ZHIHAN WANG
zw3u18@soton.ac.uk

# COMP6212 Assignment 3

May 1, 2019

### a)maximum number of bitcoins?

The maximum number of bitcoins is 21,000,000. Every block introduces 50 new coins in the system and this quantity halves every 210,000 blocks. Therefore, the maximum number of bitcoins can be calculated as a sum of geometric series.

$$Maximum = \sum_{n=0}^{\infty} \frac{210000 \times 50}{2^n} = 210000 \times 50 \times \frac{1}{1-\frac{1}{2}} = 21000000$$

### b)when will the last and 97% of bitcoin be mined?

1. Sometime in the year 2140.
2. At year 2025.217.

$$num = 97\% \times maximum = 0.97 \times 21000000 = 20370000, finding\ t, so\ that$$

$\sum_{n=0}^{t} \frac{210000 \times 50}{2^n} = num \to \sum_{n=0}^{t} \frac{1}{2^n} = 1.94 \to \frac{1-(\frac{1}{2})^{t+1}}{\frac{1}{2}} = 2-(\frac{1}{2})^t = 1.94 \to t = \log_2 100 - \log_2 6$

$\to Time = \frac{t \times 10 \times 210000}{365 \times 24 \times 60} = 4.058893 \times 3.99543378995 = 16.217038242$. As the first bitcoin was mined at 2009, 97% of bitcoin would be mined at around 2025.217.

### c)desired properties of a Hash Function?

There are three desired security properties. **1.**One-way: The Hash Function should be infeasible to invert. When given input, it's easy to compute output; however, given output, it is hard to invert the input. **2.** Collision-resistance: It is hard to find two inputs that hash to the same output. In other words, if the hash function H is collision-resistant, then for inputs *a* and *b*, if *a* is not equal to *b*, it is difficult to find an H, such that H(a)=H(b). **3.**Deterministic: Any small changes to the input will completely change the output.

### d)stale block? soft fork? hard fork?

1. A stale block is a block that is no longer a part of the current best block chain because it was overridden by a block in a longer chain.
2. Soft fork: A soft fork is a backward compatible method of upgrading a blockchain. It runs much stricter rules; therefore, blocks recognized by new version rules are compatible to the older ones, but only previously valid blocks are invalid under the new rules. It does not require all nodes to upgrade and agree on the new rules.
3. Hard fork: In contrast to the soft fork, a hard fork is a change to a protocol that renders older versions invalid, for example, increasing block size from 1MB to 4MB. Blocks

considered valid by miners running new versions will be rejected by nodes running the old version. Therefore, a hard fork requires all nodes to upgrade and agree on the new version. Otherwise, it potentially results in creating stale blocks and double-spending.

### e)double-spending? How to achieve consensus?

1. Double-spending is the risk that a digital currency can be spent twice. The holder could make a copy of the digital token and send it to an another merchant while retaining the original, or send to different merchants. This problem only occurs in digital currencies as the digital information is easily reproduced but physical currencies are not.

2. Generally, the bitcoin network achieve consensus by using a process named mining. Members of the network who choose to take part in the process of reaching a distributed consensus are called miners. Miners try to find the proof of work for blocks which are used to collect transaction. When the proof of work is found, validated and broadcasted, the new block containing transaction is received by the previous block.

   However, in this process, a 'forked' problem may occur. That is, more than one block are received by the previous block. At that time, the network needs some way to reach a consensus on which block to accept as the next block. As finding proof of work is computationally difficult, the more blocks have been added to the blockchain, the more secure it is. Therefore, a simple way in bitcoin network to achieve consensus is to **trust the longest chain of blocks**. When more than one "next block" are received, generally two, the previous block saves both and start to work forward. If one of the current two blocks receives a new next block, the shorter chain will be discarded and the work will keep going on in this longer chain.

### f)routine tasks? strategic considerations? 51% attack?

1. **1.**Verify the new blocks: If some miner solves a new block and broadcasts, other miners will listen to it and verify it. **2.**Check the transaction valid. **3.**Assemble prospective blocks: Firstly, select valid transactions from UTXO and hash them to build a new block in the current longest chain. Then find a nonce to make the block meet the current target of the network. Finally, wait for others to validate it.

2. **1.**which transactions to choose in the new block. **2.**which block to choose as a previous one and keeping mining on top of it. **3.**choose when to announce a new block. Besides, if someone has enough computational power, what they would do.

   The default strategy exists and most miners are following these. That is, to choose the transaction with the transaction fee above the minimum at random, to choose the longest chain and to announce a new found block immediately after it is found. However, it might be possible to make more money if miners change the default stragety.

3. 51% attack refers to an attack on a blockchain by a group of miners controlling more than 50% of the network's mining hash rate, or computing power. The attackers would be able to prevent new transactions from gaining confirmations. They would also be able to reverse completed transactions, which means they could double-spend coins.

### g)bottlenecks?

**1.**Scalability: In blockchain, the size of each block is only 1 MB, equivalent to 3000 Bitcoin transactions in average. At the same time, it takes miners 10 minutes to mine a block, which means in every second, only around 5 transactions could be written, in contrast to Paypal handling 193 and Visa 1667 transactions per second. Bitcoin still needs more upgrade to compete with these. **2.**Energy consumption: Miners collect Bitcoin rewards by mining blocks. However, mining blocks is equivalent to solve programming puzzles, which requires a large amount of computational power. Electricity is 90% of the cost to mine bitcoin. According to Digiconomist, the estimated power used for verifying cryptocurrency transactions is 30.14TWh a year as much electricity as being taken to power the entire nation of Ireland in one year.

### h)interconnection between block size, generation interval......?

With the block size increasing, the block could include more transactions, which means the difficulty of solving a programming puzzle rises as well. Therefore, the block generation interval, also known as the time period between previous block and current block, will increase if the size of block goes up. Assuming that all miners are nice and will not accept any double-spends that come after the original transaction, then a shorter block generation interval will make sure less double-spending as each transaction could be confirmed and included in a block at once. As a result, the number of stale blocks goes down.

If the block generation interval decreases, in the same time period, more blocks will be mined; therefore, the number of forks will increase and the length of forks will be longer. Increasing number of forks forces the block propagation time rise as well because a new block needed to be seen by more nodes.

### i)pros and cons of mining pool? three possible payments? strategic behavior?

1. -Advantages: **1.**For miners: Miners participating in large mining pools share processing power to solve puzzles and also split the block reward. This process helps to minimise the variance of individual income and lower the risk. **2.**For ecosystem: The mining pool makes computational power concentrated and as a result, prospective blocks are intensively assembled. This facilitates network update. **3.**Easy setup: Individuals do not need to consider too more and less setup is required. **4.**Less space: Individuals do not need to keep a copy of the block anymore. The pool will address this issue.

-Disadvantages: **1.**Possible attacks: The mining pool makes the power concentrated. This might cause the double spending issue and possible attacks(51% attack). **2.**Less reward: The overall reward is shared by participants in the pool. **3.**Trust problem: Bitcoin network is designed to be decentralized at the very beginning and does not require trust. However, mining pool results in centralization. Therefore, miners in the pool have to trust each other and the agencies, violating the original principle. **4.**Reduced number of nodes: Each mining pool is only regarded as one node and only pool owners have rights to vote for big decisions but other related miners not.

2. **1.**Pay Per Share(PPS): Miners receive shares that can be paid out at any point along the hashing process. And regardless of whether a block has been solved, the participated miners can receive shares. The shares rate is fixed and known in advance.

   *Advantages: PPS guarantees payments and miners are in low risk of not being paid for their contribution. *Disadvantages: The pool owners always charge high fees.

   **2.**Proportional(PROP): Miners submit shares along the block finding period. The more shares they submit, the more reward they receive once the block is found.

   *Advantages: Reasonable for miners(work more to get more). *Disadvantages: If there are a large number of miners in the pool, each miner will receive very tiny rewards.

   **3.**Pay Per Last N Shares(PPLNS): Only a few lucky miners(the last N shares) get paid for shares at the end of block solving.

   *Advantages: Reduce pool-hopping as miners have no idea which time is the right time to join the pool. *Disadvantages: Large variance of the income that miners can receive.

   **4.** Strategic behavior: PPS is good for people who want to get the fixed reward and be in low risk. PPLNS is good for people who are not pool-hopping and are eager to get more rewards(more than 100% some time) with less consideration in risk. For people who have more computational power, PROP is a good choice.

### j)transaction fees dominate the block reward, when? changes?

1. The bitcoins are the reward of mining blocks but the value of the reward goes down from 50 coins/per block, to 25, 12.5... With fewer and fewer new coins introduced to the network, the mining process reaches the end, and the transaction fees dominate block reward.

2. Fewer miners keep mining blocks as there are no attractive rewards. Therefore, the requirements for computing power is not as high as before. 51% attack might be easily achieved. What's more, as transaction fees begin to dominate block reward, minimum transaction fees might climb. The block owners would have more power to make decisions and if they team up, the decentralized network would be broken down.