ASSIGNMENT 2

CS6504 Cryptography and Blockchain fundamentals

Dr Manish Singh

Andrew Graff
2231290

Assignment 2

LO: Explain blockchains and the cryptocurrency ecosystem

LO: Analyse the role cryptography plays in a blockchain

Providing *comprehensive solutions – include any code snippets or diagrams*

Cryptographic Primitives

1. **With respect to cryptographic hash functions what are Preimage, Second Preimage, and Collision Resistance?**

   Pre-image Resistance (one-way function) is where it is computationally infeasible (meaning today's computation would take more time than is available) to reconstruct the original message from the given hash value (because no attack is significantly more efficient than brute force).

   An example would be the given hash **h**, it would be infeasible to find the *original message* (pre-image) "**x**"; H (Hashing algorithm example MD5) so H(**x**) = **h** (16 bytes in Hex fixed-length hash value).

   Second Pre-image Resistance (Weak Collision Resistance) is where it is computationally infeasible to find a second message (pre-image) that produces the *same hash value*. An example would be the given message "**x**", it is infeasible find the second message (pre-image) "**y**" where "**y**" not equal "**z**" at different inputs with H(**y**) = H(**x**) being the same hash value.

   Collision Resistance (Strong Collision Resistance) is where computationally infeasible to find two different messages that produce the same hash value. It is infeasible to find two messages **x** and **y** where **x** does not equal **y** such that H(**x**) = H(**y**). MD5 would not be collision resistance because if two same MD5 hash values were encrypted it would produce the *same* hash value.

   Preimage, Second Preimage and Collision Resistance are some of the properties of the cryptographic hash function.

2. **What is the general algorithm for ECDSA? Why is ECDSA a good cryptographic function?**

Elliptic Curve Digital Signature Algorithm (ECDSA) general algorithm has four elements. This digital scheme uses the same global domain parameters which signifies the collection of rules when applying the algorithm. It defines the elliptic curve and a point of origin on the curve which is significant in the cryptographic function.

A signer first generates a key pair (private and public). A hash value is generated for the message to be signed using a combination of the private key, domain parameters and hash value for the digital signature to be generated.

To verify the signature, the verifier uses the signers public key as input, domain parameters, integer S, the output is a value v that is compared to r); the signature is verified if v=r.

In ECDSA there are signatures and private/public keys. Alice message “x” is signed and encrypted using a private key. Bob verifies the message using public key.

The public key would verify the private key was used in the signature. The public key would make sure the person spending the money has access to the private key. The digital signature is an authentication method where the public key pair and a digital certificate are used as a signature to verify the identity of a recipient or sender of information.

This is why ECDSA is a good cryptographic function as we can confirm the sender of information. A method used in Bitcoin to provide signatures that a transaction is valid.

- Alice and Bob. Alice wants to send a message, and to prove she is the one signing for the message with a digital signature.
- Alice takes a hash of the message and the creates a signature.
- The signature is an (R value and an S value). These two values make up the signature so Bob can check.
- Alice has a public key and a private key.
- Alice will send Bob her public key, and sign the message with her private key
- This is how Bob can prove that Alice sent the message.

Bitcoin

3. **Describe how the blocks in bitcoin protocol are tamper evident?**

   The blocks in bitcoin protocol are tamper evident as each owner (of the bitcoin simply a chain of signatures) digitally signs a hash of the previous transaction and the public key, when transferring the coin to the next owner. These transactions are recorded on the coin with the payee to verify signatures to verify the chain of ownership. This is what makes the bitcoin protocol tamper evident with the involvement of a complex computation (elliptic curve digital signature algorithm) to digitally sign. It creates a hashing code and reinforces data integrity so only the owner would have the private key generated from the hash and public key. Everyone else can see the public key and is also verified by computers worldwide. A peer-to-peer network with this validation method works for both and public to see, and the production of coins are immutable.

4. **Explain how bitcoin address double spending**

   Bitcoin addresses double spending by using a timestamp server. The time-stamp server proves the data existed at the time. It takes a hash block of items (in this case all the transactions made on the electronic coin) and publishes this hash for the wide public to see becoming the proof of work (consensus algorithm). A chain is formed using the timestamp server, that will always include the timestamp before in the hash and further additional timestamps. This database and public broadcasting are how bitcoin will address double spending with the verification of the transaction to all nodes. The peer-to-peer network and proof of work is how the payee will see all the transactions before to be factually assured the bitcoin received has not been double spent. It is the chronological order of transactions agreed between peers that bitcoin resolve the double spending issue.

5. **How does bitcoin prevent denial of service attacks?**

   The proof of work is the blockchain technology verifying every single transaction. This process scans for a value that matches a hash number of zero bits when hashed. Hence the timestamp network and the accumulation of all the timestamps chained together. The block cannot be changed without redoing the entire work. There is a complex cryptographic puzzle that requires to be solved to add a new block to the block chain. The peer-to-peer network involves multiple nodes to continue the transactions and blocks even if other nodes are being attacked. This is how the bitcoin can prevent the denial-of-service attacks. It would be infeasible for attackers to modify all the proof of work before and after affecting a mass of CPU power. Transaction fees are involved in the process of purchasing bitcoin that further add to an increase desire to not pursue a denial-of-service attack.

6. **On the event where there are two blockchains with divergent histories, which blockchain does bitcoin protocol tells miners to mine on?**

   Miners will work on the first blockchain received and save the other blockchain until a tie break when the database finds the next proof of work with only one chain extends. The longest blockchain is always considered to be the correct one and will often resource the working nodes from previous blocks to the longer chain. The longest chain has the greatest proof of work given the amount of CPU power involved and is controlled by honest nodes (computers/servers) it will also be the fastest block chain. This is how miners will know which to mine on and add transactions to the blockchain.

7. **Who controls Bitcoin? (miners, core developers, companies, journalists, regulators and why?)**

   According to the bitcoin white paper, it is the parties involved in the bitcoin peer to peer electronic cash system transaction that control bitcoin that includes the requiring efforts of the miners to support the blockchain with the necessary CPU power required to run this long and ongoing extensive chain of mathematical operations and sequential blocks. There are no requirements for a third party (such as financial institutions or 'government involvement' to mediate the transactions) thus commending this new style of electronic payment as a way to secure legitimate transactions via digital signature and a proof of work between peer to peer only. The transaction is made available to the public to verify by seeing the published authenticated transactions. This is a cryptographic proof instead of a trust-based system. It is simply the peer-to-peer computer network that control bitcoin.

Lightning

8. **List issues that limit bitcoin scalability**

   The issues that limit bitcoin scalability are the limited ability of the network to process transactions rapidly and efficiently. These are the number of nodes in the system that miners that are needing more CPU power to process and develop the growing blockchain with its volume of transactions. The original bitcoin block header with no transactions was 80 bytes supposedly generated every 10 minutes, according to the bitcoin white paper (it was estimated a prediction of 1.2GB every year in 2008). High peak transactions with a block creation time of 10 minutes results into increased transaction fees during congested periods.

9. **List two solutions which are developed to solve scaling issue.**

   These are the two solutions that have been developed to solve scaling issue.

   1. The Lightning Network was created to fix the blockchain scalability issues. As discussed before, each block on the blockchain takes a creation time of 10 minutes which limits the number of blocks than can be produced. To save time and saving costs for a faster and cheaper blockchain creation, a protocol was proposed by developers Thaddeus Dryja and Joseph Poon in 2016.

      "This lightning network creates a second layer on top of the bitcoin blockchain that uses user-generated, micropayment channels to conduct transactions more efficiently", (Acheson et al, 2023).

      The layer two solution reduces the load of the main blockchain and can allow for off-chain smaller transactions between two parties as a way of bidirectional payment channel. The separate blockchain improves instant and low-cost transactions between users.

   2. Improved Consensus Mechanisms. This approach was developed to help update the networks consensus mechanisms (verifying transactions and maintaining the security of the underlying blockchain) from the original security-based proof-of-work mechanism.

      Proof of Stake is proposed to solve scalability by operating faster than the less speedy proof of work consensus. POS is known for lesser energy consumption and a quicker handling of transactions.

10. What value did Ethereum add to the blockchain space? How?

Ethereum added digital “Contracts” to the blockchain space becoming the largest application of this programmable money blockchain technology. It diverts the form of crypto transaction as means of direct payment to an asset driven per basis exchange. So Ethereum is still using the decentralized methods as per bitcoin, however implementing a slightly more complex exchange between peer to peer that involve a little more complexity. It could be such as in the contract, Alice sends Bob “x” if Charlie wins, and Bob sends “y” to Alice if Charlie does not.

The programmable transactions add an extra amount of value for peer to peer, being able to perform complex authenticated and transparent transactions without requiring multiple third parties involved. This is simply a new use case for the blockchain technology space.

11. What is the difference between storage and memory in Solidity?

The difference between storage and memory in Solidity is the data locations of where to store variables.

- Storage refers to variables stored permanently on the blockchain.

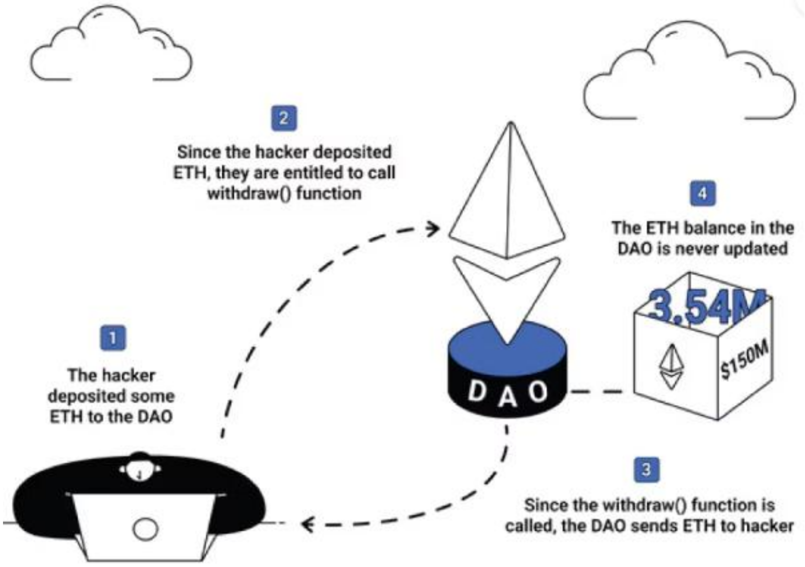
- Memory variables are temporary and are erased between external function calls to your contract.

During execution, solitude smart contracts can use any amount of memory, which is then wiped once execution ends. Storage is persistent and smart contracts can always access this stored data.

12. Explain what re-entrancy attack is and how it led to creation of Ethereum Classic?

A re-entrancy attack is where a cyber-criminal hijacks the cycle before the balance update. The Ethereum withdrawal is a three-step cycle is a balance confirmation, remittance, and balance update. This re-entrancy attack would repeat itself emptying the crypto wallet of its funds. The attack would perform a continuous withdrawal of funds before the next update exploiting the vulnerability.

One of the largest blockchain hacks, as per image above was the Ethereum DAO hack causing the hard-fork. “A hard-fork is a change to the underlying Ethereum protocol, creating new rules to improve the system” (Jameson, 2016). ETC facilitates smart contracts and leans towards a more digital store of value so it can be saved and exchanged, keeping its value.


2
Since the hacker deposited ETH, they are entitled to call withdraw() function
4
The ETH balance in the DAO is never updated
3.54M
$150M
DAO
1
The hacker deposited some ETH to the DAO
3
Since the withdraw() function is called, the DAO sends ETH to hacker

This cyber hack resulted in millions of ETH loss and led to the creation of Ethereum Classic. ETC had a re-entrancy guard using a checks-effects-interactions pattern. “Although re-entrancy attacks continued to happen and sophistication of attack methods continue to evolve”, (Group, 2021).

13. **Compare and contrast proof of work and proof of stake. List other distributed consensus algorithms used/considered in different blockchain**

Consensus mechanisms is used by cryptocurrency and blockchain technology. This mechanism ensures the computers that run the blockchain keep records of transactions and parties involved reach agreement.

As we discussed earlier, consensus is used to prevent double spending. Below are two types of consensus mechanisms where we compare the differences and similarities.

Proof of Work (PoW)	**Proof of Stake (PoS)**
Proportion to computing power	**Proportion to ownership**
Verifying cryptocurrency transactions through mining	Validators are chosen based on set of rules depending on the stake owned in blockchain
Decentralised and distributed	Decentralised (more so for wealthy) and distributed
Competition between miners to solve cryptographic puzzle and validate transactions to earn rewards	Randomly chosen validators to make sure transaction is reliable and receiving crypto as compensation
Environmentally less friendly as requires a significant amount of energy to verify transactions. These are the CPU's on the network required to run the block chain made up miners.	Large initial investment is required to qualify as a validator dependant on the network size.
Cryptocurrencies: Bitcoin, Dogecoin	Cryptocurrencies: Ethereum, Cardano, Solana
More tested in terms of security strengths and weaknesses	Uses less computational power than Proof of Work
Miners are the nodes that validate transactions and propose new blocks on the blockchain	Validators are the nodes that verify transactions and propose new blocks – that have a large stake in the token

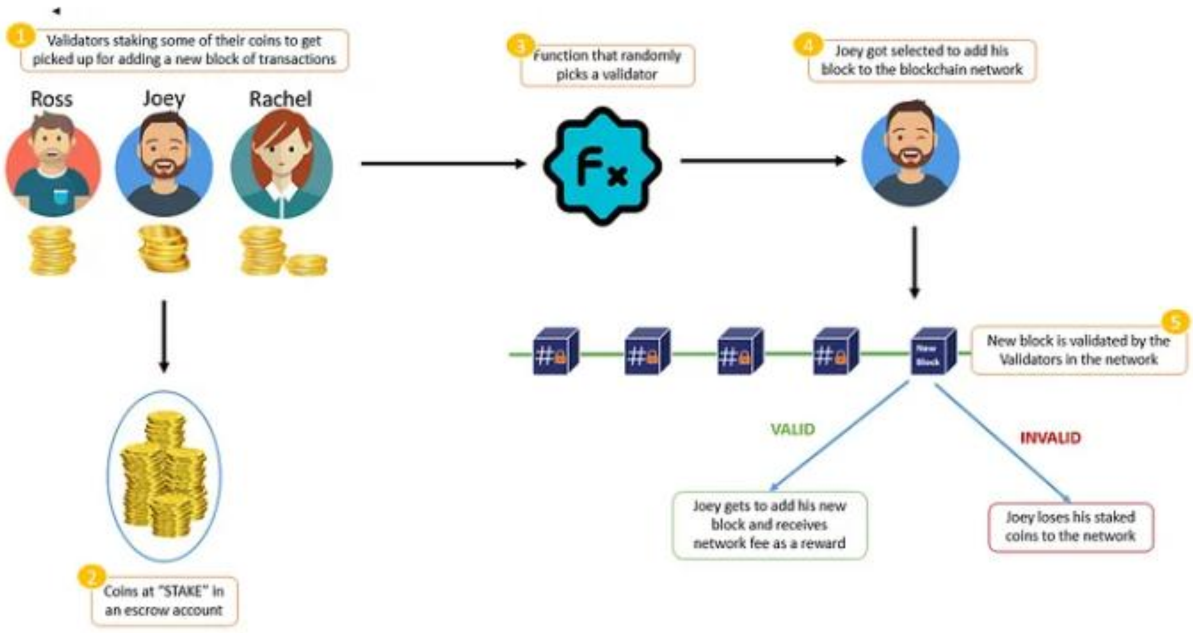
Other consensus algorithms used/considered in different blockchains are;

Byzantine Fault Tolerance (BFT)

Uses a voting process to reach consensus and the majority of nodes to agree on the current state of the blockchain. This is designed to work in the presence of malicious nodes. Often used in permissioned blockchains, for only known and trusted nodes. Fast and increased capacity to handle a large number of transactions by the second. Ripple and Hyperledger Fabric are some of the cryptocurrencies using BFT.

Delegated Proof of Stake (DPoS)

Delegated proof of stake is a variant of the (PoS) where the token holders elect a small group of delegates to add blocks to the chain and validate transactions. The delegates carry such responsibilities that if not acting honestly, could potentially lose their position and rewards. Cryptocurrencies Tron or Bit shares use DPoS.


1
Validators staking some of their coins to get picked up for adding a new block of transactions
Ross
Joey
Rachel
2
Coins at "STAKE" in an escrow account
3
Function that randomly picks a validator
Fx
4
Joey got selected to add his block to the blockchain network
New Block
5
New block is validated by the Validators in the network
VALID
INVALID
Joey gets to add his new block and receives network fee as a reward
Joey loses his staked coins to the network

Credit — Shiksha Online

Proof of Authority (PoA)

Again, uses a smaller group of trusted validators for validating transactions and adding new blocks to the chain. The validators are elected given their reputation and expertise and as explained before, risk incentives if not acting within authority. This type of consensus suitable for a private blockchain network.

14. **What are some possible ways you could imagine a blockchain application used in governance? List some of the similar systems if already implemented.**

A blockchain application being used in Governance could be for voting systems. This could mean voters are verified so that everyone taking part in the voting are authenticated. The voting will be secure to defeat any cheating in the voting system. The transparency adds to confidence in the public vote to see the block chain votes.

Another way could be for property or land ownership. Where the distributed ledger system contains rightful ownership of the property or land. The database of recording these would be accurate, detailed and most importantly fast and secure.

Transport services in Governance could adapt the blockchain application verifying the passengers who use the services, tracking and recording the passengers and transactional processes.

Some countries who are currently using the blockchain technology are Dubai. “Adopting blockchain technology Dubai stand to unlock 5.5 billion dirham in savings annually in document processing alone” (Hamdan, 2022).

Dubai government expresses its great interest in adapting the blockchain technology seeing the great savings for the country to build further infrastructure.

El Salvador is the first nation that recognizes Bitcoin as legal tender that means it has accepted this as a decentralised form of currency payment between peer to peer or in this case peer to government.

Switzerland appreciates a tax-free city introducing “Crypto-Valley” where investors enjoy the virtual currency hub.

References

(Acheson et al, 2023)	Acheson, N. Nguyen, H. Biggs, J. Tan ,E. May 30, 2023. *What is Bitcoin's Lightning Network?*, What is Bitcoin's Lightning Network? - The Lightning Network Explained (coindesk.com)
(Group, 2021)	Group A. September 27, 2021. *Preventing Re-Entrancy Attacks – Lessons from History.* Preventing Re-Entrancy Attacks — Lessons from History | by Amber Group | Amber Group | Medium
(Hamdan, 2022)	Hamdan, S. 2022. *What is the Dubai Blockchain Strategy?* Dubai Blockchain Strategy | Blockchain Dubai | Digital Dubai
(Jameson, 2016)	Jameson, H. October 18, 2016. *Upcoming Ethereum Hard Fork.* FAQ: Upcoming Ethereum Hard Fork | Ethereum Foundation Blog
(Nakamoto, 2008)	Nakamoto, S. 2008. *Bitcoin Whitepaper.*