Exercise 2

A. Blockchain

1. Name the three key properties of the Bitcoin Blockchain according to the lecture and explain them.

Solution:

- The Blockchain is trust-free. This means that we do not need to trust a third party which maintains the platform. The decentralized network ensures the validity of the contents of the Blockchain.
- The Blockchain is tamper-proof. No entity can single-handedly manipulate the data after it is stored in the Blockchain.
- The Blockchain is transparent. All contents of the Blockchain can be seen by any node of the network.

2. Decide if changing the following contents of the block alters the hash of the block header.
   - Transaction ordering (Tx stay the same)
   - Transaction add/removal
   - Difficulty
   - Previous blocks
   - Nonce

Solution:

- Transaction ordering (Tx stay the same) Yes
- Transaction add/removal Yes
- Difficulty Yes, but you cannot change it (defined by the network)
- Previous blocks Yes, but you should not change it (results in invalid blocks)
- Nonce Yes

3. Explain how chaining is implemented in a Blockchain.

Solution:
Blocks are chained through adding the hash of the previous block (n-1) to the current block (n).

B. Genesis Block

4. Discuss reasons, why Satoshi Nakamoto might have included a message or a newspaper article in the genesis block? In which field did he store the information?

Solution:

There are different reasons possible, we only can speculate:

- He wanted some proof that he created the Blockchain not before that date.
- He wanted to criticize the behavior of saving banks, therefore creating a new decentralized currency.

Satoshi stored the data in the ScriptSig of the first transaction which was the coinbase transaction and therefore needs no previous Output.

5. 10 years after the first Bitcoin Block the first page of The Times looks like following[1]:

BRITAIN'S MOST TRUSTED NATIONAL NEWSPAPER

THE TIMES

Thursday January 3 2019 | thetimes.co.uk | No 72734 £1.60 Subscribers save 50p

Romps, royals and lesbians

Costume drama tipped for Oscars glory INSIDE TIMES2

Would you drink wine from a can? Trends of 2019

Universities face credit crunch as debt spirals

Borrowing tops £10bn in race to attract students

Rosemary Bennett Education Editor
Nicola Woolcock, Ryan Watts

Universities have been warned that they are on the brink of a "credit crunch" after embarking on a record borrowing spree despite deep uncertainty over their financial future.

The sector's debts have risen over the past year to £103billion, three times more than before the financial crash, figures compiled by *The Times* show.

Five universities, including Southampton, UCL and Imperial College London, have more than doubled their borrowing in the past year to compete in the ever-tougher battle to attract more students from home and abroad.

The move comes amid what experts describe as "unprecedented uncertainty" for higher education, with ministers said to be considering a cut in tuition fees — now the main source of university income — and predictions that Brexit could result in a fall in student numbers.

Nick Hillman, director of the Higher Education Policy Institute, said there was now a consensus that "too many institutions are borrowing too much".

He added: "There are unprecedented levels of uncertainty with Brexit, the tuition fees review and the spending round. These factors are material for those who lend large sums to universities. Oxford, Cambridge and some universities will always be fine, but others will face a credit crunch in 2019."

Sir Michael Barber, head of the Office for Students watchdog, accused universities of behaving like overconfident banks before the financial crisis, thinking that they were "too big to fail". He said that there would be no bailouts with public cash if universities could not service their debts.

Imperial College London has the greatest debt pile at £470 million, having borrowed to fund a vast expansion in White City and Kensington, among other projects. UCL has begun its largest capital programme, with £1.2billion to be spent on refurbishment of its Bloomsbury buildings and a new 11-acre campus on the 2012 Olympic site in east London, to combine science and arts teaching.

Southampton has also borrowed to install new hardware and software laboratories in the school of engineering and computer science and to build new life sciences labs, an innovation campus for geomechanics and infrastructure engineering and a £36 million hall of residence.

Newer universities are also spending heavily on facilities. Northampton has taken on debts of £200 million to fund a £330 million town centre campus.

Many universities make use of the international capital markets, issuing 40-year or 60-year bonds in the same

Continued on page 8, col 1

Silver streak Dave Ryding became Britain's most successful skier with a second place in the parallel slalom at the world championships. Northern grit, page 5

Police failed women sent to Somalia for 'marriage'

Paul Morgan-Bentley
Head of Investigations

Police failed to investigate the families of the young British women sent to a school in Somalia where they were beaten and prepared for forced marriages, *The Times* can reveal.

Seven victims, aged between 17 and 22, were rescued last year from a "correctional religious school". They were chained to walls and whipped for forgetting verses of the Koran.

After being flown back to Britain, the young women were all interviewed by police. However, despite it being illegal to force someone to marry, or to use deception to take someone abroad for a forced marriage, officers decided that none of the allegations required the arrest of any family members.

One of the victims said yesterday that she felt she had been abandoned by officers, who have called her once since she returned to Britain. They also failed to question her father, who she believes oversaw her imprisonment in Somalia.

Ministers are under pressure over their handling of forced marriage cases after a Times investigation revealed yesterday that victims who are rescued abroad are made to repay the Foreign Office for their flights home, basic food and shelter.

It has now emerged that:

- Boris Johnson knew officials were charging forced marriage victims repatriation fees when he was foreign secretary but failed to stop them.
- Jeremy Hunt, now foreign secretary,

Continued on page 4, col 3

Buying The Times: Austria €1.10, Belgium €1.10, Cyprus €1.10, North Cyprus TL15, Denmark DKK23, France €1.10, Gibraltar £2.70, Greece €1.10, Italy €1.10, Luxembourg €1.10, Malta €1.10, Netherlands €1.10, Portugal €1.10, Spain €1.10, Switzerland CHF1.80, Turkey TL 21

BitMEX

Thanks, Satoshi. We owe you one.

Happy 10th birthday, Bitcoin.

00000000000000000037e741045a99121918e6ee717188fc77ec40b7419a829

You decide to start your own coin on the day the newspaper came out. You want to do the same as Satoshi Nakamoto and include a headline in your Genesis Block. Why is it a bad idea to include "Thanks Satoshi, we owe you one" in your Genesis Block?

[1]This exercise is inspired by a Tweet from Peter Todd: https://twitter.com/peterktodd/status/1080778448216428544

Solution:

The headline you intend to use is an advertisement. Therefore, it would be possible for you to know of this text ahead of time and actually create the first Block before that date.

C. Network

6. Name and briefly explain three roles in the Bitcoin network.

Solution:

Wallet Owner:

- The wallet owner owns different private keys to unspent transaction outputs (UTXOs)
- He is the owner of all stored currencies on these addresses
- He sends money by signing and publishing new transactions to a connected light node, full node or miner

Light Node:

- The light node can act as a relay for transactions of one wallet owner
- It validates whether a single transaction of the wallet owner was executed correctly
- The light node also requires a full node to connect to the network
- Almost no relevance in practice today. Today, centralized services are used to create transactions.

Full Node:

- The full node maintains the complete blockchain. Its record of the chain is complete, it contains every single transaction and block until the genesis block.
- Is connected to other full nodes and exchanges information. Namely:
- Validates every transaction and block it receives
- Relays all new transactions and blocks

Miner:

- The miner needs the same record as a full node in order to work properly. He also is connected with other nodes and maintains the network.
- Additionally, the miner is responsible for creating new blocks by trying to solve the mining puzzle.
- The miner gets rewarded by creating new blocks.

(Taken from the lecture notes)

7. Explain the function of the memory pool.

Solution:

The memory pool stores all transactions which are not contained in a block yet. Each full node maintains the list of these transactions and updates it when 1) a new block arrives and 2) new transactions arrive.

8. Alice wants to send 1.0 BTC to Bob. What steps does her transaction take until being completed?

Solution:

1. The transaction is created and signed by Alice.
2. The signed transaction is sent to a full node for validation.
3. If the transaction is valid, the full node publishes the transaction to the network and is added to the memory pool.
4. A miner includes Alice's transaction from the memory pool to its block. The miner solves the puzzle and publishes the block to the network.
5. Other nodes receive the mined block and validate all contents.

D. Storing Bitcoins

9. What is the difference between a hot storage and cold storage? Give an example for both types. Which type do exchange wallets fit in?

Solution:

A hot storage wallet is immediately available to use. An example is a wallet software on your PC connected to the internet. A cold storage is a method of storing private keys in an isolated environment. These wallets are not immediately available but provide higher security. An example is a printed paper wallet.
Exchange wallets resemble hot wallets, as (depending on limitations and security) funds are immediately available. However, transferring coins to an exchange wallet means handing the possession of your coins to the exchange. You no longer own the private key, but the exchange does. In many cases exchanges got hacked and users lost their funds.