ECE 8930: Blockchain Technology and Web 3.0

Homework 1

Saurabh Sharma
09/17/2023

Q1) What security features can the blockchain provide? Explain how the blockchain data structure enforces these features.

- Blockchain provides immutability i.e., once data is stored in the blockchain, it can't be altered. This is because each node stores a cryptographic hash of the previous block and changing any block in between would entail rehashing all further blocks, which is computationally infeasible, and also consensus algorithm won't allow it.
- Blockchain operates on a decentralized network of users, and this means that no single entity or person controls the blockchain; thus, there is no single point of failure or corruption. Each person has a copy of the ledger, and if any one person gets attacked, the attacker tries to corrupt the data, the consensus algorithm won't allow it.
- Permissioned access. Some blockchains only allow certain individuals to participate in the blockchain, and it implements it by only giving the ledger to those selected individuals, and thus only they get to participate in creating new blocks or conflict resolutions.
- Time-Stamping. Each block in a blockchain contains a timestamp, providing a chronological order of transactions. This ensures that the sequence of events is maintained and can be used for various legal and auditing purposes.
- Resistance to DDoS attacks. Due to it's distributed nature there is no single point of failure and hence performing ddos attack would require a very large-scale attack on a lot of users at the same time.
- Consensus Mechanisms: Different consensus mechanisms like Proof of Work and Proof of Stake ensure that all the users in the network agree on the validity of transactions. This prevents any conflict of transaction down the road and also prevents any third person to alter the blockchain.
- Cryptography. Public and private keys are used to verify ownership of assets and to secure data.
- Transparency and auditable transactions. Because each person has a copy of up to date ledger, all transactions are visible to every user and this allows easy auditing to ensure all transactions are valid.
- Data integrity and trustlessness. The combination of cryptographic hashing, decentralization and consensus algorithm ensures that the data stored in blockchain is trustworthy and there is no need of trust in bigger institutions.

Q2) Data on the blockchain is secure and private. Explain what is true /not true in this statement.

Data on blockchain is very secure but it is not private. Data is highly secure in blockchain because as mentioned above everyone has a copy of the ledger and they can verify any suspicious activity. The consensus algorithm does it automatically. No one can change any block in the chain. Because each further block stores the hash of previous block any changes

in a block would require rehashing of all further blocks, which is not feasible. Hence the data is very secure in a blockchain.
The data is not private at all by the very basic nature of how blockchains work. The blockchains themselves can be private (i.e. selected few have access to the blockchain) or public but every single user in the network will have access to all current and past records and conduct mining activities.

Q3) Compared to this legacy address scheme, how does SegWit address the transaction malleability? Where is the witness data stored? Why doesn't the segregation of the witness data from the transaction data cause other security concerns?
Transaction malleability arises when the digital signatures, or witness data, within a Bitcoin transaction, can be modified by a third party without invalidating the transaction itself. While this alteration doesn't change the ultimate outcome of the transaction, it can lead to confusion and complications, especially for services built on top of the Bitcoin blockchain. SegWit or Segregated Witness addresses this by changing the data structure in Bitcoin transactions. It separates witness data (including digital signatures) from transactional data. The witness data is stored in a "witness" data structure. This ensures that any modification to witness data doesn't impact the transaction's core ID and its essential information, and thus, third parties aren't able to manipulate the transaction.

The witness data is stored in a dedicated data structure called "witness". It is closely associated with the transaction but kept separate to ensure the security of transactions as described above.

This segregation doesn't cause other security concerns because the data integrity is maintained (witness data is cryptographically linked to the transaction), security against malleability (prevents third parties from altering digital signatures without invalidating the transaction), block capacity is increased (block capacity is increased thus there is less risk of network congestion), segregation of data is clear (there is a clear distinction between essential data and associated signatures which makes verification straightforward and makes it more secure and scalable).

Q4) I set up a BTC account by generating a pub/priv key pair. Assume that the software has no bugs. How likely is it that someone else could redeem my coins? Compare that likelihood to the likelihood of that person winning the powerball lottery, winning the powerball lottery twice, being hit by lightning, and being hit by lightning twice. Is that risk acceptable? Why or why not?
When we generate a Bitcoin public/private key pair using secure software and best practices, the likelihood of someone else being able to guess or compute it is extremely low. To be precise, it is 1/ 2^160 (as bitcoin has 2^160 possible addresses), which is almost negligible. Modern-day computers can not compute or guess this private key in any reasonable timeframe (let's say a human life) hence modern-day cryptography is considered secure.
To put this in perspective, you are more likely to win a Powerball lottery (1 in 2.9 * 10^8 chance), to win back to back Powerball lotteries (1 in 9 * 10^18 chance) to be hit by lightening on random

chance (1 in 1.5 * 10^4) and to be hit by lightening twice back to back (1 in 3* 10^8). These extremely rare events are still common compared to the event of guessing a private key hence the chance of guessing a private key is considered zero for all practical purposes.

Q5) What is the difference between the "absolute chronological order" and "relative chronological order"? Which one of the two is employed in the BLC technology, and how is it implemented?

In absolute chronological order, the events are ordered based on their actual timestamp or time of occurrence (for eg. according to UTC time of events), whereas in relative chronological order, the events don't rely on actual timestamps but are arranged based on their position relative to each other, it doesn't require exact time measurements.

Absolute chronological order is implemented in BLC technology. Each block in the blockchain contains a timestamp (usually Unix epoch time) of the time when the block was mined. This timestamp provides an absolute chronological order of the blocks and the transactions within them. This timestamp is also validated by the network through a consensus mechanism so that the timestamp is consistent with the network's rules and is not manipulated. Nodes on the network periodically synchronize their clocks with other nodes to maintain a consistent understanding of time. Each block also contains a hash of the previous block, and since each timestamp is unique, the use of timestamps also ensures data security and trustworthiness.

Q6) What determines the difficulty of PoW? How is the difficulty adjusted? Why do we need to set a difficulty for PoW?

The difficulty of proof of work is a crucial aspect of blockchain security. The difficulty of PoW is set the by network and it represents the level of computational challenge miners must meet in order to contribute to validating a new block of transactions. Miners compete to find a nonce which when combined with the block's data produces a hash. This difficulty is regularly adjusted, typically once every two weeks (2016 blocks) to ensure a consistent time is required to validate new blocks of transactions.

We need to set the difficulty for PoW because of several reasons. The first one is that it ensures network security by requiring significant computational effort to add a new block, making it economically impractical for any single entity to control the network. Second, it maintains a predictable block creation/validation time which is essential for operational stability and fairness. Third, this difficulty provides resilience against DDoS and Sybil attacks as attackers would need substantial computational power to compromise the blockchain's integrity. Lastly, it encourages competitive mining by ensuring the process is challenging and rewarding, discouraging attempts to flood the network with blocks.