlesen.		
3	Öffentliche Blockchains eignen sich gut um grosse Datenmengen zu speichern.		
4	Krypto-Mining kann mit jedem Rechner profitabel betrieben werden.		
5	Die Kostenfaktoren bei Krypto-Mining sind Anschaffungs- und Stromkosten.		

1. F / Neo (we showed Tezos this year): no encryption – tx, neo exercise
2. T / Ethereum: in HS19 we looked at the protocol: java solidity wrapper alternative, create tx
3. F / ETH yellow paper, 20'000 gas for 32bytes, 45gwei / gas -> 1KB ~15USD
4. F / Talk with Nello -> No, rarely profitable, HW needs to have a high H/kWh ratio, CPU cannot compete
5. T / Talk with Nello -> main factors, however one could argue fees

- Aussage: Ethereum ist eine Blockchain welche «immutability» garantiert. Argumentieren Sie warum diese Aussage nicht stimmt.
  - DAO incident: chain fork ethereum classic
  - Smart contract can allow modifications
- Wie kann man sich gegen einen Fork bei einer Protokolländerung schützen? Beschreiben Sie einen möglichen Mechanismus.
  - Ice Age
  - Tezos: protocol upgrade via voting

Aufgabe 2: Distributed Systems (24 Punkte)

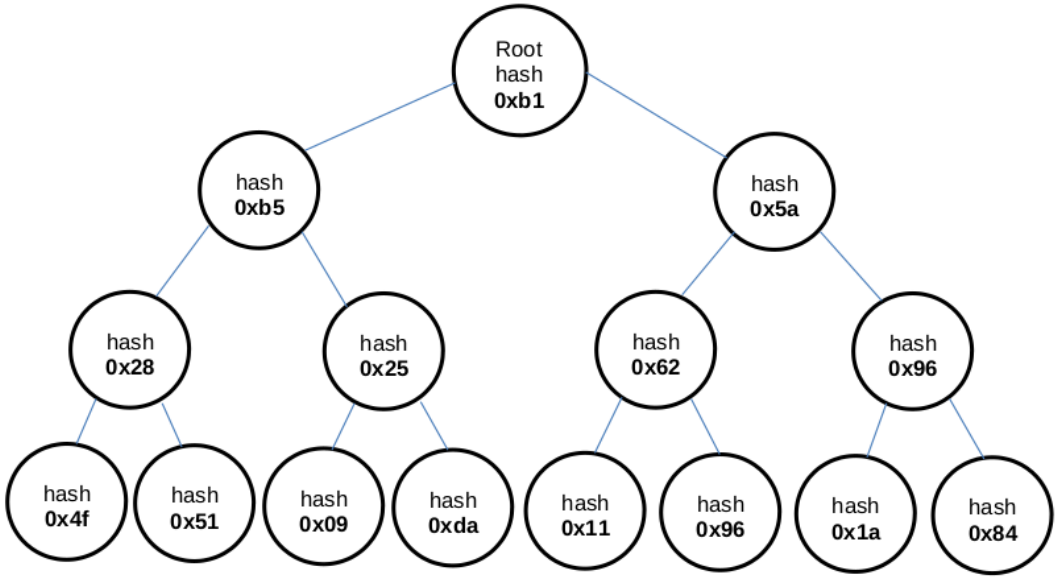
	Statement	True	False
1	In verteilten Systemen gibt es keine exakte globale Zeit.		
2	Mit WebRTC können Browser untereinander kommunizieren.		
3	In Paxos können 2 Phasen unterschieden werden: die «prepare/promise» und die «accept» Phase.		
4	Bei Raft startet die Leader Election nachdem ein Leader nicht mehr erreichbar ist.		
5	Bei einem byzantinische Fehler verhält sich ein System beliebig falsch.		

1. T / recent incident: OAuth token was issues by a server that was running 5 sec in the future. Token verification → invalid as token also the creation time was set
2. T / WebRTC lecture
3. T / No Paxos in HS20
4. T / No Raft in HS20
5. T / Blockchain need to deal with that, centralized system not necessarily

- Was ist das grundsätzliche Problem mit Replikas in einem verteilen System?
  - Updates, accessing old replicas
- In P2P Systemen braucht es einen Bootstrap Peer/Node, um dem System beizutreten. Was braucht es bei WebRTC?
  - WebRTC lecture, slide 14-16: signaling server
- Was für Probleme sehen sie, wenn Sie eine Applikation mit Raft implementieren und es auf einem mobilen Gerät laufen lassen?
  - Network is down, leader change, lots of changes
  - Always on, battery drain

Aufgabe 2: Distributed Systems (24 Punkte)

e) (5P) In dem folgenden Merkle tree befinden sich Hashes von 8 Dateien zum Zeitpunkt **t** in den leaf nodes. Sie besitzen bereits 7 Dateien und laden 1 Datei mit Hash **0xda** herunter. Was sind die minimalen Informationen um sicherzustellen, dass Sie alle Dateien mit dem richtigen Inhalt zum Zeitpunkt **t** haben.



- Solution: 0x09,0x28,0x5a

- Was sind Vor- und Nachteile von einer WebRTC Applikation, wie zum Beispiel WebTorrent gegenüber einer Applikation welche TCP/UDP direkt benutzt, wie zum Beispiel BitTorrent? Nennen Sie je 2 Vor- und 2 Nachteile.

  + Works with installing a plugin, just use the browser, always newest app release

  + Encrypted by default

  - Performance can be worse, browsers bloated?

  - Compatibility issues among browsers

Aufgabe 3: UTXO (16 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 idx:0 bezeichnet) zum Output. Es fallen keine Mining-Gebühren an. (Hinweis: es müssen nicht alle Inputs und Outputs verwendet werden).

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

a) (4P) Alice besitzt die Schlüssel zu den folgenden Adressen F und E. Bob besitzt den Schlüssel zur Adresse M. Erstellen Sie eine Transaktion in welcher Alice 7 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 10 ist bestätigt und Charlie besitzt den Schlüssel zur Adresse N. Erstellen Sie eine Transaktion in der Bob 1 Coins an Charlie schickt:

TX	Input	Output	Betrag (Coins)
11			

- a) 8, idx:0 / 6, idx: 1 – M – 7
- b) 9, idx:0 / 7, idx: 1 – X – 15
- c) 10, idx:0 – N, P – 14, 1

- Eine Transaktion von Dave beinhaltet 2 Outputs mit den Beträgen 1 und 0.2566221. Bei welchem von diesen Outputs handelt es sich um eine mögliche Bezahlung und bei welcher um einen Output an die Wallet von Dave. Argumentieren Sie warum Sie sich so entschieden haben.
  - 2 outputs, could be private wallet
  - More than 2 outpus, can be exchange
  - Pro: chances are higher that the price 1 and the exchange is 0.25.., e.g., 1 BTC
  - Contra: if price is in CHF, it is unlikely that it will be exactly 1, so it must be 0.25..

Aufgabe 4: Praktische Aufgaben (21 Punkte)

- In Ihrer dezentralen Game Applikation müssen Sie sich zwischen einer Blockchain (z.B. Ethereum) und WebRTC für die Kommunikation entscheiden. Nennen Sie je 1 Vor- und Nachteil von Blockchain und WebRTC für die Kommunikation.

  - Ethereum: delays, needs a plugin

  + Ethereum: fully decentralized

  - WebRTC: needs a server

  + Works without plugin, faster

- Sie wollen Ihren Smart Contract zuverlässig, schnell und automatisiert testen. Was müssen Sie beachten?
  - Use, regtest, or testchain (parity -dev), that creates a block for every TX, don’t use rinkeby etc…

- Sie verwenden für Ihre Applikation eine DHT. In einer DHT kann man entweder direkt oder indirekt replizieren. Welchen Replikationsmechanismus wählen Sie für den Online/Offline Status Ihrer Game Applikation und warum?
  - Direct, drawback is that if you are offline, data is lost, but no data can mean offline

- Für Ihre Applikation haben Sie die Wahl zwischen NEO, Ethereum oder Monero. Nennen Sie je 3 Eigenschaften pro Blockchain. Welche werden Sie in Ihrer Applikation verwenden und warum?
  - Privacy, pBFT, smart contracts, costs, popularity, …

Aufgabe 5: Solidity/Ethereum (12 Punkte)

Dieser Smart Contract hält in der Variable ***balances*** fest, welche Adresse wie viele Ethers hat. Die Funktion ***transfer()*** überweist Ethers von diesem Contract auf eine Empfängeraddresse.

```
pragma solidity ^0.4.25;

contract Exam {
    mapping (address => uint256) private balances;
    event Message(string msg);
    ...
    function transfer(address recipient, uint256 value) public {
        require(balances[msg.sender] - value >= 0);
        require(recipient.call.value(value)());
        balances[msg.sender] = balances[msg.sender] - value;
    }

    function payin() public {
        ...
        emit Message("done");
    }
}
```

- Nennen Sie mindestens zwei Probleme in der Funktion transfer()
  - Reentrancy attack [slide10]
  - First require always true, as ist uint [slide11]
    - Balances[] can increase

- In der Funktion payin() wird ein Event erzeugt. Wozu können diese Events verwendet werden? Können andere Smart Contracts direkt auf diese Events reagieren?
  - No, contracts cannot directly react on events. In order to use them one has to have a running server, listening on that event, and issue a transcation
  - As an example, a new transaction could be triggered if an event from a transfer had a higher value that a certain limit

Other Interesting Topics (not a complete list!)

- ERC20, but read-only
- Ethereum Random
- Bloom filter
- Payment channels
- Virtualization
- …