CT703D-N Blockchain Technology
Assignment / Sample Questions for Quick Reference

UNIT #1: Background Theories

[1.1] What is Blockchain?

A Blockchain is a constantly growing ledger(file) that keeps a permanent record of all the transactions that have taken place, in a secure, chronological, and immutable way. It can be used for the secure transfer of money, property, contracts, etc. without requiring a third-party intermediary like bank or government.

Blockchain is the backbone of the most famous cryptocurrency named Bitcoin. It is a peer to peer electronic cash system and a decentralized network which allows users to make transactions directly without the involvement of third-party to manage the exchange of funds.

[1.2] What are the different types of Blockchains?

There are mainly three types of Blockchains introduced to the world.

1. Public Blockchain: A Public Blockchain is a kind of Blockchain which is "for the people, by the people, and of the people." There is no in-charge it means anyone can read, write, and audit the Blockchain. It is an open-source, distributed, and decentralizes public ledger so anyone can review anything on a public Blockchain. They are considered to be Permissionless Blockchain.

2. Private Blockchain: A Private Blockchain is a private property of an individual or an organization. It is controlled by a single organization that determines who can read it, submit the transaction to it, and who can participate in the consensus process. They are considered to be permissioned Blockchain.

3. Consortium Blockchain or Federated Blockchain: In this Blockchain, the consensus process is controlled by a pre-selected group, i.e., group of companies or representative individuals. These pre-selected group is coming together and making decisions for the best benefit of the whole network. Such groups are also called consortiums or a federation that's why the name consortium or federated Blockchain.

[1.3] List the key features of Blockchain*.*

1. Immutability: Immutability means something that can't be changed or altered. This is one of the top Blockchain features that help to ensure that the technology will remain as it is – a permanent, unalterable network. Every node on the system has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof. So, without the consent from the majority of nodes, no one can add any transaction blocks to the ledger.

2. Decentralized: The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework. Rather a group of nodes maintains the network making it decentralized. As the system doesn't require any governing authority, we can directly access it from the web and store our assets there.

3. Enhanced Security: Added with decentralization, cryptography lays another layer of protection for users. Cryptography is a rather complex mathematical algorithm that acts as a firewall for attacks. Every information on the Blockchain is hashed cryptographically. In simple terms, the information on the network hides the true nature of the data. For this process, any input data gets through a mathematical algorithm that produces a different kind of value, but the length is always fixed.

4. Distributed Ledgers: Usually, a public ledger will provide every information about a transaction and the participant. It's all out in the open, nowhere to hide. Although the case for private or federated Blockchain is a bit different. But still, in those cases, many people can see what really goes on in the ledger. That's because the ledger on the network is maintained by all other users on the system. This distributed computational power across the computers to ensure a better outcome. This is the reason it's considered one of the Blockchain essential features. The result will always be a higher efficient ledger system that can take on the traditional ones.

5. Consensus: In simple terms, the consensus is a decision-making process for the group of nodes active on the network. Here, the nodes can come to an agreement quickly and relatively faster. When millions of nodes are validating a transaction, a consensus is absolutely necessary for a system to run smoothly. You could think of it as kind of a voting system, where the majority wins, and the minority has to support it.

6. Faster Settlement: Traditional banking systems are quite slow. Sometimes it can take days to process a transaction after finalizing all settlements. It also can be corrupted quite easily. Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster, which saves a lot of time in the long run.

[1.4] How does Blockchain differ from relational databases?

The Blockchain differs from the relational database in the following ways.

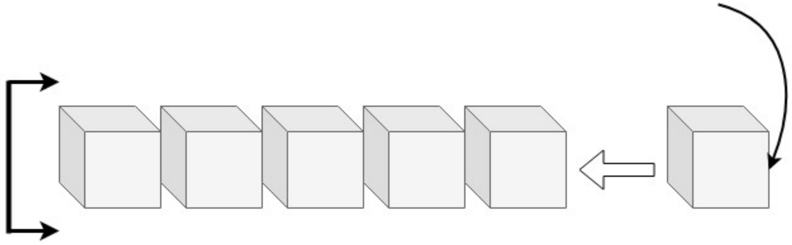
Points	Blockchain	Relational Database
Unit of data	Block	Table
Failure	None	Can happen
Centralized Control	No	Yes
Modification in data	Not Possible	Possible
Single Point of Failure	Does not exist	Exists

[1.5] Name some popular platforms for developing Blockchain applications.

- Ethereum
- Hyperledger Sawtooth
- Quorum
- Ripple
- R3 Corda
- Qtum
- IOTA
- EOS

[1.6] What do you mean by blocks in the Blockchain technology?

A Blockchain consists of a list of records (some or all of the recent transaction). Such records are stored in blocks. Each time a block gets completed, a new block is generated. The block linked with other blocks constitutes a chain of blocks called Blockchain. Each block, after added into the Blockchain, will be stored as a permanent database. We cannot delete or reverse any block from the Blockchain.



[1.7] Every block of Blockchain consist of what elements?

Every block must include these three things:

- A hash pointer to the previous block
- Timestamp
- List of transactions

[1.8] Can you modify the data in a block?

No, it's not possible to modify the data in a block. In case any modification is required, you would have to erase the information from all other associated blocks too.

[1.9] What type of records can be kept in the Blockchain? Is there any restriction on the same?

No, it is not possible to give restriction for keeping records in the Blockchain approach. We can put any type of data on a Blockchain. Some of the common types of records which can be kept in the Blockchain are:

- Records of medical transactions
- Transaction processing
- Identity management
- Events related to organizations,
- Management activities
- Documentation

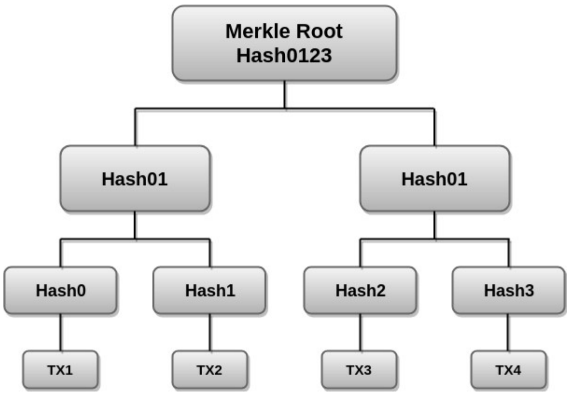
[1.10] Which cryptographic algorithm is used in Blockchain?

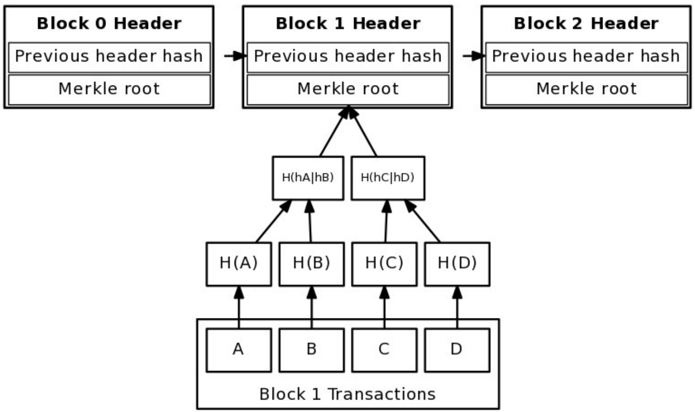
Blockchain uses SHA-256 Hashing algorithm.

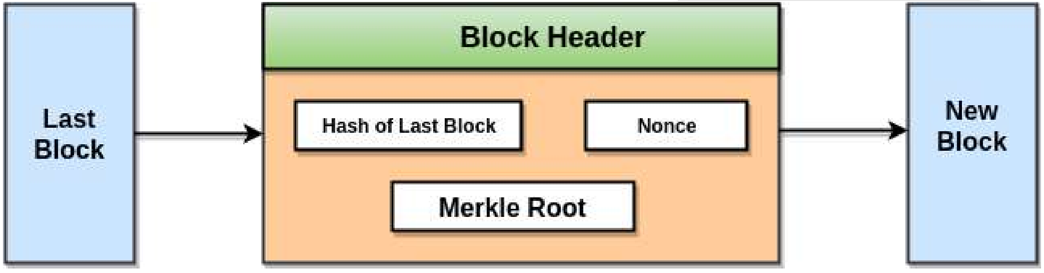
[1.11] What are the Merkle trees? What is its importance in Blockchain?

Merkle tree is a fundamental part of Blockchain technology. It is a mathematical data structure composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. It also allows for efficient and secure verification of content in a large body of data. It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure. Merkle Tree is also known as Hash Tree.

The Merkle tree plays a vital role in Blockchain technology. If someone needs to verify the existence of a specific transaction in a block, then there is no need to download the entire block to verify the transaction in a block. He can only download the chain of block headers. It allows downloading a collection of a branch of the tree which contains this transaction is enough. We check the hashes which are relevant to your transactions. If these hashes check out is correct, then we know that this particular transaction exists in this block.



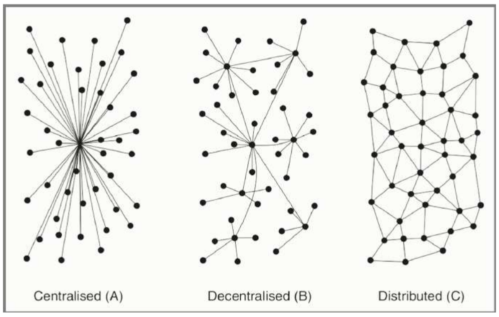




[1.12] What is Double Spending?

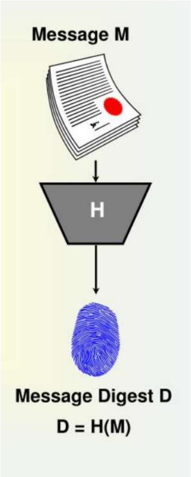
Double-spending is a potential flaw in a digital cash scheme in which the same single digital token can be spent more than once. Unlike physical cash, a digital token consists of a digital file that can be duplicated or falsified. As with counterfeit money, such double-spending leads to inflation by creating a new amount of copied currency that did not previously exist. This devalues the currency relative to other monetary units or goods and diminishes user trust as well as the circulation and retention of the currency. Fundamental cryptographic techniques to prevent double-spending, while preserving anonymity in a transaction, are blind signatures and, particularly in offline systems, secret splitting.

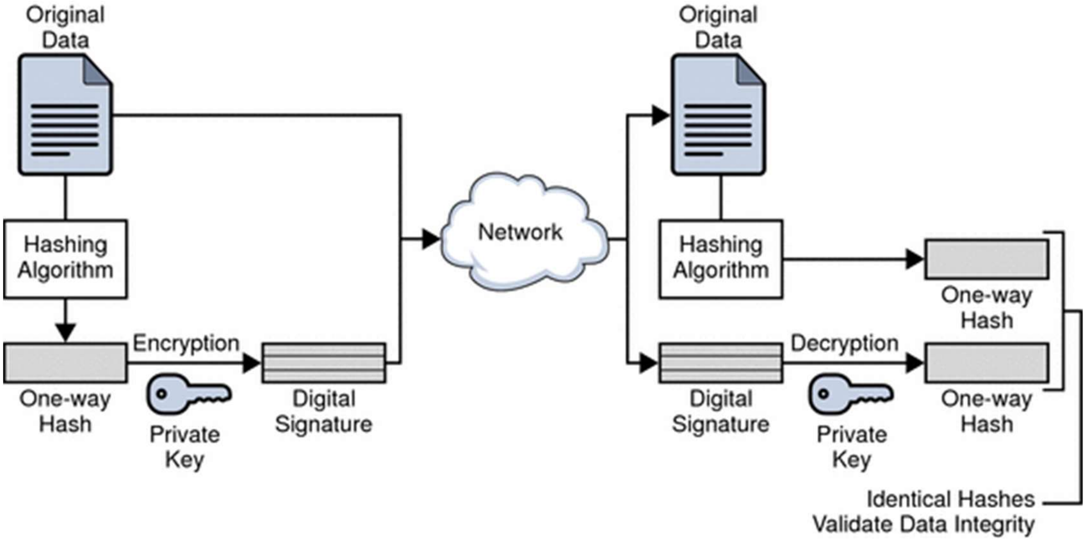
[1.13] Centralized Vs. Decentralized Vs. Distributed



Centralized systems are systems that use client/server architecture where one or more client nodes are directly connected to a central server. This is the most commonly used type of system in many organizations where a client sends a request to a company server and receives the response. In ***decentralized systems***, every node makes its own decision. The final behaviour of the system is the aggregate of the decisions of the individual nodes. Note that there is no single entity that receives and responds to the request. In ***distributed systems***, every node makes its own decision. The final behaviour of the system is the aggregate of the decisions of the individual nodes. Note that there is no single entity that receives and responds to the request. [For more detail, please refer: https://berty.tech/blog/decentralized-distributed-centralized]

[1.14] What is a hash function?

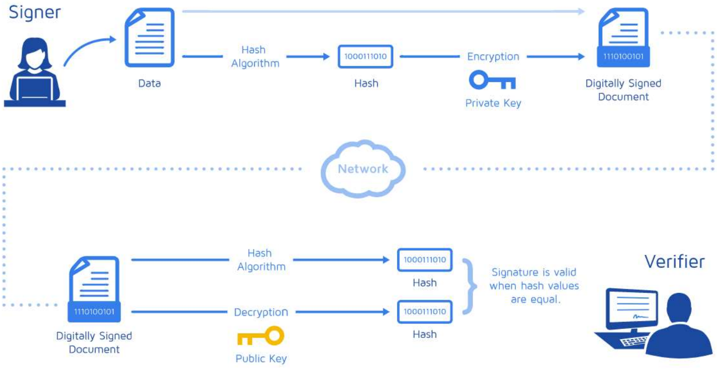




[1.15] What are the features of a hash function?

- It is deterministic so the same message always results in the same hash
- It is quick to compute the hash value for any given message
- It is infeasible to generate a message from its hash value except by trying all possible messages
- A small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value (avalanche effect)
- It is infeasible to find two different messages with the same hash value

[1.16] What is a digital signature?



A digital signature (standard electronic signature) takes the concept of traditional paper-based signing and turns it into an electronic "fingerprint." This "fingerprint," or coded message, is unique to both the document and the signer and binds both of them together. The digital signature ensures the authenticity of the signer. Any changes made to the document after it is signed invalidate the signature, thereby protecting against signature forgery and information tampering. Digital signatures help organizations sustain signer authenticity, accountability, data integrity and non-repudiation of electronic documents and forms.

[1.17] Actors Involved in Blockchain Solution

There are some actors which are involved to develop a Blockchain solution, they are classified into 8 types:

Blockchain Architect: Responsible for architecture and design of the Blockchain. Blockchain Architect is the one who is going to design, how the Blockchain solution is going to be built. He will figure out what is some information that needs to get stored, what are the transactions and the business logic that needs to be embedded onto the network, and so on.

Blockchain Developer: The developer of applications and smart contracts that interact with the Blockchain and are used by the Blockchain users. The Blockchain developer is the one who is going to take what has been an architect and then develop the actual code that will run on the Blockchain network itself.

Blockchain Network Operator: Manages and monitors the Blockchain network. Each sub-work or the business in the network has a Blockchain network operator. He also runs the Blockchain network.

Traditional Processing Platforms: An existing computer system may be used by the Blockchain to augment processing. The system may also need to initiate the request to the Blockchain. Other systems send or get information that is required to build a Blockchain solution.

Traditional Data Sources: An existing computer system may provide data to influence the behavior of the smart contract. They are also part of the overall solution to store external data.

Membership Services: It manages different types of certificates, which are required to run a permission Blockchain. Membership services provide the identity for users to come and transact on the Blockchain. For example, if you open an account with the bank, they give you a username and password, a kind of login to access web services, Membership services is going to do more than that not only username and password but also give a digital certificate that will allow you to transact on the network.

Blockchain User: The business user, operating in a business network. User experiences the application of that Blockchain solution. They are not aware of Blockchain. Blockchain user is the one who is going to perform the business transactions on the Blockchain, So, these users could belong to multiple organizations that are participating in that Blockchain.

Blockchain Regulator: The overall authority is a business network. Specifically, regulators are required to read the ledger's content broadly. The Blockchain regulator is an optional one, they might have only, read-only access onto the network where they see the transactions being performed are legitimate or not, following policies or not, etc.

UNIT #2: Bitcoins

[2.1] What Is Bitcoin?

Bitcoin is a cryptocurrency, a virtual currency designed to act as money and a form of payment outside the control of any one person, group, or entity, and thus removing the need for third-party involvement in financial transactions. It is rewarded to Blockchain miners for the work done to verify transactions and can be purchased on several exchanges. Bitcoin was introduced to the public in 2009 by an anonymous developer or group of developers using the name Satoshi Nakamoto.

- Launched in 2009, Bitcoin is the world's largest cryptocurrency by market capitalization.
- Bitcoin is created, distributed, traded, and stored using a decentralized ledger system known as a Blockchain.
- Bitcoin's history as a store of value has been turbulent; it has gone through several boom and bust cycles over its relatively short lifespan.
- As the earliest virtual currency to meet widespread popularity and success, Bitcoin has inspired a host of other cryptocurrencies in its wake.

[2.2] How to Mine Bitcoin?

A variety of hardware and software can be used to mine Bitcoin. When Bitcoin was first released, it was possible to mine it competitively on a personal computer. However, as it became more popular, more miners joined the network, which lowered the chances of being the one to solve the hash. You can still use your personal computer as a miner if it has newer hardware, but the chances of solving a hash are individually being minuscule.

This is because you're competing with a network of miners that generate around 220 quintillion hashes (220 exa hashes) per second. Machines, called Application Specific Integrated Circuits (ASICs), have been built specifically for mining—can generate around 255 trillion hashes per second. In contrast, a computer with the latest hardware hashes around 100 mega hashes per second (100 million).

To successfully become a Bitcoin miner, you have several options. You can use your existing personal computer to use mining software compatible with Bitcoin and join a mining pool. Mining pools are groups of miners that combine their computational power to compete with the large ASIC mining farms.

[2.3] How Do You Buy Bitcoin?

If you don't want to mine bitcoin, it can be bought using a cryptocurrency exchange. Most people will not be able to purchase an entire BTC because of its price, but you can buy portions of BTC on these exchanges like U.S. dollars. For example, you can buy bitcoin on Coinbase by creating an account and funding it. You can fund your account using your bank account, credit card, or debit card.

[2.4] How Long Does It Take to Mine 1 Bitcoin?

It takes an average of 10 minutes for the mining network to validate a block and create the reward. The Bitcoin reward is 6.25 BTC per block.

[2.5] What Is a Nonce?

"Nonce" is a portmanteau of "number used only once." It is a number added to a hashed—or encrypted—block in a Blockchain that, when rehashed, meets the difficulty level restrictions. The nonce is the number that Blockchain miners are solving for. When the solution is found, the Blockchain miner that solves it is given the block reward.

[2.6] What is Double-Spending?

Double-spending is a potential flaw in a digital cash scheme in which the same single digital token can be spent more than once. Unlike physical cash, a digital token consists of a digital file that can be duplicated or falsified. As with counterfeit money, such double-spending leads to inflation by creating a new amount of copied currency that did not previously exist. This devalues the currency relative to other monetary units or goods and diminishes user trust as well as the circulation and retention of the currency. Fundamental cryptographic techniques to prevent double-spending, while preserving anonymity in a transaction, are blind signatures and, particularly in offline systems, secret splitting.

[2.7] How anonymous is Bitcoin?

Cryptocurrency, and Bitcoin especially, has a reputation for being a completely anonymous form of payment, free from tracking and interference. However, if you look a little closer, you'll see that these digital currencies reveal a lot more information about you than you might think.

The main issue with Bitcoin is with its wallet, where your Bitcoin is stored. Cryptocurrency wallets are generally pseudonymous rather than anonymous. Anonymity is about being "nameless"—it comes from the Greek word for "without name"—but instead, your wallet gives you a fake name, a pseudonym. Instead of "Mark Twain," you get some scrambled numbers and letters, but the idea is the same.

Despite the Bitcoin Project itself disclosing this information on its website, plenty of people have taken the scrambled nature of their wallet addresses to mean that payments can't be tracked. That's the point behind using a fake name, after all. But your Bitcoin wallet address can be tracked, and rather simply, too: It's right there in the way that the system is set up.

[2.8] Are cryptocurrency transactions actually anonymous?

Since the original 2008 white paper introducing Blockchain technology, bitcoin and other cryptocurrency transactions have been touted as completely anonymous and private. But how anonymous are crypto transactions really?

Because cryptocurrency allows for direct peer-to-peer transactions made via the internet, the idea is that only two parties are involved in the activity. No banks, governments or intermediaries are necessary. Although this appears to set up the perfect framework for privacy and anonymity, this year's bust and other examples paint a different picture of crypto transactions.

[2.9] Are bitcoin transactions anonymous?

No. Bitcoin transactions can be traced, as demonstrated by the recent bust in Manhattan as well as last year's Colonial Pipeline hack, in which authorities were able to recoup some of the ransom payment from the attackers.

[2.10] What are the features of bitcoin script?

Script is a Forth-like, stack-based, reverse-polish, Turing incomplete programming language.

Stack-based: Bitcoin Script uses a data structure that can be thought of as a linear structure represented by a physical stack or pile. Items at the top of the stack can be added (pushed) or removed (popped) in a "Last In, First Out (LIFO)" queue.

Forth-Like: Script resembles Forth, a programming language that first appeared in 1970. Forth is used in the Open Firmware Bootloader, space applications (including the Philae spacecraft), and a variety of other embedded systems involving interactions with hardware.

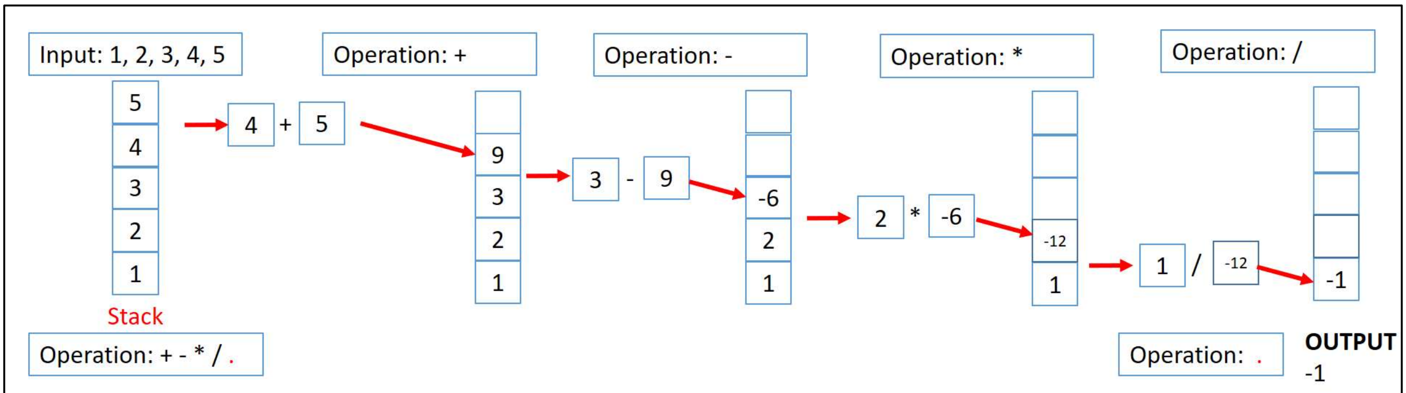
Reverse-Polish Notation (RPN): Also known as postfix notation, RPN is a method of placing the operation function at the end of a sentence. For example, adding 5 and 6 in Script must be written as "5 6 +" rather than "5 + 6."

Turing Incomplete: It means that Script for Bitcoin and other cryptocurrencies does not allow infinite loops. This has both advantages and disadvantages. One advantage of using a Turing incomplete language is the inability to run malformed scripts, regardless if they are intentional malicious attacks or unintentional programming errors. Essentially, Script is able to prevent the halting problem. Other Blockchains developed since Bitcoin have mainly chosen to be Turing Complete, or at least have a high degree of Turing completeness. Although this potentially brings the halting problem into play, it also provides better support for the complex logic required for developing smart contracts.

FORTH (https://www.forth.com/starting-forth/**)**

- Developed by Chuck Moore in 1970
- Stack based programming language, Reverse Polish Notation

To download SwiftForth, go to https://www.forth.com/download/



Operation: 18 5 mod .

OUTPUT

3

Operation: ." Hello World"

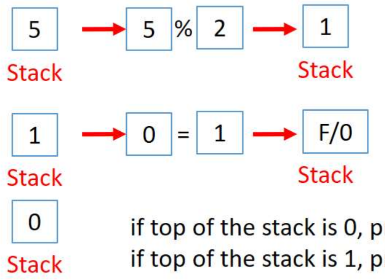
OUTPUT

Hello World

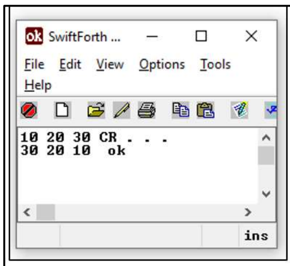
Operation: : even 2 mod 0 = if . " even" else . " odd" then ;

OUTPUT

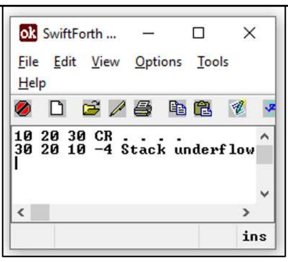
Odd



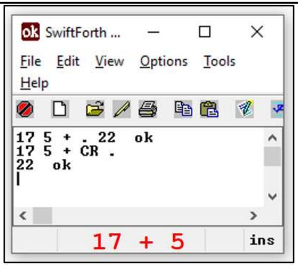
if top of the stack is 0, print ODD else
if top of the stack is 1, print EVEN



```
10 20 30 CR . . .
30 20 10  ok
```

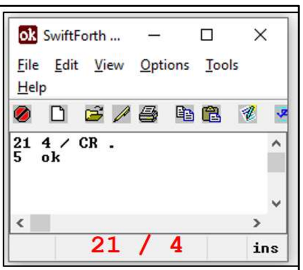


```
10 20 30 CR . . . .
30 20 10 -4 Stack underflow
```



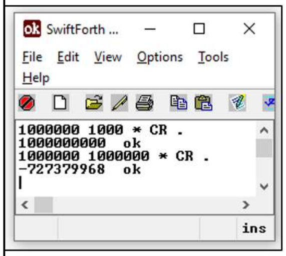
```
17 5 + . 22  ok
17 5 + CR .
22  ok
```

17 + 5

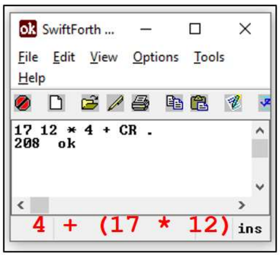


```
21 4 / CR .
5  ok
```

21 / 4

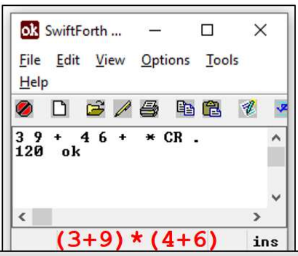


```
1000000 1000 * CR .
1000000000  ok
1000000 1000000 * CR .
-727379968  ok
```



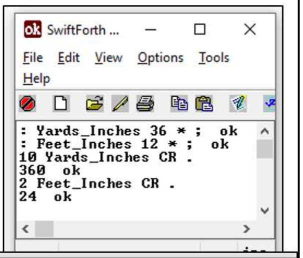
```
17 12 * 4 + CR .
208  ok
```

4 + (17 * 12)

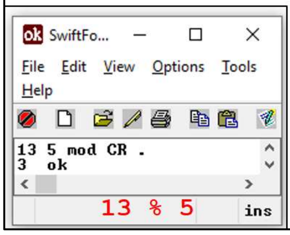


```
3 9 +  4 6 +  * CR .
120  ok
```

(3+9)*(4+6)

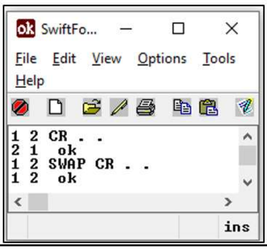


```
: Yards_Inches 36 * ;  ok
: Feet_Inches 12 * ;  ok
10 Yards_Inches CR .
360  ok
2 Feet_Inches CR .
24  ok
```

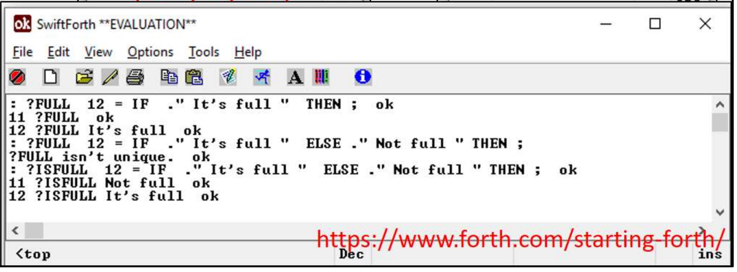


```
13 5 mod CR .
3  ok
```

13 % 5

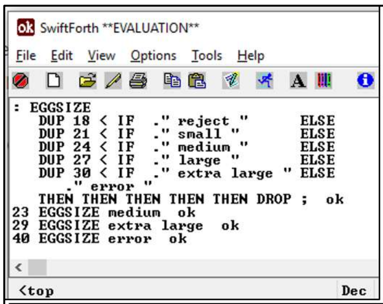


```
1 2 CR . .
2 1  ok
1 2 SWAP CR . .
1 2  ok
```

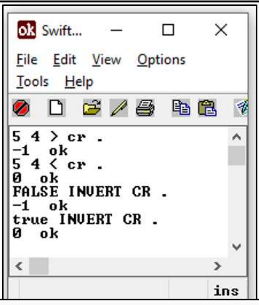


```
: ?FULL  12 = IF  ." It's full "  THEN ;  ok
11 ?FULL  ok
12 ?FULL It's full  ok
: ?FULL  12 = IF  ." It's full "  ELSE ." Not full " THEN ;
?FULL isn't unique.  ok
: ?ISFULL  12 = IF  ." It's full "  ELSE ." Not full " THEN ;  ok
11 ?ISFULL Not full  ok
12 ?ISFULL It's full  ok
```

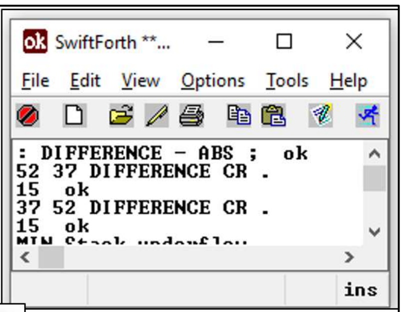
https://www.forth.com/starting-forth/



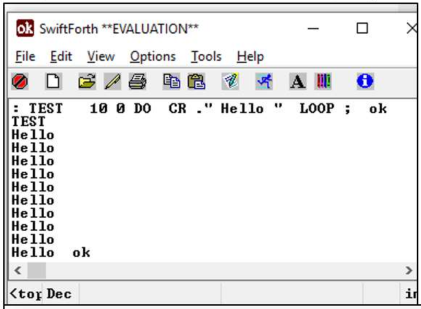
```
: EGGSIZE
   DUP 18 < IF  ." reject "       ELSE
   DUP 21 < IF  ." small "        ELSE
   DUP 24 < IF  ." medium "       ELSE
   DUP 27 < IF  ." large "        ELSE
   DUP 30 < IF  ." extra large " ELSE
      ." error "
   THEN THEN THEN THEN THEN DROP ;  ok
23 EGGSIZE medium  ok
29 EGGSIZE extra large  ok
40 EGGSIZE error  ok
```



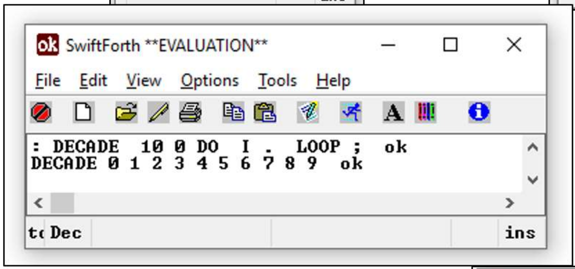
```
5 4 > cr .
-1  ok
5 4 < cr .
0  ok
FALSE INVERT CR .
-1  ok
true INVERT CR .
0  ok
```



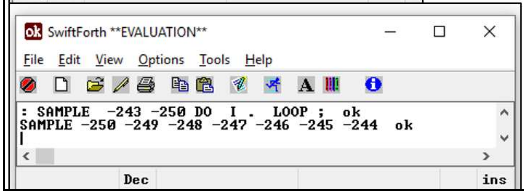
```
: DIFFERENCE - ABS ;  ok
52 37 DIFFERENCE CR .
15  ok
37 52 DIFFERENCE CR .
15  ok
MIN Stack underflow
```



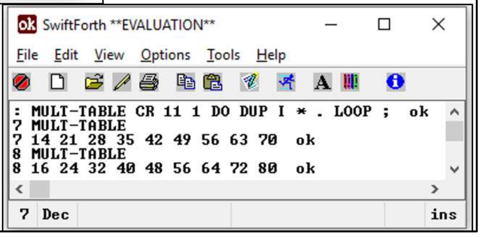
```
: TEST    10 0 DO  CR ." Hello "  LOOP ;  ok
TEST
Hello
Hello
Hello
Hello
Hello
Hello
Hello
Hello
Hello
Hello  ok
```



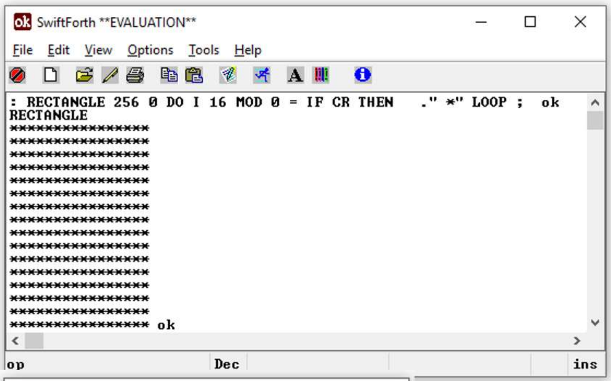
```
: DECADE  10 0 DO  I .  LOOP ;  ok
DECADE 0 1 2 3 4 5 6 7 8 9  ok
```



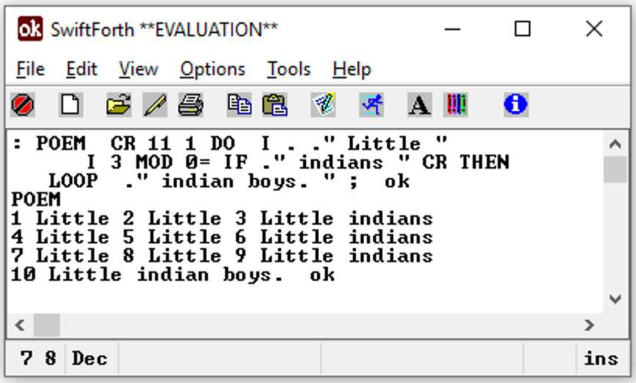
```
: SAMPLE  -243 -250 DO  I .  LOOP ;  ok
SAMPLE -250 -249 -248 -247 -246 -245 -244  ok
```



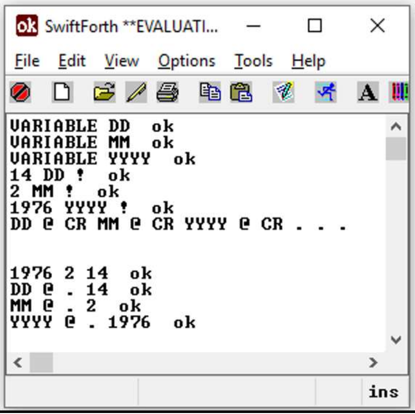
```
: MULT-TABLE CR 11 1 DO DUP I * . LOOP ;  ok
7 MULT-TABLE
7 14 21 28 35 42 49 56 63 70  ok
8 MULT-TABLE
8 16 24 32 40 48 56 64 72 80  ok
```



```
: RECTANGLE 256 0 DO I 16 MOD 0 = IF CR THEN   ." *" LOOP ;  ok
RECTANGLE
****************
****************
****************
****************
****************
****************
****************
****************
****************
****************
****************
****************
****************
****************
****************
**************** ok
```



```
: POEM  CR 11 1 DO  I . ." Little "
     I 3 MOD 0= IF ." indians " CR THEN
   LOOP  ." indian boys. " ;  ok
POEM
1 Little 2 Little 3 Little indians
4 Little 5 Little 6 Little indians
7 Little 8 Little 9 Little indians
10 Little indian boys.  ok
```

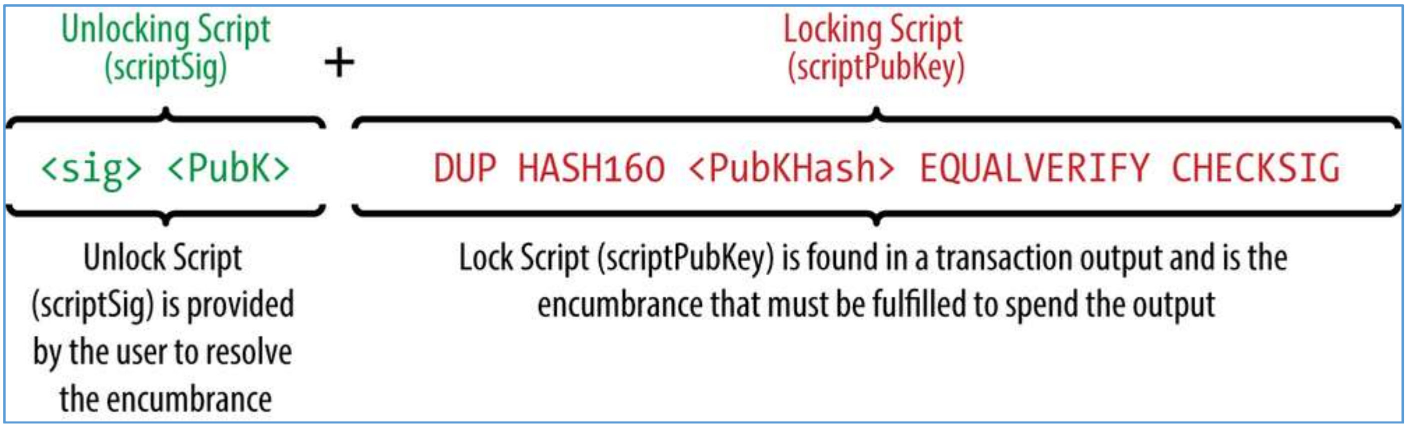


```
VARIABLE DD  ok
VARIABLE MM  ok
VARIABLE YYYY  ok
14 DD !  ok
2 MM !  ok
1976 YYYY !  ok
DD @ CR MM @ CR YYYY @ CR . . .


1976 2 14  ok
DD @ . 14  ok
MM @ . 2  ok
YYYY @ . 1976  ok
```

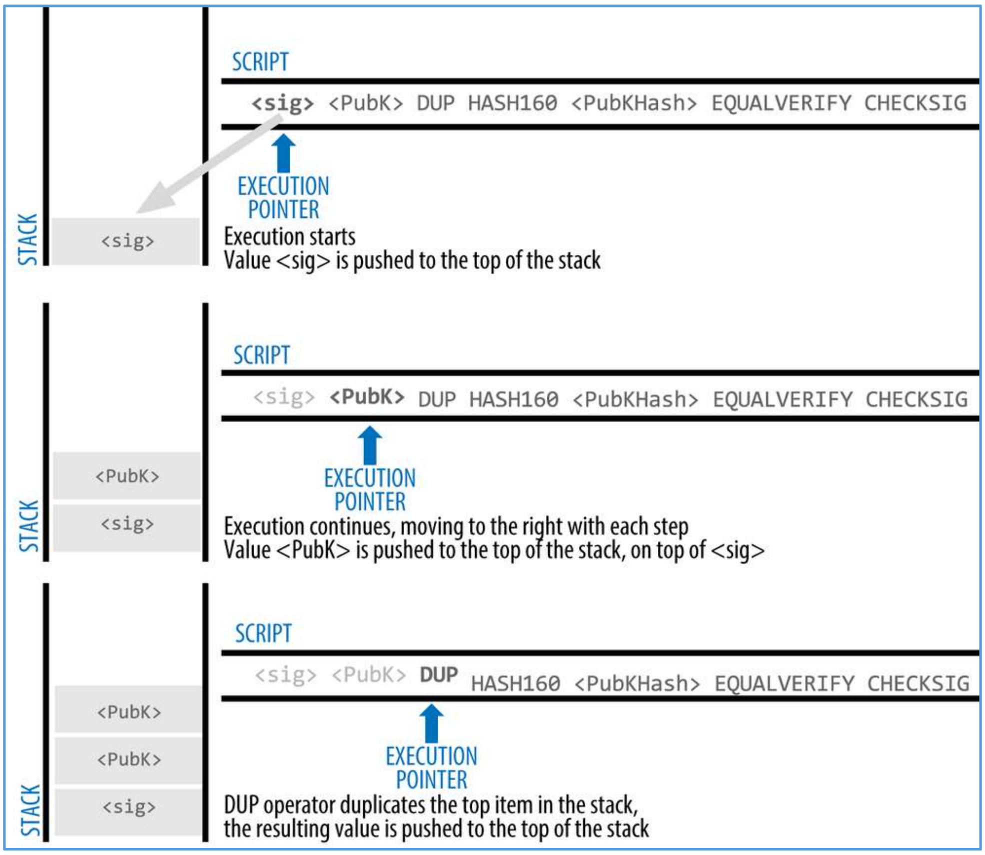
[2.11] Locking and Unlocking Script

(Source: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch05.html)



Unlock Script (scriptSig) is provided by the user to resolve the encumbrance

Lock Script (scriptPubKey) is found in a transaction output and is the encumbrance that must be fulfilled to spend the output


SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<sig>

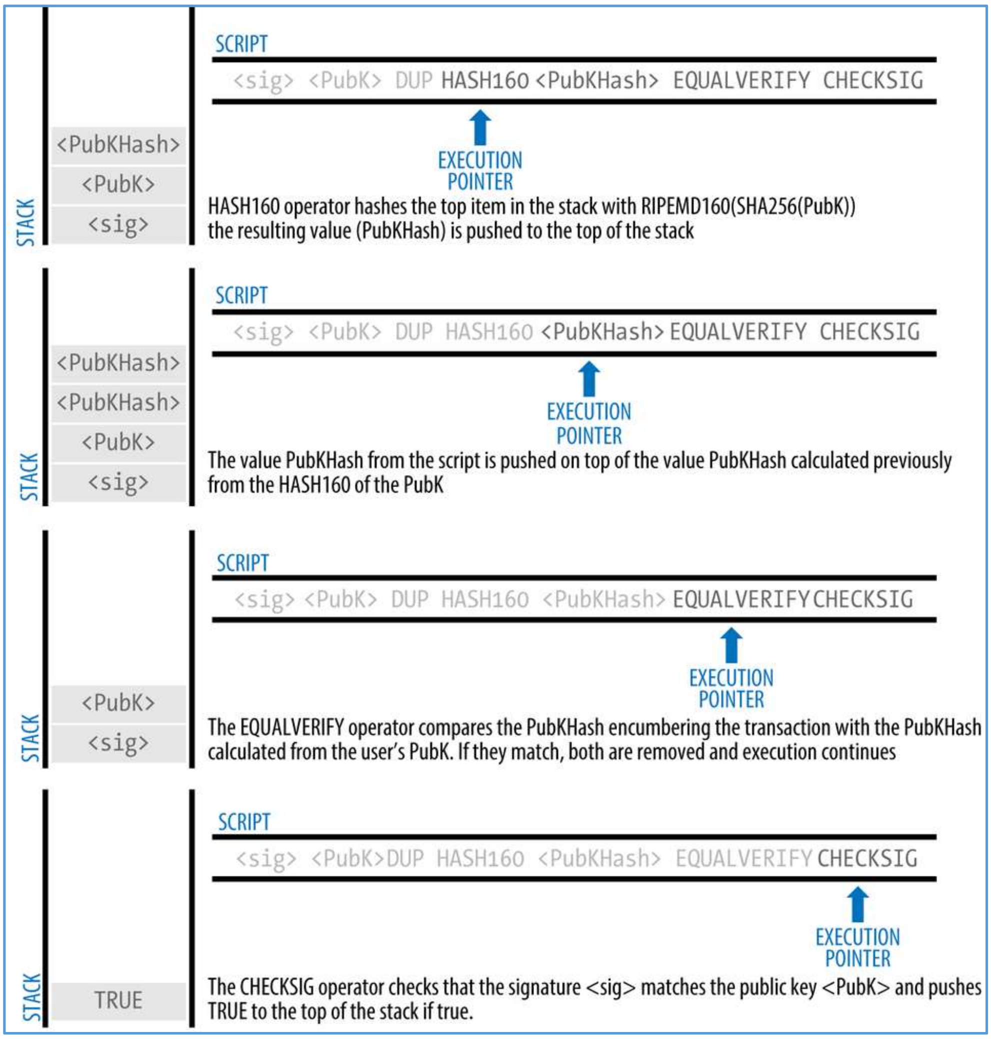
Execution starts
Value <sig> is pushed to the top of the stack

SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubK>
<sig>

Execution continues, moving to the right with each step
Value <PubK> is pushed to the top of the stack, on top of <sig>

SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubK>
<PubK>
<sig>

DUP operator duplicates the top item in the stack,
the resulting value is pushed to the top of the stack



SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubKHash>
<PubK>
<sig>

HASH160 operator hashes the top item in the stack with RIPEMD160(SHA256(PubK)) the resulting value (PubKHash) is pushed to the top of the stack

SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubKHash>
<PubKHash>
<PubK>
<sig>

The value PubKHash from the script is pushed on top of the value PubKHash calculated previously from the HASH160 of the PubK

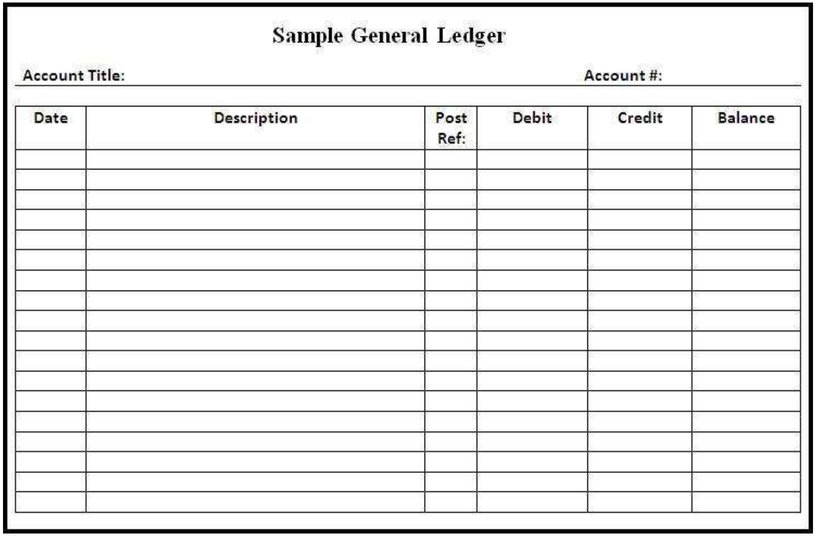
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubK>
<sig>

The EQUALVERIFY operator compares the PubKHash encumbering the transaction with the PubKHash calculated from the user's PubK. If they match, both are removed and execution continues

The CHECKSIG operator checks that the signature <sig> matches the public key <PubK> and pushes TRUE to the top of the stack if true.

UNIT #3: Introduction to Blockchain

[3.1] What is a ledger?

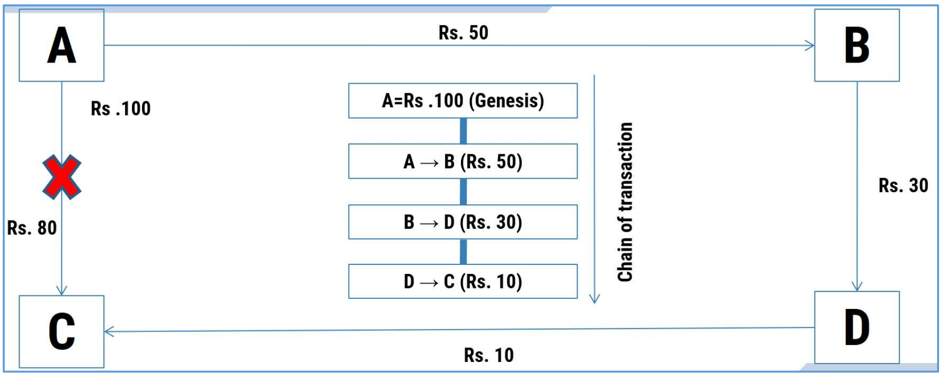


Sample General Ledger

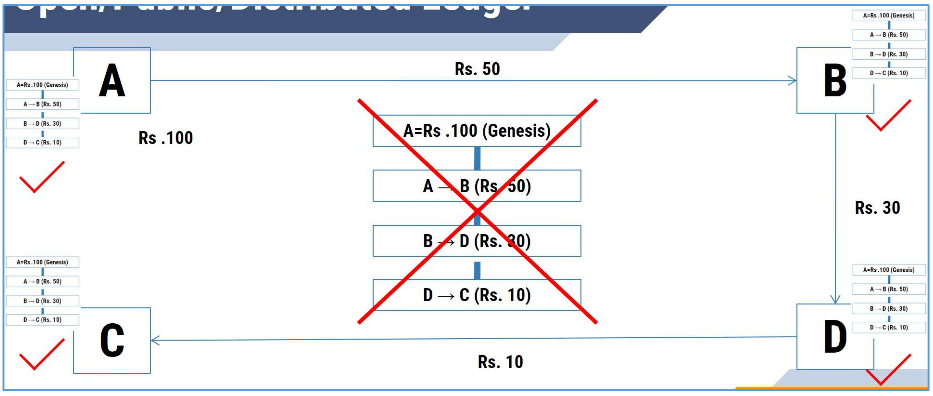
Account Title: Account #:

Date	Description	Post Ref:	Debit	Credit	Balance

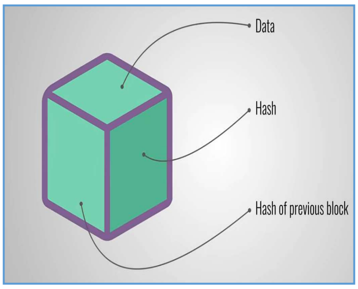
[3.2] What is a centralized ledger?



[3.3] What is a distributed ledger?

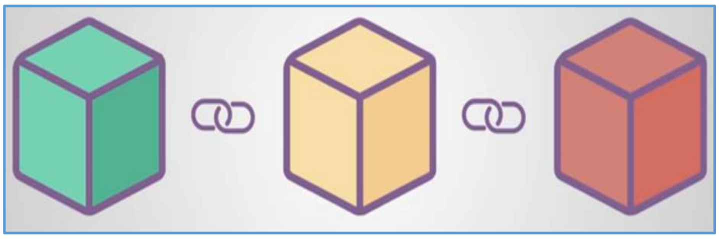


[3.4] What is a Block?

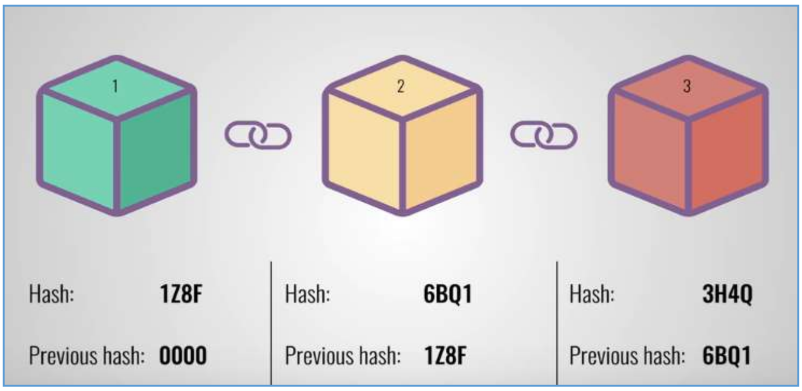


(Source: A video on "How does a Blockchain work - Simply Explained" URL: https://www.youtube.com/watch?v=SSo_EIwHSd4)

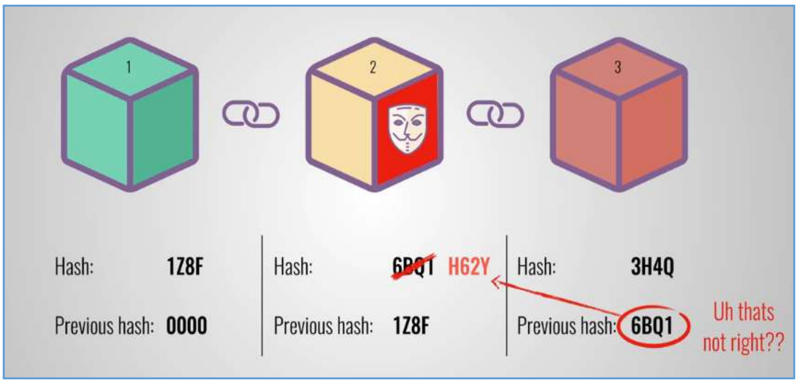
[3.5] What is a chain?



[3.6] How blocks are chained?



[3.7] How tempering in any block is detected?



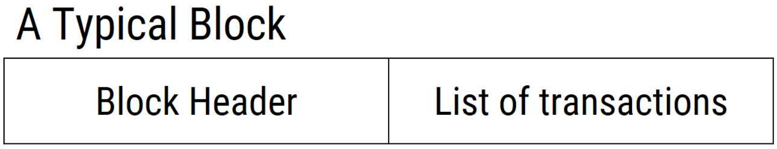
[3.8] What are Blockchains?

They are immutable digital ledger systems implemented in a distributed fashion (i.e. without a central repository) and usually without a central authority. (Source: NIST Draft [PNISTIR 8202 (DRAFT)] Published in January 2018)

[3.9] What is a typical block structure in bitcoin?

For bitcoin, a typical block structure contains:
- Number of average transaction: >500
- Average Size 1 MB (May grow upto 8MB+)

(Larger the block size, more the transactions which can be accommodated and processed at a time)



[3.10] What is distributed consensus?

The distributed consensus problem deals with reaching agreement among a group of processes connected by an unreliable communications network. [Laura Nolan (Google)]

[3.11] What is permissioned model?

Only a restricted set of users have the rights to validate the block transactions. (aka private)

- Decentralization
- Transparency
- Governance
- Tokens
- Scalability and Performance
- Privacy

Algorithms

- **Synchronous N/w**
  - RAFT
  - Paxos
  - BFT (Byzantine Fault Tolerance)
- **Asynchronous N/w**
  - PBFT (Practical BFT)
  - DBFT (Delegated BFT)
  - FBFT (Federated BFT)

[3.12] What is permission-less model?

Anyone can join the network, participate in the process of block verification to create consensus and also create smart contracts. (aka public)

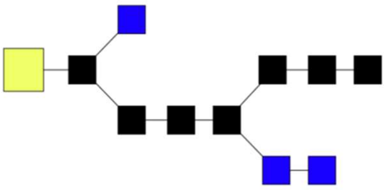
- Decentralization
- Transparency
- Governance
- Tokens
- Scalability and Performance
- Anonymity

Algorithms

- Proof of Work(PoW) (E.g. Bitcoin)
- Proof of Stake (PoS) (E.g. Ethereum)
- Proof of Activity (PoA)
- Proof-of-Location (PoL)
- Proof-of-Importance (PoI)
- Proof-of-Elapsed-Time (PoET)

[3.13] What is orphan block in Blockchain?

An orphan block is a block that has been solved within the Blockchain network but was not accepted by the network. There can be two miners who solve valid blocks simultaneously. The network uses both blocks until one chain has more verified blocks than the other. Then, the blocks in the shorter chain are orphaned.



b

[3.14] What is block propagation in Blockchain?

Block Propagation Problem in Blockchains is a well-known bottleneck that prevents Bitcoin from scaling. Block propagation time is an average time that is needed for the new block to reach the majority of nodes in the network.

Bitcoin's P2P network is formed of miner nodes where the nodes randomly connect with each other. Transactions and blocks are transmitted over this network by these nodes, until each has received the message. For a message to be diffused through the network, the transaction travel in hops. With each iteration a set of 2 nodes are sent the message, and the network diffusion grows by a factor of 2^n. The diffusion increases exponentially as the hops increase, and after 12–15 hops, the entire network receives the message.

Blockchain throughput is measured by the number of transactions per second that it can support and is measured as

Throughput = [Transactions/Block] x [Blocks/second]

where Transactions/Block is a factor of Bitcoin's current block capacity and average transaction size

Transactions/Block = Bitcoin capacity /average Transaction size

The current Block capacity for Bitcoin is 1MB for a Block interval of 10 minutes and given the average transaction size of nearly 540 bytes, the Bitcoin network currently processes ~1950 transactions per Block, which translates to ~3 transactions per second (TPS).

To increase the throughput one can either increase the Transactions/Block or Blocks/second.

A lot of work has already gone into increasing the number of transactions per block using both on-chain and off-chain methods. To increase the capacity by a factor of 10x, teams have tried increasing the block size by x10. An increased block-size generally keeps the number of hops intact — 12–15 hops for the whole network, but requires sending a larger block (1 * 10MB) over the Bitcoin link. Although the transaction/block here increases, but it leads to the issue of network throttle, increasing the propagation time by a factor of 10x, further opening up an even more critical debate of Bitcoin forks. The hard-fork of Bitcoin into Bitcoin Cash stands testimony to one such attempt.

Blocks/second on the other hand is another significant area of consideration for network scaling, but till date has been oft-neglected due to several throttling factors. The current system of gossip that determines travel time in Network plane, is certainly inefficient for its lack of features like latency optimization, pipelining, redundancy, message losses, congestion, and others, which hinders Bitcoin's network stack from reaching the per-node link bandwidth.

[3.15] What is mining in Blockchain/Cryptocurrency?

Bitcoin mining is the process of creating new bitcoin by solving puzzles. It consists of computing systems equipped with specialized chips competing to solve mathematical puzzles. The first bitcoin miner (as these systems are called) to solve the puzzle is rewarded with bitcoin. The mining process also confirms transactions on the cryptocurrency's network and makes them trustworthy.

UNIT #4: Consensus

[4.1] What is consensus for Blockchain?

Consensus for Blockchain is a procedure in which the peers of a Blockchain network reach agreement about the present state of the data in the network. Through this, consensus algorithms establish reliability and trust in the Blockchain network.

[4.2] Why Blockchains need consensus mechanisms?

Consensus mechanisms form the backbone of all cryptocurrency Blockchains, and are what make them secure. A Blockchain is a decentralized, distributed, and oftentimes public digital ledger that is used to record transactions. Each of these transactions is recorded as a 'block' of data, which needs to be independently verified by peer-to-peer computer networks before they can be added to the chain. This system helps to secure the Blockchain against fraudulent activity and addresses the problem of 'double-spending'. In order to guarantee that all participants ('nodes') in a Blockchain network agree on a single version of history, Blockchain networks like Bitcoin and Ethereum implement what's known as consensus mechanisms (also known as consensus protocols or consensus algorithms). These mechanisms aim to make the system fault-tolerant.

[4.3] What are consensus mechanisms?

Consensus is the process by which a group of peers – or nodes – on a network determine which Blockchain transactions are valid and which are not. Consensus mechanisms are the methodologies used to achieve this agreement. It's these sets of rules that help to protect networks from malicious behavior and hacking attacks. There are many different types of consensus mechanisms, depending on the Blockchain and its application. While they differ in their energy usage, security, and scalability, they all share one purpose: to ensure that records are true and honest.

[4.4] Explain Proof of Work (PoW)

Used by Bitcoin, Ethereum, and many other public Blockchains, proof of work (PoW) was the very first consensus mechanism created. It is generally regarded to be the most reliable and secure of all the consensus mechanisms, though concerns over scalability are rife. In PoW, miners essentially compete against one another to solve extremely complex computational puzzles using high-powered computers. The first to come up with the 64-digit hexadecimal number ('hash') earns the right to form the new block and confirm the transactions. The successful miner is also rewarded with a predetermined amount of crypto, known as a 'block reward'. As it requires large amounts of computational resources and energy in order to generate new blocks, the operating costs behind PoW are notoriously high. This acts as a barrier of entry for new miners, leading to concerns about centralization and scalability limitations. And it's not just the costs that are high. The most common criticism of PoW is the impact the electrical consumption has on the environment. (This has led many to seek more sustainable, energy-efficient consensus protocols, such as proof of stake (PoS).)

[4.5] Explain Proof of Stake (PoS)

As the name suggests, this popular method of consensus revolves around a process known as staking. In a proof of stake (PoS) system, miners are required to pledge a 'stake' of digital currency for a chance to be randomly chosen as a validator. The process is not unlike a lottery whereby the more coins you stake, the better your odds. Unlike in PoW where miners are incentivised by block rewards (newly generated coins), those who contribute to the PoS system simply earn a transaction fee. PoS is seen as a more sustainable and environmentally-friendly alternative to PoW, and one that's more secure against 51% attack. However, as the system favours entities with a higher number of tokens, PoS has drawn criticism for its potential to lead to centralisation. Prominent PoS platforms include Cardano (ADA), Solana (SOL), and Tezos (XTC).

[4.6] Explain Proof of Burn (PoB)

Another more sustainable alternative to Bitcoin's PoW algorithm is proof of burn (PoB). In PoB, miners gain the power to mine a block by 'burning' (destroying) a predetermined amount of tokens in a verifiable manner – namely, sending them to an 'eater address' where they cannot be recovered or spent. The more coins burned, the greater the chances of being randomly selected.

Unlike in PoS where miners are able to retrieve or sell their locked coins should they ever leave the network, burned coins are irretrievably lost. This method of requiring miners to sacrifice short-term wealth in order to gain the lifetime privilege to create new blocks helps to encourage long-term commitment from miners. The act of burning coins also leads to coin scarcity, limiting inflation and driving up demand. Cryptocurrencies that use the proof of burn protocol include Slimcoin (SLM), Counterparty (XCP), and Factom (FCT).

[4.7] Explain Proof of Elapsed Time (PoET)

Usually used on permissioned Blockchain networks (those that require participants to identify themselves), proof of elapsed time (PoET) leverages trusted computing to enforce random waiting times for block construction. It was developed by Intel in early 2016 and is based on a special set of CPU instructions called Intel software guard extensions (SGX). A time-lottery-based consensus algorithm, PoET works by randomly assigning different wait times to every node in the network. During the waiting period, each of these nodes goes to 'sleep' for that specified duration. The first to wake up (that is, the one with the shortest waiting time) is awarded the mining rights. This randomization guarantees that every participant is equally as likely to be the winner, ensuring fairness within the network. The PoET consensus mechanism is highly efficient, less resource-intensive, and scalable. It has been implemented in Hyperledger's Sawtooth.

[4.8] Explain DDOS attack in Blockchain

A Distributed Denial-of-Service (DDOS) attack in computing is an attack, where a perpetrator seeks to make a network resource unavailable to its users, by flooding the network with a large number of requests in an attempt to overload the system. It is an attack that not only Blockchains but any online service can suffer from.

In a simple form, the DOS (Denial-of-Service) attack, all these requests originate from the same source. This makes it somewhat easy to prevent. If a single IP-address sends a huge amount of requests that cannot be justified by legitimate reasons, you can have a measure in place that automatically blocks this IP-address. In the case of a DDOS attack, the distributed part refers to a large number of different sources that the malicious requests originate from.

A DDOS attack is much harder to tackle because to do so you need to differentiate between legitimate and malicious requests. This is a very hard problem. In the context of Blockchains, this comes down to an almost ideological question. The motivation to introduce transaction fees was to eliminate spam. Some people argue that as long as the requests have a transaction fee attached they cannot be considered spam by definition.

While there are certainly situations where you could consider transactions to be spammy, it would be a slippery slope to start blocking them. One of the greatest value propositions of public Blockchains is their censorship resistance. Starting to pick transactions that are not included - no matter what criteria this censorship is based on - would be a dangerous precedent for any Blockchain.

[4.9] Explain Sybil attack in Blockchain

A Sybil Attack is an attempt to manipulate a P2P network by creating multiple fake identities. To the observer, these different identities look like regular users, but behind the scenes, a single entity controls all these fake entities at once. This type of attack is important to consider especially when you think about online voting. Another area where we are seeing Sybil attacks is in social networks where fake accounts can influence the public discussion.

Another possible use for Sybil attacks is to censor certain participants. A number of Sybil nodes can surround your node and prevent it from connecting to other, honest nodes on the network. This way one could try to prevent you from either sending or receiving information to the network. This “use case” of a Sybil attack is also called Eclipse Attack.

One way to mitigate Sybil attacks is to introduce or raise the cost to create an identity. This cost must be carefully balanced. It has to be low enough so that new participants aren’t restricted from joining the network and creating legitimate identities. It must also be high enough that creating a large number of identities in a short period of time becomes very expensive.

In PoW Blockchains, the nodes that actually make decisions on transactions are the mining nodes. There is a real-world cost, namely buying the mining hardware and consuming electricity, associated with creating a fake “mining-identity”. Additionally, having a large number of mining nodes still doesn’t suffice to influence the network meaningfully. To do that you would also need large amounts of computational power. The associated costs make it hard to Sybil attack Proof-of-Work Blockchains.

[4.10] Explain Double Spending / 51% attack in Blockchain

The best-known type of attack on public PoW Blockchains is the 51% attack. The goal of a 51% attack is to perform a double spend, which means spending the same UTXO (unspent transaction output) twice. To perform a 51% attack on a Blockchain, you need to control a majority of the hash rate, hence the name. A malicious miner wanting to perform a double spend will first create a regular transaction spending their coins for either a good or for a different currency on an exchange. At the same time, they will begin mining a private chain. This means they will follow the usual mining protocol, but with two exceptions:

First, they will not include their own transaction spending their coins in their privately mined chain.

Second, they will not broadcast the blocks they find to the network, therefore we call it the private chain.

If they control a majority of the computing power, their chain will grow faster than the honest chain. The Longest Chain Rule in PoW Blockchains governs what happens in case of such a fork. The branch that has more blocks to it and accordingly represents the chain created with a larger amount of computing power is considered the valid chain.

Once the attacker has received the good or other currency bought with their coins, they will broadcast the private branch to the entire network. All honest miners will drop the honest branch and start mining on top of the malicious chain. The network treats the attacker’s transaction as if it never happened because the attacker did not include it in his malicious chain. The attacker is still in control of their funds and can now spend them again.

UNIT #5: Mining

[5.1] What Does Mining Mean?

Mining, in the context of Blockchain technology, is the process of adding transactions to the large distributed public ledger of existing transactions, known as the Blockchain. The term is best known for its association with bitcoin. Bitcoin mining is the process by which new bitcoins are entered into circulation. Bitcoin mining rewards people who run mining operations with more bitcoins.

[5.2] How does mining work?

Specialized computers perform the calculations required to verify and record every new bitcoin transaction and ensure that the Blockchain is secure. Verifying the Blockchain requires a vast amount of computing power, which is voluntarily contributed by miners.

Bitcoin mining is a lot like running a big data center. Companies purchase the mining hardware and pay for the electricity required to keep it running (and cool). For this to be profitable, the value of the earned coins has to be higher than the cost to mine those coins.

What motivates miners? The network holds a lottery. Every computer on the network races to be the first to guess a 64-digit hexadecimal number known as a “hash.” The faster a computer can spit out guesses, the more likely the miner is to earn the reward.

The winner updates the Blockchain ledger with all the newly verified transactions – thereby adding a newly verified “block” containing all of those transactions to the chain – and is granted a predetermined amount of newly minted bitcoin. (On average, this happens every ten minutes.) As of late 2020, the reward was 6.25 bitcoin – but it will be reduced by half in 2024, and every four years after. In fact, as the difficulty of mining increases, the reward will keep decreasing until there are no more bitcoin left to be mined.

There will only ever be 21 million bitcoins. The final block should theoretically be mined in 2140. From that point forward, miners will no longer rely on newly issued bitcoin as reward, but instead will rely on the fees they charge for making transactions.

[5.3] Why is mining important?

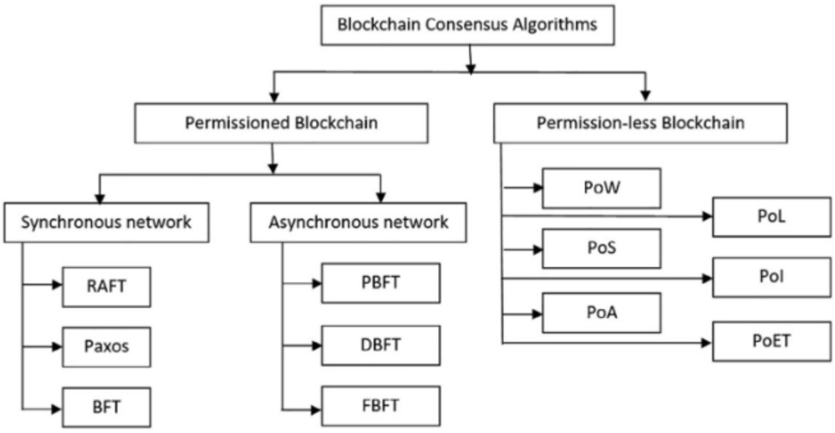
Beyond releasing new coins into circulation, mining is central to Bitcoin’s (and many other cryptocurrencies’) security. It verifies and secures the Blockchain, which allows cryptocurrencies to function as a peer-to-peer decentralized network without any need for oversight from a third party. And it creates the incentive for miners to contribute their computing power to the network.

[5.4] What is mining difficulty?

Mining difficulty refers to the difficulty of solving the math puzzle and generating bitcoin. Mining difficulty influences the rate at which bitcoins are generated. Mining difficulty changes every 2,016 blocks or approximately every two weeks. The succeeding difficulty level depends on how efficient miners were in the preceding cycle. It is also affected by the number of new miners that have joined Bitcoin's network because it increases the hash rate or the amount of computing power deployed to mine the cryptocurrency. If computational power is taken off the network, the difficulty adjusts downward to make mining easier. The difficulty level for mining in March 2022 was 27.55 trillion. That is, the chances of a computer producing a hash below the target is 1 in 27.55 trillion.

[5.5] What is the concept of Mining pool?

A mining pool is the pooling of resources by miners, who share their processing power over a network, to split the reward equally, according to the amount of work they contributed to the probability of finding a block. A "share" is awarded to members of the mining pool who present a valid partial proof-of-work. Mining in pools began when the difficulty for mining increased to the point where it could take centuries for slower miners to generate a block. The solution to this problem was for miners to pool their resources so they could generate blocks more quickly and therefore receive a portion of the block reward on a consistent basis, rather than randomly once every few years.



Permissioned Blockchain consensus mechanisms are divided into two broad categories based on the environment they work viz. (i) synchronous (ii) asynchronous Before we start understanding the protocols under the synchronous or asynchronous environment, we need to understand the idea of State Machine Replication (SMR) which is very helpful to achieve consensus in permissioned Blockchain. The smart contract can be represented through a finite state machine (FSM). A crowdfunding application is a nice example of a contract presented through FSM. Rather than running the (smart) contract on each machine/node of the network, it is recommended to run it on a (sub) set of nodes and the network makes sure that the same state is broadcasted to other nodes of the network through a certain consensus mechanism. A typical state machine is comprising of a set of states (ST) with each state having a set of inputs (IN), set of outputs (OUT), transition function (ST X IN -> ST), output function (ST X OUT -> ST) and a start state (E.g. ST1). Through distributed SMR, state machines are synchronized across multiple servers to avoid any possible breakdown.

1. Synchronous Network Environment:

[67.1] PAXOS: There are various types of faults in distributed consensus. Crash fault, network or partitioned faults, and Byzantine faults. Byzantine faults are further subdivided into malicious behavior nodes, hardware faults, and software errors. To handle crash and network faults, PAXOS and RAFT are used whereas to address Byzantine faults (including crash and network faults), BFT and PBFT are used.
The idea behind the working of PAXOS is simple. Out of total nodes in the network, one or more nodes propose a value (in the form of the proposal with a unique and constantly incrementing number) which is propagated to the entire network. These nodes are known as proposers. Other nodes (known as acceptors) either accept or reject the proposal based on comparing the number associated with the current proposal with that of the received proposal. The third category of the node knows as the learner, learns the value chosen by acceptors through the majority voting principle.

[67.2] RAFT: Primarily designed to act as an alternative to Paxos, along with the factors such as fault-tolerance and performance, RAFT mainly works on the idea of dividing the main problems into sub-problems and addressing individual sub-problem independently. Collaboratively, all nodes of the system select a leader and other nodes become followers of the leader. While selecting a leader, concept of majority voting is applied among the available candidates for leadership. The leader maintains and replicates the state transition sub-problem independently. Collaboratively, all nodes of the system select a leader and other nodes become followers of the leader. While selecting a leader, concept of majority voting is applied among the available candidates for leadership. The leader maintains and replicates the state transition (e.g. logs) among the followers. The leader keeps on informing all followers about its existence by sending a special message (called heartbeat). Followers do not issue any request on their own but simply respond to leaders' requests. Failing to receive a heartbeat from a leader (after a certain timeout), followers start a process of re-electing the leader. In case of failure or crash of a leader node, a new leader is selected (after a predefined timeout) with voting. When a failed node is recovered, it becomes the follower. Like Paxos, RAFT follows the concepts of majority voting, that is, as far as N/2 + 1 nodes are working (or in other words N/2–1 are failed nodes), it is resistant to Byzantine fault tolerance. The issue with RAFT is that the leader is supposed to be correct (or honest) as all the other nodes blindly follow the leader.

[67.3] BFT (Byzantine Fault Tolerance): The basic issue with the distributed system is to achieve reliability by agreeing upon a common consensus among various decisions taken by multiple actors of the system. This issue is momentous when there are faulty or misbehaving actors in the system which may jar the system with inconsistency. Therefore, fault tolerance is necessary for the facet of achieving consensus. To understand the concern, the Byzantine Generals Problem was described in (Lamport et al., 2019) where there are multiple army generals (one being the commander and the other being the lieutenants) communicating through a message-passing system. Various cases have been discussed by considering one or more lieutenants either loyal or traitor, including a case where the commander is also considered as loyal or traitor. The problem can be formalized as Consensus can be achieved in a system with 3 N nodes (generals) where maximum N nodes (generals) are faulty (traitor). In other words, with 66.66% (2 N/3) honest/regular/loyal nodes and 33.33% (N/3) dishonest/faulty/traitor nodes, a system can achieve consensus. Byzantine Fault Tolerance is a system which remains tolerance towards node's failure belonging to the Byzantine faults.

2. Asynchronous Network Environment

[67.4] PBFT (Practical BFT): Introduced by Castro et al. (1999), PBFT was designed for Internet type of asynchronous communication environment where there is no upper limit (in term of time) concerning when the response to a particular request will be received. It was intended to address the issues raised in the BFT mechanism (such as failure to return a result, respond with incorrect/deliberately misleading results, etc). PBFT works on the principle of state machine replication where one node is primary (master/leader) (which is selected in a round-robin fashion) and other nodes are secondary (slave/backup/follower). Like BFT, to function PBFT properly, dishonest/faulty/traitor nodes should not be greater than (N/3) where N is the total number of nodes in the network. In other words, PBFT requires 3F + 1 replicas so as to tolerate F faulty nodes. PFBT works in four phases. In the first phase, the client sends a request to the primary node which in turn broadcasts the request to secondary nodes in the second phase. All the nodes (primary and secondary) respond to the client after performing the service request in the third phase. In the last phase, the request is considered to be successful if M + 1 replies are having identical results where M is the maximum number of faulty nodes. PBFT aims to address the concerns in an energy-efficient way i.e. without going for multifarious mathematical computations. PBFT also intends to provide transaction finality i.e. once transactions have been agreed upon (or finalized), unlike PoW, they do not need multiple confirmations. Further, as all nodes in the network take part in decision making (by responding to the request) it leads to low reward variance. However, PBFT is prone to be vulnerable to Sybil attack and it does not scale well because of heavy communication cost.

[67.5] What are Smart Contracts?

A smart contract is a set of promises, specified in digital form. A smart contract is an agreement between various parties just as any traditional written contract except that smart contracts are written in computer code and are usually embedded in a Blockchain where many of the stages of the transaction are self-executing.

A unique characteristic of a smart contract is that it can be programmed to accept external input that can verify transactional steps in an automated fashion, thereby eliminating some elements of human interaction. So, rather than having to wait for pieces of paper to be signed and shuffled from hand to hand, the smart contract tracks confirmations that the terms of the contract have been fulfilled and automatically take actions, such as releasing a payment.

[67.6] How secure are smart contracts?

Blockchain is considered to be incorruptible/immutable. Once a smart contract has been concluded, it is impossible to alter any of its terms retroactively. The algorithms specified in the contracts are executed reliably and strictly the way they were programmed. But this also means that any smart contract is only as good as the underlying computer code. If the code underlying the smart contract is not secure, then the smart contract will execute this non-secure code.

[67.7] What is the role of the Blockchain in smart contracts?

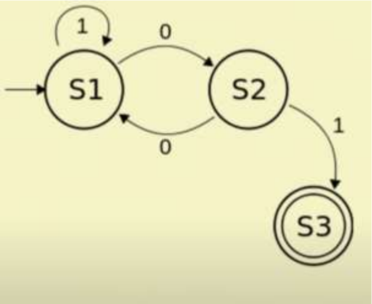
The Blockchain is integral to the function of smart contracts. A smart contract is a digital contract that is stored on the Blockchain. This contract is then automatically executed when the conditions of the contract are met. The Blockchain provides a secure and tamper-proof way to store the contract and to ensure that it is executed correctly.

[67.8] What is state machine replication? How is it useful in achieving consensus in Blockchain technology?

The state machine replication helps us to achieve a consensus in a permission model. We do not need to execute a smart contract to all the nodes. Rather, the selected subset of contract executor executes it and propagates it with other nodes to ensure the contract's status is propagated to all the nodes uniformly in the network, and they are on the same page. The distributed state machine replication technology ensures consensus in a permission Blockchain environment.

State Machine is characterized by a set of parameters such as set of Inputs, set of Outputs, and the Transition States.

- A set of state (S) based on the system design
- A set of inputs (I)
- A set of outputs (O)
- A transition function S x I –> S; takes the current state and input value and produces a set as the output.
- An output function S x I –> O
- A start state



[67.9] What is Crowdfunding?

Crowdfunding is the use of small amounts of capital from a large number of individuals to finance a new business venture. Crowdfunding makes use of the easy accessibility of vast networks of people through social media and crowdfunding websites to bring investors and entrepreneurs together, with the potential to increase entrepreneurship by expanding the pool of investors.

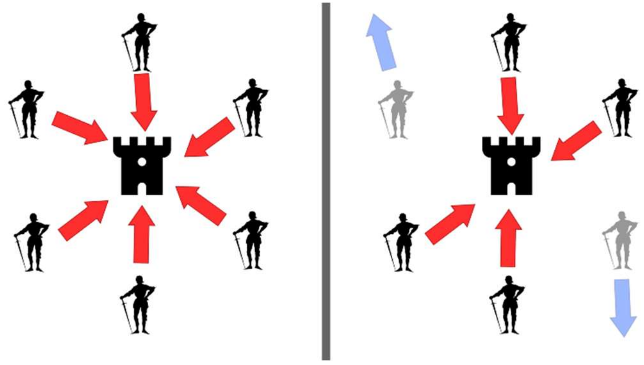
[67.10] How does Blockchain support Crowdfunding?

There are several areas where Blockchain supports and improves crowdfunding by removing the need for intermediate third party.

- Decentralization: Since block-chain is decentralized it doesn't rely on any other platforms to create funds. for starters, no longer to be obliged to any rules and any project can get visibility and funded if the investors think to invest, eliminates fees which makes crowdfunding less expensive for the creators.
- Access Equity: To provide investors equity or ownership block-chain relies on asset tokenization. For example, a person who plans to create multiple new products with the incoming funds and grant small ownerships stake in the company. This could potentially open whole new world of opportunity.
- Universal Opportunity: Any project using a block-chain-based crowdfunding model can get funded. Any person with an internet connection can contribute projects.
- Flexible Options: Using block-chain as asset tokenization grants creators and entrepreneurs more liberties. Usually asset tokens have their own currency to enable organizations to hire professionals and advertisers.
- Peer-to-Peer: The cryptocurrencies are exchangeable on a peer to peer network. This usually help the people for their investment which even generates more interest in the entire process.

[67.11] What is Byzantine General Problem?

It is a condition of a computer system, particularly distributed computing systems, where components may fail and there is imperfect information on whether a component has failed.

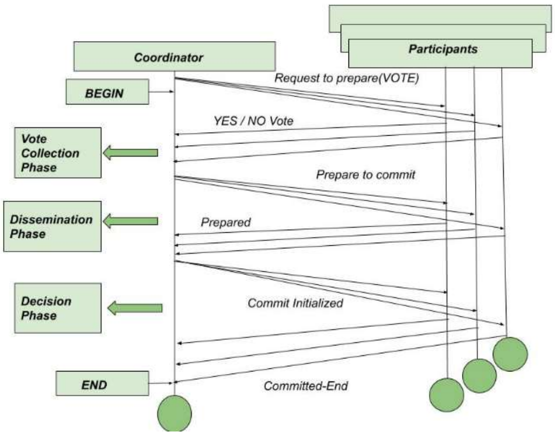


In its simplest form, a number of generals are attacking a fortress and they must decide as a group whether to attack or retreat. Some generals may prefer to attack, while others prefer to retreat. The important thing is that all generals agree on a common decision, for a half-hearted attack by a few generals would become a rout, and would be worse than either a coordinated attack or a coordinated retreat.

If all generals attack in coordination, the battle is won (left figure). If two generals falsely declare that they intend to attack, but instead retreat, the battle is lost (right figure).

[67.12] Three Phase Commit Protocol

It is an extension of the Two-Phase Commit (2PC) Protocol that avoids blocking problem. Instead of directly noting the commit decision in its persistent storage, the coordinator first ensures that at least ‘k’ other sites know that it intended to commit transaction. In a situation where coordinator fails, remaining sites are bound to first select new coordinator. This new coordinator checks status of the protocol from the remaining sites. If the coordinator had decided to commit, at least one of other ‘k’ sites that it informed will be up and will ensure that commit decision is respected. The new coordinator restarts third phase of protocol if any of rest sites knew that old coordinator intended to commit transaction. Otherwise, new coordinator aborts the transaction.



[67.13] List few Blockchain use cases.

- Banking, Insurance and Financial Market
- Smart contracts
- Internet of Things (IoT)
- Personal identity security
- Healthcare
- Logistics
- Non-fungible tokens (NFTs)
- Government
- Media and Advertising
- Supply Chain Management

[67.14] Supply Chain Management using Blockchain

Every product that reaches an end-user represents the cumulative effort of many organizations and stakeholders. These are referred to collectively as the supply chain. Organizations within a supply chain are linked through physical and information flows:

Physical flows involve the transformation, movement, and storage of goods and materials.

Information flows involve the coordination between partners to control the day-to-day flow of goods and materials up and down the supply chain; it also involves long-term planning.

The management of the product development, sourcing, procurement, production, and logistics of raw materials, products, and finished goods from one point to another is called supply chain management (SCM). Effective supply chain management can lower costs, speed up production cycles, and mitigate risk.

Blockchain technology allows companies to track all types of transactions more securely and transparently.

UNIT #9, #10: Smart Contracts / Ethereum, Research

[910.1] What do you understand about the Ethereum Network?

Ethereum operates as a Blockchain platform under the Ethereum Foundation. Instead of operating on a single computer, the Ethereum platform is an open-source software platform that uses Blockchain technology. In addition, you may use it to construct decentralized apps on top of the Ethereum Blockchain that can be monitored by thousands of peers without relying on centralized entities.

[910.2] What is Solidity? What are some important features of Solidity?

Solidity is a high-level language used in the Blockchain ecosystem for implementing smart contracts. Designed specifically for targeting Ethereum Virtual Machine, Solidity was influenced by several programming languages, such as JavaScript, Python, and C++.

Solidity has some salient features, which include libraries, contracts, and inheritance support. With Solidity, users can also create custom data types which can be a crucial part of smart contract development.

[910.3] With reference to Ethereum, explain following.

- Token: Ether (ETH)
- Wei and Ether: 1 ETH = 10^18 Wei
- Average block time: ~14 seconds
- Average block size: Around 2KB
- How do you get Ethers?
- There are a few ways: 1. Become a miner 2. Trade other currencies 3. Ether faucets like https://faucet.metamask.io 4. Receive Ethers from others
- Where do Ethers come from? 60 million were first created in a presale in 2014. Also, ethers are created when a block is mined.
- What is a node? A node is essentially a computer, connected to the network, which processes transactions.
- What are some ways to interact with a network? Wallet or a DApp
- Where are transactions recorded? In the public ledger.
- Why would you have a private network? There are many reasons, but mainly because of data privacy, performances, distributed database, permissions control and testing.
- How can you easily see details about transactions and blocks? Using blockchain explorers like etherscan.io or live.ether.camp
- What about private network? You can do it using open source explorer clients (like https://github.com/etherparty/explorer)
- What consensus model does Ethereum use? Shifted from PoW to PoS
- How can you mine Ethers? Using a wallet or geth cli
- What is used to sign transactions? User's private key.

[910.4] Ethereum Virtual Machine (EVM)

It is designed as the runtime environment for smart contracts in Ethereum. It is sandboxed and isolated from the other parts of the system. This means that any operation on EVM should not affect your data or programs in any way, no matter how many times you call a particular function on it.

The Ethereum Virtual Machine (EVM) is a Turing complete programmable machine, which can execute scripts to produce arbitrary outcomes. It has been built with the purpose of being a “world computer” and has immense power. The Ethereum Virtual Machine makes the process of creating new tokens on Ethereum Blockchain easy. Here, script means a set of instructions or an algorithm which tells the computer what it needs to do in order for something to work properly. The EVM requires that one has access over any network node so as to be able to execute the desired commands and create new tokens on the Blockchain without any difficulties.

[910.5] Blockchain Research

Refer following sites to see the latest research in Blockchain Technology

- https://ieeexplore.ieee.org/
- https://www.acm.org/
- https://www.sciencedirect.com/
- https://www.elsevier.com/