ECE8930 Introduction to Blockchain Technology

Final Exam

Biyang Fu

biyangf@g.clemson.edu

July 31, 2020

1. How do PoW-based cryptocurrencies address the “double spend”?

   The blockchain is an open and immutable ledger that ensures that transactions are completed through inputs confirmed by miners. Confirmation makes each unique Bitcoin and its subsequent transactions legal. If you try to repeat the transaction, the deterministic function of the original block will change, indicating that the network is fake and will not be accepted. Proof of Work (PoW) is the original consensus algorithm in the blockchain network. This algorithm is used to confirm transactions and generate new blockchains. Miners use PoW to verify transactions and mine new coins, but its main goal is to prevent potential cyber-attacks or suspicious activities in the network. Every time a miner confirms a transaction, he will receive a coin reward. If one were to try to send one hundred bitcoins to the peer, the transaction would first be in the unconfirmed pool, waiting to be added to the chain. Once it is time for the block to be transmitted, each

computer (or node) in the network will verify it. Here, if double spending occurs, the first transaction is usually added to the blockchain, but the entire network will reject the second and subsequent transactions, thereby avoiding potential double spending. In other words, in order to maintain a PoW-based blockchain and prevent double spending on it, miners must have sufficient rewards to incentivize them to maintain the blockchain accurately and honestly.

2. Compare the "punishment mechanisms" adopted by Casper FFG and IOTA?

   Casper FFG is inspired by PBFT and can be regarded as an improved PBFT. It inherits the important design of PBFT, while adding new mechanisms and simplifying several rules. Vitalik found that PBFT requires **4** rules. **Minimal Slashing Conditions (4)**:

   (1). Sending a **commit** requires seeing 2/3 **prepares**.

   (2). If you make a **prepare** in some epoch pointing to some particular previous epoch, then you need to have seen 2/3 prepares in that epoch, and those **prepares** must point to the same previous epoch.

   (3). If you make a **commit** during some epoch, then you clearly saw 2/3 **prepares** during that epoch, and so any future prepares that you do should better be referencing that epoch or something newer.

(4). You can’t prepare **twice** in a single epoch.

These four rules can be further simplified into two. Minimal Slashing Conditions (2):

(1). A validator must NOT publish two distinct votes for the same target height.

(2). A validator must NOT vote within the span of its other votes.

DAG (Directed Acyclic Graph) is a commonly used data structure in the field of computer science. It satisfies that each edge is directed and cannot return to that point via several edges from any vertex. IOTA is an innovative digital token that uses DAG as a data structure to record transaction history and uses Tangle technology to form a consensus on transactions. The Tangle consensus does not require miners specifically responsible for bookkeeping, but new transactions provide verification for historical transactions, so no transaction fees are required. The price that traders have to pay is to pay computing power to verify whether the two tips conflict with historical transactions in the tangle, and to provide security for the network. The advantage of the Tangle consensus is that there is no need to package transactions into blocks. Since a single node verifies the tip efficiently, the speed at which the transaction is confirmed depends on the speed at which new transactions are added to the Tangle.

3. If you were a member of the Bitcoin community during the DAO attack? Which side would you take or support? Please explain you answer.

   I support ETH. After Ethereum founder Vitalik adopted the hard fork scheme, the stolen coins were recovered. At the same time, Ethereum was divided into two chains, one for the original chain (ETC) and the other for the new fork chain (ETH). There are also two tokens, ETC (Ethereum Classic) and ETH (Ethereum), which represent the consensus and values of the old and new communities respectively.

   At the time of the hard fork vote, about 10% of the voting participants opposed the hard fork. This part of the miners still maintained the computing power of the old chain. They believed that the code could not be tampered with for their own benefit. The code is the law. It is the essence of decentralization and cannot be tampered with, and a hard fork means that the code can be modified at will, and the decision-making is still centralized. But I don’t think so. As an investor, I may be more concerned about my money, and I don’t want hackers to succeed. This is not justified morally. The consequences of so much Ethereum falling into the wrong hands will be very serious, and the community should stop it. Through a hard fork, regulators and legal departments can also be kept out. Our problems are solved by

ourselves. So I support ETH, because that is theft and illegal, and we must fight it.

4. Explain why the Byzantine fault tolerant solution can tolerate up to one- third of the nodes being faulty?

   Oral agreement algorithm OM(m): Suppose that in a team with n generals and m traitors, as long as n>=3m+1 is satisfied, this problem can be solved under the oral agreement algorithm. Among the m traitors, there can be 1 general and m-1 adjutants, or m adjutants.

   ①OM(0) algorithm: The general sends his order to each adjutant. Each adjutant executes the command of the general, if not received the command, the default command is executed.

   ②OM(m) algorithm: The general sends his order to each adjutant. For any i<=n, Vi is the command received by the adjutant i from the general, and the adjutant i serves as the general in OM(m-1) and sends Vi to n-2 adjutants except the general and adjutant i. For any j≠i, Vj is the command received by the adjutant i from the adjutant j using the OM(m-1) algorithm in step 2, and finally the adjutant i uses the majority (V1, V2...Vn-1)) Calculate the final command executed by the adjutant i. Among them, majority (V1, V2...Vn-1) = Vk, where the value of Vk has the most occurrences, that is, the adjutant executes the

command that most people will execute, otherwise the default command is executed.

Note that the value of Vk is unique. For example, there are 5 A and 4 R in V1 to Vn-1, and the number of occurrences of the remaining values is less than 5, then majority (V1,, V2...Vn-1)=A. But if there are 5 A and 5 R, and the other values are less than 5, then majority (V1,, V2...Vn-1) = O, where O is the default command.
Mathematical proof: Proposition: Prove that the OM(m) algorithm holds when n>3m (equivalent to n>=3m+1). Review the two constraints in the oral algorithm:

IC1: All loyal adjutants must obey the same order, that is, consistency;

IC2: If the general is loyal, every loyal adjutant should obey the general's orders;

First introduce a lemma LEMMA1: For any non-negative integer m and k, when n>2k+m and there are at most k traitors, then the algorithm OM(m) satisfies IC2. The mathematical proof of this lemma is as follows:

(1) When k=0, if the general is loyal, according to the algorithm OM(0), it can be known that the loyal minister will directly obey the order sent by the general. According to the assumption of IC2, the

general is loyal, so all the loyal ministers receive the order All have the same value. Therefore, when k=0, the OM(k) algorithm can satisfy IC2;

(2) When k>=1, since n>2k+m, from OM(k) to OM(k-1), since the loyal generals are reduced, the total number of the algorithm is n-1, and The number of traitors is still k. Since n>2k+m, n-1>2k+m-1>=2k, that is, n-1>2k. That is, in the OM(m-1) algorithm, the number of loyalists (n-1-k) is greater than the number of traitors (k). Since OM(k-1) is established, voting according to the majority function, if the general is loyal, if the number of loyalists is greater than the number of traitors, all loyalists will execute the general's instructions.

Then prove that the original proposition OM(m) algorithm holds when n>3m:

(1) First, suppose that the general is loyal, then replace k in LEMMA1 with m, then OM(m) satisfies IC2. Since the general is loyal, all loyal adjutants will execute the general's orders, which naturally meets IC1;

(2) If the general is a traitor, there is no need to consider whether IC2 is satisfied, just prove IC1.

Refer to the proof of LEMMA1, if the general is a traitor, from OM(m) to OM(m-1), since the reduced general is a traitor, the total

number of the entire algorithm is n-1, and the number of traitors is also m -1, the number of loyal ministers n-m+1, since n>3m, the number of loyal ministers n-m+1>2m+1>m-1, that is, the loyal ministers can reach an agreement when OM(m-1) of. In the case of OM(m-1) to OM(m-2), in addition to the general' who wants to send instructions, that is, the adjutant A mentioned in the above case, there are more than 3m-1, and 3m-1 >3(m-1), so in the case of OM(m-1), the original propositional conditions can also be met.

5. What are the benefits of adopting the tree-like data structures (e.g., Merkle tree, and Trie) in the blockchain blocks?

   In virtual currencies such as Bitcoin, the tree structure of the Merkle tree is usually used to record all transaction information. These transaction information are related to each other, and any information changes will be discovered. The so-called Markle tree, to put it bluntly, is a tree composed of hash values according to certain rules. Unlike the hash list, the Markle tree is more convenient to verify and is regionally verified. Binary trees are often used to achieve fast data query.

   The biggest advantage of the Merkle Tree algorithm is that each transaction can be deleted directly, and only the Hash value of this transaction can be retained. In this way, for the entire block, its

cryptographic security and integrity are not changed, but the amount of data can be greatly reduced. (Hash value is 32 bytes, and a transaction generally takes more than 400 bytes). If there is only one transaction in a block without subsequent transactions, then deleting all other transactions will greatly reduce the amount of data in the entire block. Therefore, in UTXO's accounting mode, using the Merkel tree structure, there is usually no need to worry about the problem of excessive data caused by the continuous growth of data.

At the same time, compared to the Hash List, the obvious advantage of the Merkel tree is that it can take out a branch (as a small tree) to verify part of the data. The application in many occasions brings a hash list that cannot be compared. Convenient and efficient. Because of these advantages, Merkel trees are often used in distributed systems or distributed storage.

The use of Merkle trees in the Bitcoin system has many other advantages: First, it greatly improves the operational efficiency and scalability of the blockchain, so that the block header only needs to contain the root hash value instead of encapsulating all the underlying data, which makes Hash operations can be efficiently run on smartphones and even Internet of Things devices; secondly, Merkle trees can support "Simplified Payment Verification Protocol" (SPV), that is, transactions can also be performed without running a complete

blockchain network node. Data is checked. Therefore, it is very meaningful to use tree data structure, like the Merkle tree, in the blockchain.

6. How does the Bitcon blockchain achieve data immunity?

   In the Bitcoin blockchain, shared data is the history of every Bitcoin transaction in history: an accounting ledger. The ledger is stored in multiple copies on a computer network called "nodes." Every time someone submits a transaction to the ledger, the node checks to make sure that the transaction is valid that everyone who spends Bitcoin will spend Bitcoin. Their subsets compete to package valid transactions into "blocks" and add them to the previous chain. The owners of these nodes are called miners. Miners who successfully add a new block to the chain will receive Bitcoin as a reward. The so-called blockchain system security guarantee is "decentralization." If a copy of the blockchain is stored on a large and widely distributed network of nodes, then there is no vulnerability to attack, and it is difficult for anyone to build enough computing power to subvert the network.

   In theory, the system is not disturbed by two things: each block has a unique encrypted fingerprint, and the "consensus agreement", which is the process by which nodes in the network reach a consensus on shared history. Fingerprints are called hashes and require a lot of

calculation time and effort at first. Therefore, this can prove that the miner who added the block to the blockchain has completed the calculation work to obtain the Bitcoin reward (hence, Bitcoin is said to use the "Proof of Work" protocol). It can also be used as a kind of seal, because changing blocks will require generating new hashes. However, it is easy to verify that the hash matches its block, and once a node does so, the node will update its respective blockchain copy with the new block. This is a consensus agreement.

The final security element is that the hash also acts as a link in the blockchain: each block contains the unique hash of the previous block. Therefore, if you want to retroactively change an entry in the ledger, you must calculate a new hash not only for the block it is in but also for each subsequent block. And you must add new blocks to the chain faster than other nodes. Therefore, unless you have a more powerful computer than the rest of the node combination (and even then, success is not guaranteed), any blocks added will conflict with existing blocks, and other nodes will automatically reject your changes. This is what makes the blockchain tamper-proof or "immutable".

7. What are the differences between the sidechain and Ethereum’s sharding?

Both of these two architectures involve a hub-and-spoke architecture, which consists of a central main chain supporting the consensus of the system and a set of sub-chains containing actual user transactions. The key technical difference between the two is related to the concept of tight coupling. Tight coupling is a feature of Sharding, but it is not a feature of side chains. That is to say, in the Sharding system, the effectiveness of the main chain (called beacon chain in Ethereum 2.0) and the sub-chain are inseparable. In other words, if a block on the sub-chain is attached to an invalid block on the main chain, then the sub-chain block is also an invalid block; more importantly, if a block on the main chain Contains an invalid sub-chain block, then the main chain block is also an invalid block.

The basic idea of Ethereum sharding is to divide the nodes in the network into different shards, and each shard can process different transactions in parallel, so that transactions that are not connected to each other can be processed in parallel to increase network concurrency. The feature of the fragmentation scheme is that as the number of nodes increases, the network throughput also increases. In the latest tweet, Vitalik Buterin stated that the most important principle of Ethereum's sharding technology is to "maximize the same properties as a single blockchain." The purpose of quadratic sharding is to increase transaction capacity through a two-layer design. The first

layer does not require a hard fork, and the main chain remains the same. However, a contract called a validator management contract (VMC) needs to be published on the main chain, which is used to maintain the sharding system. There will be O(c) shards in this contract (currently 100), and each shard is like an independent "Galaxy": it has its own account space, and transactions need to specify which shard they should be published to, and communication between shards is limited. Most users in a sharding system will run two parts of the program. (i) A full node (requires O(c) resources) or a lightweight node (requires O(log(c)) resources) on the main chain. (ii) A "sharding client" that interacts with the main chain via RPC.

The sidechain is an off-chain expansion, which belongs to off-chain transactions, which corresponds to the Lightning Network of Bitcoin and the Raiden Network of Ethereum. Pay some Ethereum or Bitcoin as a deposit in advance, and then you can use some means off-chain to trade with other people. Put this settlement on the blockchain after the transaction is over. It is more effective to participate in major nodes such as mainstream exchanges and wallets. The core idea is that each chain can handle transactions or things independently, without communicating with each other, and finally put the settlement information on the main chain. The most essential difference from

sharding is that sharding is an on-chain expansion, a reconstruction of the entire blockchain network, and the nodes are also interrelated.

8. Choose two anonymous cryptocurrencies and explain the strategies/approaches they adopted to provide user anonymity.

(1). Monero

Monero uses complex on-chain cryptographic methods such as Ring signatures, RingCT, Kovri, and Stealth addresses to protect the privacy of its users. Monero, launched in 2014, is the world's first private, secure, and untraceable digital currency of the internet. Ring signatures were invented by Ron Rivest, Adi Shamir, and Yael Tauman, and introduced in 2001. They are digital signatures that can be performed by any member of the ring or group, and all the signatures are potential and eligible signatures. A ring signature is by default applicable to the blockchain, and it enables transaction mixing. This means that when money is sent, it is sent as a group of randomly picked ring signed transactions of the same amount. And out of this, only one is the actual sender, though all may be eligible to send. Any incoming transaction is coming as a group of transactions and has many possible senders, and each sender has the same chance of being the true sender. This makes Monero a top choice for maintaining a sender's privacy.

Stealth addresses take care of the recipient's privacy. Stealth addresses

don’t allow a third party to see any transactions done in and out of that address on the blockchain. To make it easier to understand, consider your stealth address as your bank account number. In traditional banking, even if you give your account number to someone, they can’t see your transactions, identify your balance, or find out your spending habits. Stealth addresses guarantee the same level of transactional privacy in Monero. When a transaction is done on the Monero blockchain, it doesn’t list the public address of the receiver on the blockchain. It instead creates a new one-time destination address which is not linked to a receiver’s public address. Irreversible cryptographic math ensures this unlinkability between both the public and stealth addresses. The receiver can only scan the blockchain for these one-time stealth addresses and verify their funds.

Ring CT stands for “ring confidential transactions”. This hides the amount that’s been transacted on the Monero blockchain. This feature is now implemented and will not only hide the source of the funds but also hide amounts being sent in a transaction.

Kovari is an open source technology. It uses routing technology and encryption technology to hide IP and geographic location of transactions by creating a new layer on the Internet. This work is still in progress, but it is worth the wait. I think this is the final nail in the coffin for this anonymous cryptocurrency. And will make Monero the most trusted, open source, decentralized, and fully anonymous cryptocurrency.

(2). Komodo

Komodo is the underdog in the cryptocurrency world, and also one many are unaware of. The interesting thing, however, is that they are also anonymous crypto. Komodo archives this by implementing zk-SNARK protocol also known as zero-knowledge proofs inherited from Zcash. By inherited I mean they have forked out of Zcash and implemented a better proof of algorithm for security reasons on it. That’s why Komodo also has similar limitations like Zcash in terms of private transactions which their team is trying to solve. Also, Komodo is not only for private transactions because they are much more focused on decentralized exchanges, cross chain atomic swaps etc. Hence, it is quite a decent project to look into.

The Komodo blockchain platform uses Komodo's open source cryptocurrency for transparent, anonymous, private and fungible transactions. Then, through the delayed proof-of-work (dPoW) protocol, the blockchain using Bitcoin makes them super secure. dPOW is a new protocol developed by Komodo developers. This is a consensus mechanism that uses a conventional proof-of-work protocol (just like Bitcoin), but it is different. dPoW involves a mechanism that can notarize blocks on the blockchain to ensure that they are completely unchanged and provide a second layer of security for transactions. 64 pre-selected notary nodes perform this notarization work and reduce the risk of immutability. This means that if some attacker wants to change a historical Komodo

transaction, he/she must first change the Bitcoin blockchain, which we already know is impossible.

SuperNET is a decentralized organization that is developing open source and decentralized tools for the cryptocurrency market, such as multi-currency wallets, decentralized exchanges and price stability products. Komodo cryptocurrency is also the official currency of the SuperNET ecosystem.

Komodo team has developed a decentralized exchange powered by the novel tech of atomic swaps and that's why I see them a step ahead than other decentralized exchanges. Other decentralized exchanges use proxy tokens or concept of pegged assets to enable exchange on their platforms but BarterDex bypasses those workarounds via atomic swaps. And on almost all decentralized exchanges too, one needs to exchange currencies by keeping BTC as an intermediary, they don't have decentralized order matching and settlements while on BarterDex there is no such limitation.

So far BarterDex has powered more than 50,000 atomic swaps and has more than 80 cryptocurrencies integrated on their DEX. A less user-friendly GUI version is available for advanced users but soon a very easy to use exchange with enhanced UI is expected to be released this year.