

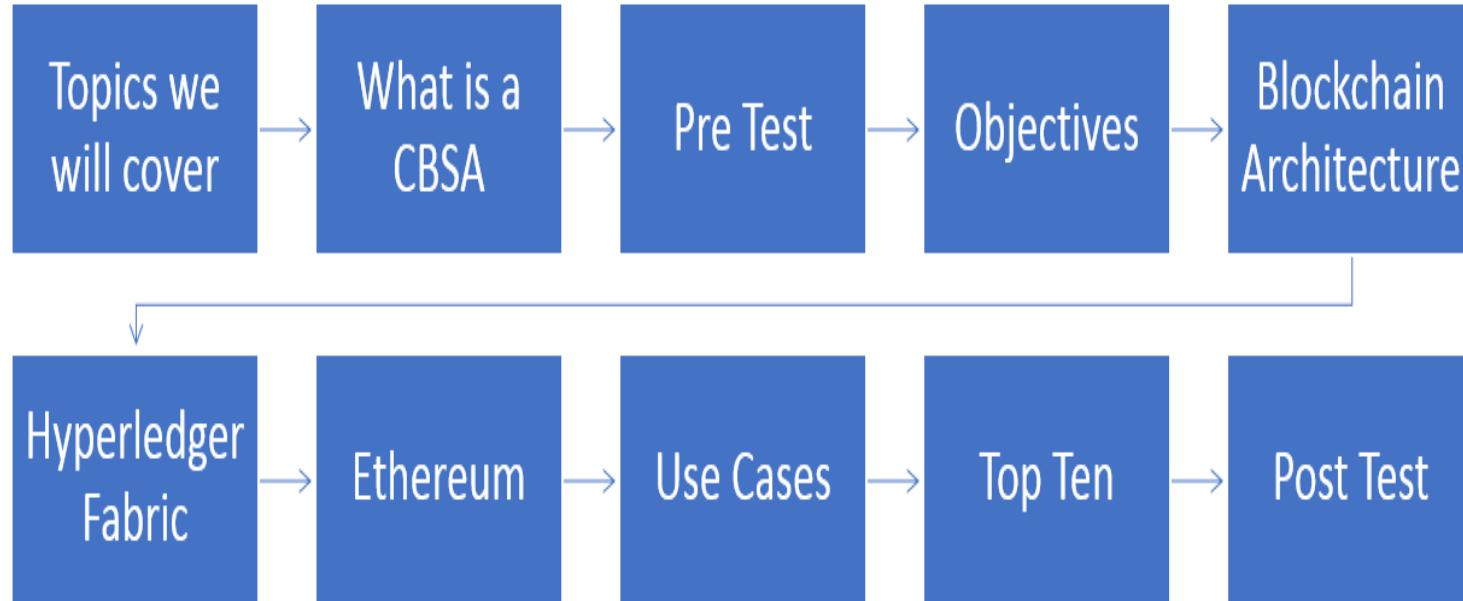


CBSA Crash Course

Certified Blockchain Solutions Architect Crash Course

Exam as 01/19/2019

CBSA Exam Crash Course



CBSA Exam Crash Course



Course Expectations



Engineers/Architects with basic knowledge in programming, IT networking and IT architecture



Basic understanding of Golang, Java, or Javascript would be helpful but not needed for this foundations course



Recommended preparation:



Basic Blockchain knowledge, which can be gained by watching Introducing Blockchain LiveLessons

CBSA Exam Crash Course

Course Audience

Course is geared towards enterprise customers that are already considering “Permissioned” blockchains such as Hyperledger Fabric

Course is mainly for Architects, Engineers, PreSales.

Some focus for developers and programmers but not a development course or coding course.

CBSA Exam Crash Course

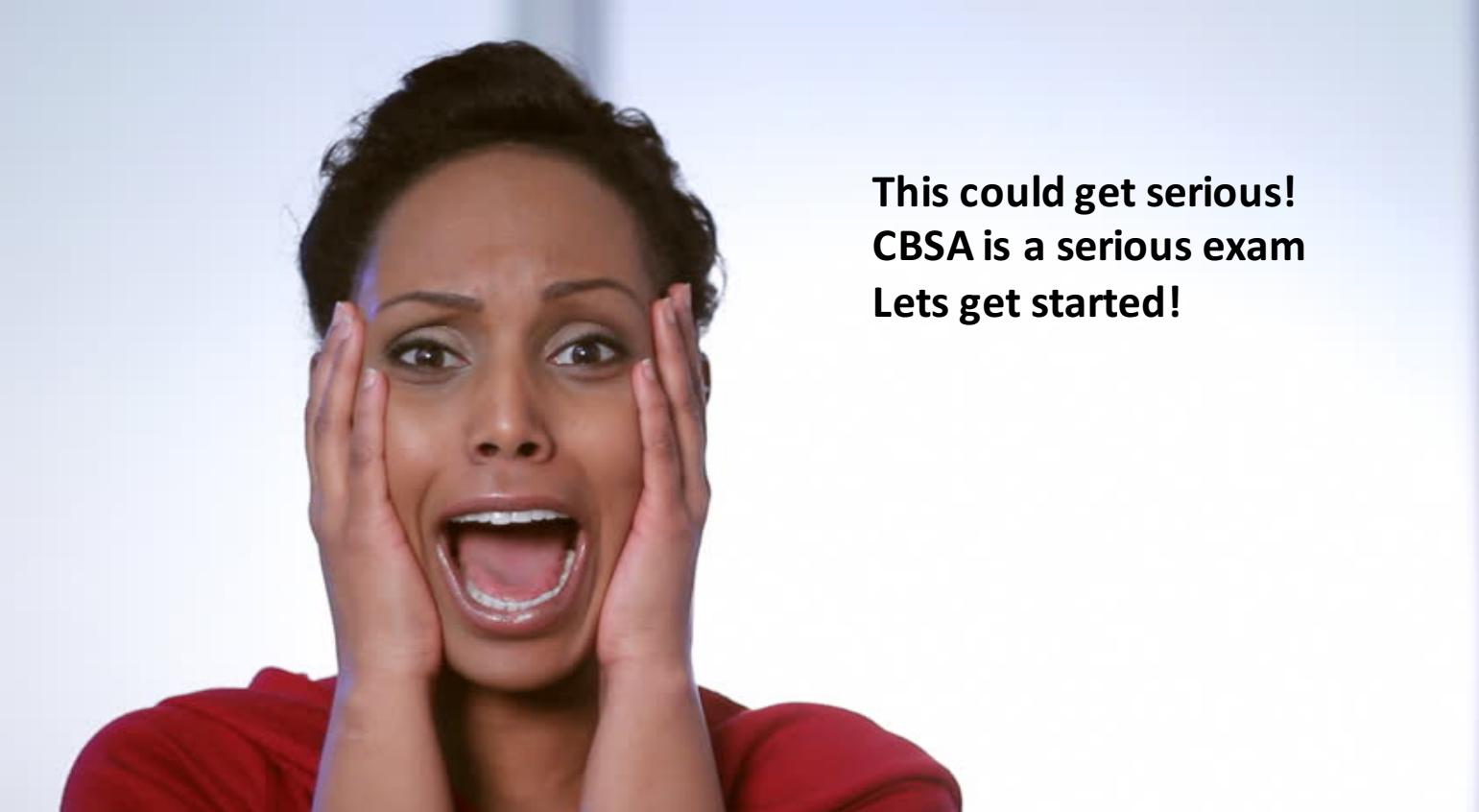
What you'll learn-and how you can apply it

- CBSA Exam Objectives
- Blockchain Basics
- Blockchain Architecture
- Hyperledger Fabric
- Ethereum
- Smart Contracts
- Top Ten Thing to Study
- Lots of practice questions

CBSA Exam Crash Course

Lots of Practice Questions Provided

CBSA Exam Crash Course



**This could get serious!
CBSA is a serious exam
Lets get started!**

CBSA Exam Crash Course

Lets Find out More about the Audience



CBSA Exam Crash Course

Survey Question

What is your current role in your company (Closest)

- **IT Infrastructure Manager**
- **C Level or Director Level**
- **Blockchain Focused/Dedicated Developer/Architect/Lead**
- **Cloud Architect/Admin**
- **Data Engineer/Big Data Engineer**
- **Developer Other than Blockchain**
- **IT Security Focused**
- **Other roles not listed**

CBSA Exam Crash Course

Survey Question

What type of company Vertical/Sector are you working for?

- **IT Consulting/Professional Services**
- **IT Vendor/VAR/Reseller**
- **Financial Sector (Banking/Payments/Investments)**
- **Energy Sector (Fossil Fuels/Solar/PetroChems)**
- **Manufacturing (Electronics/Machines/Cars/Planes)**
- **Government Employment (Federal/State/etc)**
- **Logistics (Transportation/Shipping)**
- **Real Estate (Commercial/Residential/Industrial)**
- **Other Industry Vertical Sector Not Listed**

CBSA Exam Crash Course

Survey Question

Who currently is or is planning on using Hyperledger Fabric in their enterprise environments or in the IBM BaaS?

- Yes
- No plans to at this time
- Will be in 3 Months
- Will be in 6 Months or more

CBSA Exam Crash Course

What is a CBSA?

CBSA Exam Crash Course

- The Certified Blockchain Solution Architect (CBSA) exam is an elite way to demonstrate your knowledge and skills in the Blockchain arena.
- You will become a member of a community of Blockchain leaders.



CBSA Exam Crash Course

- The Certified Blockchain Solution Architect (CBSA) exam is a professionally delivered exam which is proctored thru Pearson.
- Passing this certification will distinguish you as one that is knowledgeable from a pre sales perspective



CBSA Exam Crash Course

CBSA Exam Objectives

CBSA Exam Crash Course

- The Certified Blockchain Solution Architect (CBSA) exam has clearly defined objectives on the website.
- Before taking this exam or for that matter any exam you should review all objectives and prerequisites for preparing for the exam.



CBSA Exam Crash Course

This exam will prove that a student completely understands:

- The difference between proof of work, proof of stake, and other proof systems and why they exist
- Why cryptocurrency is needed on certain types of blockchains



CBSA Exam Crash Course

- The difference between public, private, and permissioned blockchains
- How blocks are written to the blockchain
- Where cryptography fits into blockchain and the most commonly used systems



CBSA Exam Crash Course

- The Common use cases for public blockchains
- Common use cases for private & permissioned blockchains
- What is needed to launch your own blockchain
- Common problems & considerations in working with public blockchains



CBSA Exam Crash Course

- The awareness of the tech behind common blockchains
- When is mining needed and when it is not
- Byzantine Fault Tolerance
- Consensus among blockchains
- What is hashing
- How addresses, public keys, and private keys work



CBSA Exam Crash Course

- What is a smart contract
- Security in blockchain
- Brief history of blockchain
- The programming languages of the most common blockchains
- Common testing and deployment practices for blockchains and blockchain-based apps



CBSA Exam Crash Course

Test Our Knowledge Before – Pre Test

Pre Test Question

1. What application is used by Hyperledger Fabric to communicate with the network?
 - a. JSON
 - b. Binary
 - c. **SDK**
 - d. RPC API

Pre Test Question

2. What consensus algorithm uses miners to validate transactions?
 - a. Proof of Stake
 - b. Proof of Elapsed Time
 - c. **Proof of Work**
 - d. Proof of Capacity

Pre Test Question

3. Blockchain technology is built from which of the following sets of technologies?
- a. P2P Networks, Public Key Encryption and Programs
 - b. Centralized Networks, RSA Encryption and Programs
 - c. P2P Networks, RSA Encryption and Enforcement
 - d. P2P Networks, Private Key Encryption and Contracts
 - e. Centralized Networks, RSA Encryption and Contracts

Pre Test Question

4. An X.509 certificate is used for _____
- a. certification of transaction consensus
 - b. validating node performance
 - c. the issuing of private keys
 - d. identity validation

Pre Test Question

5. Blockchain's use of cryptographic hashing provides for

-
- a. the maintaining of data integrity
 - b. making data blocks tamper proof
 - c. network security to work in unison
 - d. All of the above

Pre Test Question

6. What application is used by Hyperledger Fabric to communicate with the network?
- a. JSON
 - b. Binary
 - c. **SDK**
 - d. RPC API

Pre Test Question

7. Voting-based algorithms are advantageous because they provide _____

- A) low-latency finality
- B) high-performance
- C) low-latency consensus
- D) high-security

Pre Test Question

8. Hyperledger Fabric Consensus is planned out into 3 phases.

Which one is NOT a phase?

- A) Endorsement
- B) Ordering
- C) Validation
- D) Segregation

Pre Test Questions

9. The primary purpose of Hyperledger Composer is:
- a) Allowing blockchain applications to run on computers with slow processing power
 - b) Accelerate the time to develop a blockchain application
 - c) Make it easy to integrate blockchain technology into legacy systems
 - d) Both B and C

Pre Test Questions

What type of fork describes a major modification to the blockchain protocol which makes previously invalid blocks or transactions valid?

- a. Hard fork
- b. Soft fork
- c. Either hard or soft forks
- d. Segwit Fork

Pre Test Questions

When discussing Ethereum with your customers, what would be the best statement to use when comparing to cryptocurrencies?

- a. Ethereum is the platform and Ether is its cryptocurrency.
- b. Ether is a platform and Ethereum is the cryptocurrency for Ether.
- c. Ethereum is a platform and Ether is the test platform. Bitcoin is used as the cryptocurrency for Ethereum.
- d. None of the above.

Pre Test Questions

10. Which of the following would NOT be true about what a smart contract gives your organization?
- a. Autonomy
 - b. Trust
 - c. Legal assurance
 - d. Savings

Pre Test Questions

11. Ethereum has four main components. Which of the following components executes smart contracts?
- a. EVM
 - b. Node
 - c. Smart Contract code
 - d. dApps

Pre Test Questions

12. A limitation of the EVM not associated with other types of virtual state machines is that the EVM is intrinsically bound by which variable parameter ?
- a. Gas
 - b. CPU
 - c. Code Base
 - d. Location

Pre Test Questions

13. In what year was the whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System” by Satoshi Nakamoto, which outlines a solution to the double-spending problem, published?
- a. 2008
 - b. 2009
 - c. 2011
 - d. 2012

Pre Test Questions

14. When the distributed ledger has been updated and all nodes maintain their own identical copy of the ledger, the nodes have reached which point?
- a. Consensus
 - b. Agreement
 - c. Distributed
 - d. Immutable

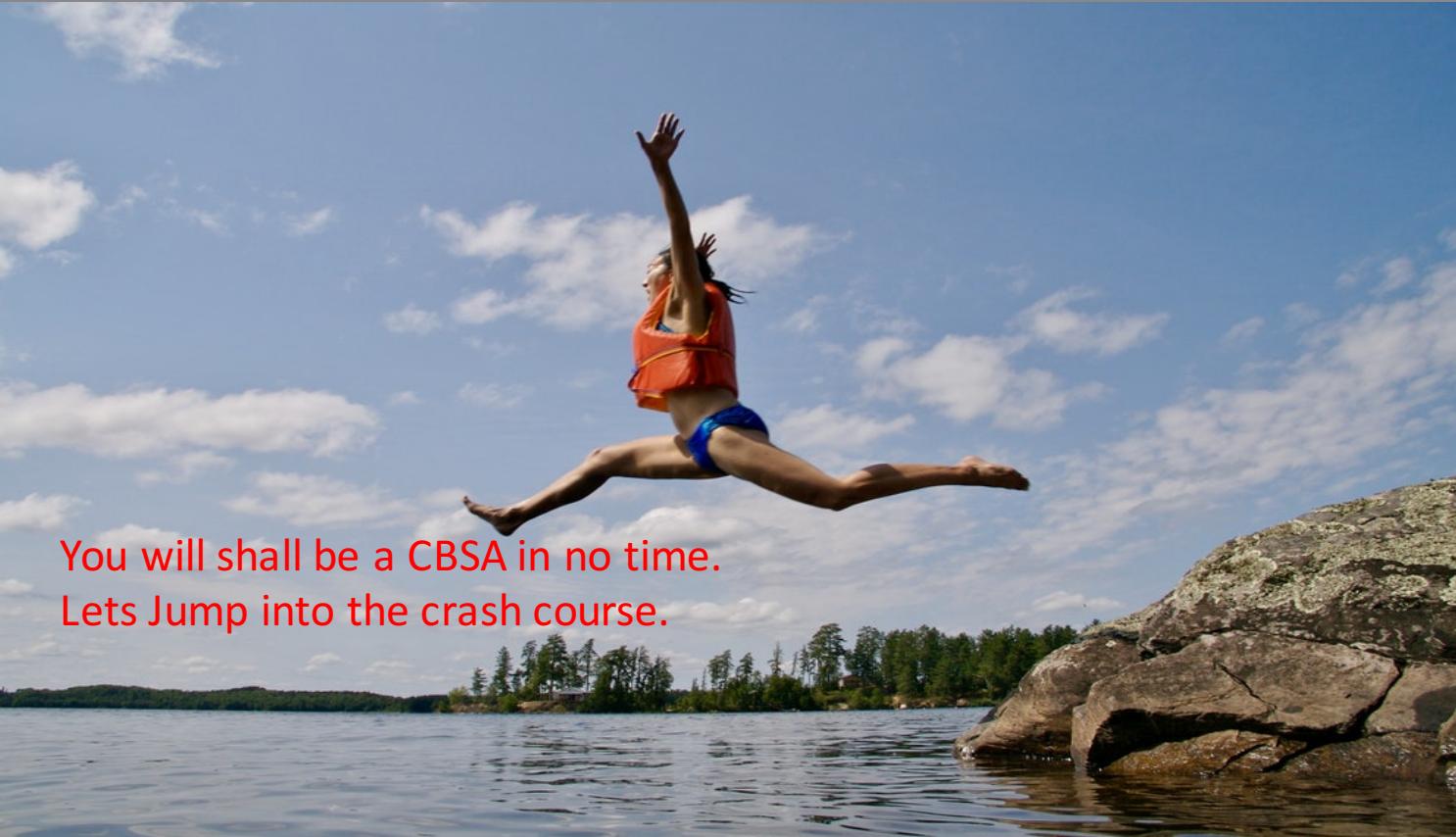
Pre Test Questions

15. What consensus algorithm is advantageous because it presents scalability and low-cost transactions, but, like Delegated Proof of Consensus (DPoS), introduces a component of centralization? Select One
- a. Proof of Work
 - b. Proof of Stake
 - c. Practical Byzantine Fault Tolerance (PBFT)
 - d. Proof of Authority

Pre Test Questions

15. What consensus algorithm is advantageous because it presents scalability and low-cost transactions, but, like Delegated Proof of Consensus (DPoS), introduces a component of centralization? Select One
- a. Proof of Work
 - b. Proof of Stake
 - c. Practical Byzantine Fault Tolerance (PBFT)
 - d. Proof of Authority

No Worries – You will learn.



You will shall be a CBSA in no time.
Lets Jump into the crash course.

CBSA Exam Crash Course

Objective

The difference between proof of work, proof of stake, and other proof systems and why they exist

CBSA Exam Crash Course

- Consensus is a dynamic way of reaching agreement in a group.
- While voting just settles for a majority rule without any thought for the feelings and well-being of the minority.
- Consensus makes sure that an agreement is reached which could benefit the entire group as a whole



CBSA Exam Crash Course



Safety = Each node is guaranteed the same sequence of inputs and results in the same output on each node. Consistency is the real requirement.



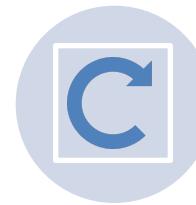
Liveness = Each non-faulty node will eventually receive every submitted transaction with the presumption that communication does not fail for example with a network outage.

CBSA Exam Crash Course

Blockchains Mining



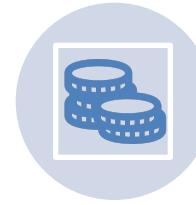
For Example in Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger.



This ledger of past transactions is called the block chain as it is a chain of blocks.



The blockchain serves to confirm transactions to the rest of the network as completed



Bitcoin nodes use the blockchain to distinguish legitimate Bitcoin transactions from attempts to re-spend coins that have already been spent.

CBSA Exam Crash Course

Blockchain Mining

- Bitcoin mining is so called because it resembles the mining of other commodities
- Requires exertion and it slowly makes new currency available at a rate that resembles the rate at which commodities like gold are mined from the ground.



CBSA Exam Crash Course

Blockchains Mining

1

A reward *is given when a block is discovered, the discoverer may award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network.*

2

Currently this bounty is 25 bitcoins but this value will halve every 210,000 blocks.

3

The miner is awarded the fees paid by users sending transactions.

4

The fee is an incentive for the miner to include the transaction in their block.

Blockchains Consensus

*Blockchain
Algos vary
based on
mining...*

- *Proof of Work*
- *Proof of Stake*
- *Delegated Proof-of-Stake (DPoS)*
- *Byzantine Fault Tolerance (BFT)*
- *Directed Acyclic Graphs (DAGs)*
- *Many other algos ...*

Proof of Work

- *Proof of Work* was the first blockchain consensus algorithm.
- Satoshi Nakamoto created for the Bitcoin blockchain
- PoW, *miners* solve hard problems to create blocks.
- PoW runs on a system of “the longest chain wins.”
- Expensive both cost and environmentally
- Bitcoin, Ethereum, Litecoin

CBSA Exam Crash Course

Proof of Stake

Proof of Stake the blocks aren't created by miners doing work

Instead by *minters* staking their tokens to "bet" on which blocks are valid.

In the case of a fork, minters spend their tokens voting on which fork to support.

Attacks costly but more environmental

Peercoin and Ethereum will go to.

Delegated Proof of Stake

*Delegated Proof-of-Stake
(DPoS)*

In DPoS, miners can collaborate to make blocks instead of competing like in PoW and PoS.

By partially centralizing the creation of blocks, DPoS is able to run orders of much faster than most other algorithms.

Cheap transaction and faster. Centralized

Steemit and EOS

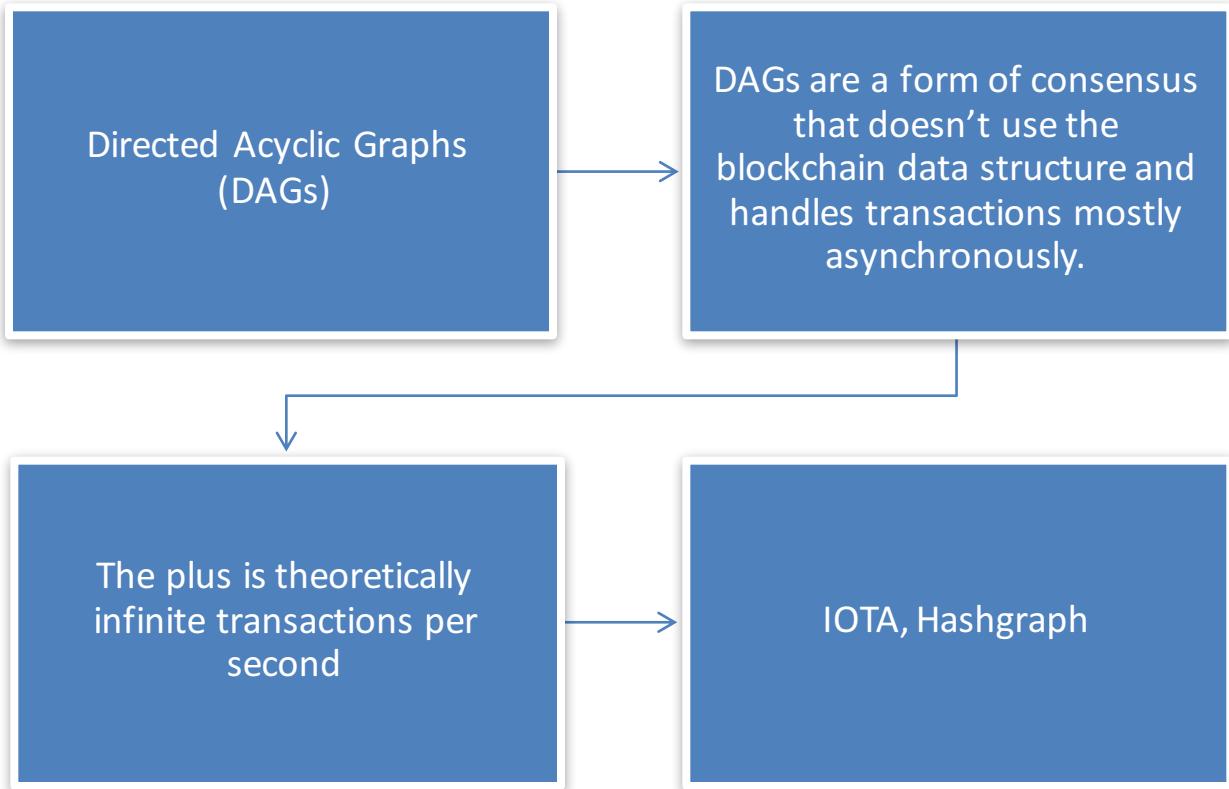
CBSA Exam Crash Course

Byzantine Fault Tolerance (BFT)

- Classic problem in distributed computing and is explained with Byzantine generals
- Pre-selected generals and meant for a private blockchain
- PBFT runs incredibly efficiently.
- High transaction throughput BUT Centralized/permission based.
- Hyperledger, Ripple and Stellar

CBSA Exam Crash Course

DAGS



CBSA Exam Crash Course

Proof of Elapsed Time



Every participant in the blockchain network waits a random amount of time to be verified.



The first participant to finish waiting gets to be the “leader” for the new block.

CBSA Exam Crash Course

Consensus Method	Used in	Primary Pros	Primary Cons
Proof of Work (PoW)	BTC, ETH, LTC	Widely Tested	Slow and Resource Intensive
Proof of Stake (PoS)	Peercoin, ETH Casper	Energy Efficient	Nothing at Stake
Proof of Elapsed Time (POET)	Hyperledger Sawtooth	Participation Cost	Specialized Hardware(Intel)
Delegated Proof of Stake (DPoS)	Steemit, EOS, LISK	Fast and Efficient	Centralized
Delegated Byzantine Fault Tolerance (DBFT)	NEO	Fast and Scalable	Root Chain control
Practical Byzantine Fault Tolerance (PBFT)	Hyperledger Fabric	Transaction Throughput	Centralized
Federated Byzantine Fault Tolerance (FBFT)	Ripple, Stellar	Low Cost and High Throughput Transactions	Centralized

Practice Questions

What consensus algorithm is advantageous because it presents scalability and low-cost transactions, but, like Delegated Proof of Consensus (DPoS), introduces a component of centralization? Select One

- a. Proof of Work
- b. Proof of Stake
- c. Practical Byzantine Fault Tolerance (PBFT)
- d. Proof of Authority

Practice Questions

What are some advantages of Proof of Stake(POS) mining over Proof of Work(POW) mining? Select Three

- a. No need for expensive hardware
- b. Energy efficient in regards to what it could consume for electricity as compared to PoW
- c. Faster validations compared to POW
- d. Better Security
- e. Faster Hashing capacity

CBSA Exam Crash Course

Objective

Why cryptocurrency is needed on certain types of blockchains

CBSA Exam Crash Course

What is a Cryptocurrency?

- Digital currencies are secured using cryptography and combining that with their role as a currency.
- Are mined. Not printed.
- Considered digital gold, silver..
- Bitcoin is the most widely known and has the largest market cap.

CBSA Exam Crash Course

Cryptocurrency examples

- Bitcoin
- Litecoin
- Monero
- Dash
- Ether
- Ripple
- And thousands more.....



CBSA Exam Crash Course

Initial Coin Offering (ICO) is an event in which a new cryptocurrency sells advance tokens from its overall coinbase, in exchange for upfront capital.

- ICOs are frequently used for developers of a new cryptocurrency to raise capital.

ICO

Initial Coin Offering

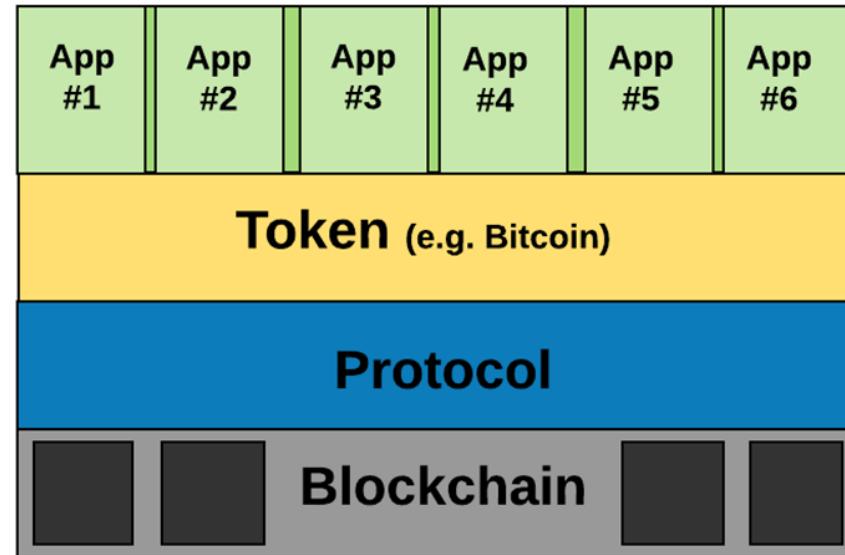
CBSA Exam Crash Course

- Digital currencies are secured using cryptography and combining that with their role as a currency.
- Are mined. Not printed.
- Need a blockchain platform
- Considered digital gold, silver..
- Bitcoin is the most widely known and has the largest market cap.
- Bitcoin is “enabled” by blockchain
 - Lets think of the blockchain as a book that can be written to but not erased.
 - Blockchains can be private or public
 - Blockchains are revolutionary way of implementing “trust” into a platform.
 - Blockchain is the “enabler” for Bitcoin

CBSA Exam Crash Course

Whats the Difference

- Cryptos like Bitcoin use the Blockchain Platform.
- Blockchain is the enabler...
- Cryptocurrency uses blockchain technology.
- Bitcoin is the first known software(Token) for blockchain.
- Platform vs Application.



Courtesy blockgeeks

CBSA Exam Crash Course

What is a difference?

BTC is a P2P
cryptocurrency that
uses the P2P Platform
(Blockchain)

Ethereum is a
platform for example.

Ether is the
cryptocurrency

CBSA Exam Crash Course

Whats the Difference



What is a difference in simple terms?



Blockchain is the train track.
(Platforms are the enabler)



Cryptos are the train on the track. (Applications are enabled)

CBSA Exam Crash Course

- With blockchains its clearly important to note that permissioned or permissionless blockchains have very different use cases.
- Part of the use case may require a cryptocurrency or use of a token.
- Enterprises can off chain to a payment gateway

CBSA Exam Crash Course

- Blockchains serve as the basis technology in which cryptocurrencies are a part of the ecosystem.
- They go hand in hand, and cryptocurrency is often necessary to transact on a permissionless blockchain.



CBSA Exam Crash Course

- Blockchains that are cryptocurrencies are the tokens used within these networks to send value and pay for these transactions.
- Can be used to digitize value of an asset as well.
- Ex: Bitcoin, Litecoin and Monero



CBSA Exam Crash Course

- Blockchains that are private for an enterprise don't generally need a cryptocurrency.
- The enterprise controls the peers, nodes and clients
- Private or Private Chain
- These are "Permissioned"
- Ex: Hyperledger, R3 Corda

Practice Questions

Blockchain is the _____ for Bitcoin?

- a. Enabler
- b. Enabled
- c. Enabler and Enabled
- d. None of the above

Practice Questions

Cryptocurrencies are usually deployed in both permissioned and permissionless blockchains. True or False

- a. False
- b. True

CBSA Exam Crash Course

Objective

The difference between public, private, and permissioned blockchains

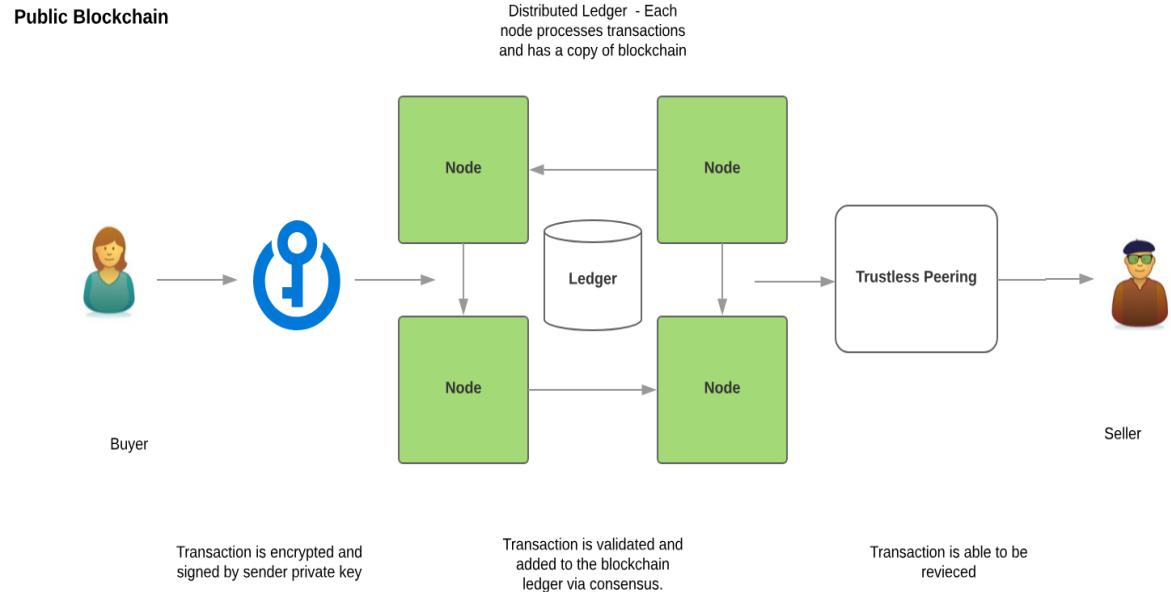
CBSA Exam Crash Course

- What is a Public Blockchain?
- Public Blockchains are also referred to as permissionless or Open blockchains.
- Bitcoin was the original permissionless blockchain.
- Transactions are processed by all nodes in the blockchain
- Transactions are publicly viewable(transparent) in the blockchain
- Widely distributed. For example Ethereum has over 16,000 nodes worldwide

CBSA Exam Crash Course

Public Blockchain

What is a Public Blockchain?



Public Blockchain

Public Blockchains Benefits

- Open Read and Write (Transparency)
- Ledger is distributed (P2P)
- Censorship resistant (Immutability)
- Secure due to mining (51% rule)

CBSA Exam Crash Course

Public Blockchain

- Public Blockchains Examples
- Bitcoin
- Ethereum
- Monero



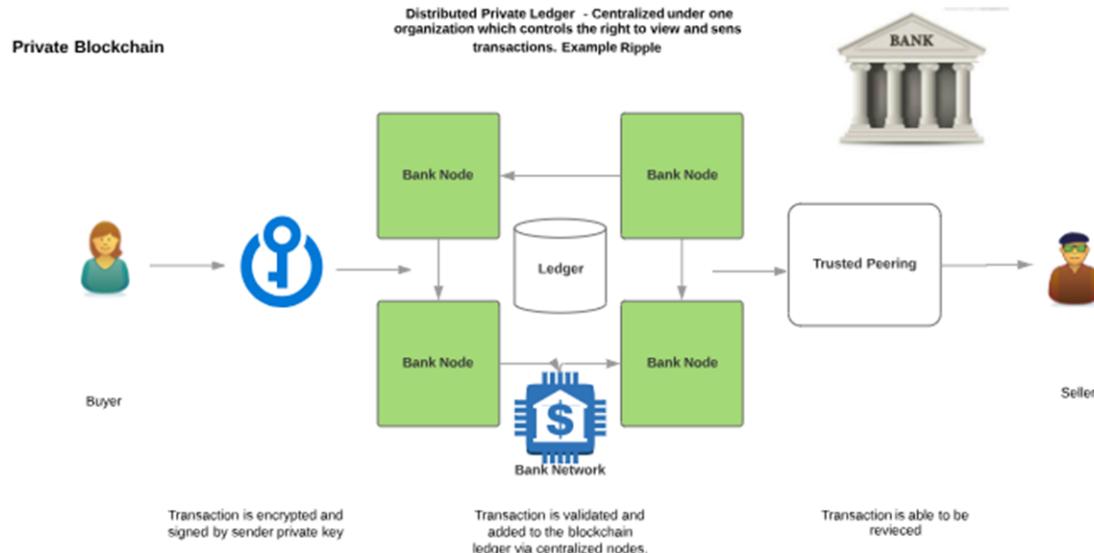
CBSA Exam Crash Course

What are Private Blockchains?

- Private Blockchains are also referred to as permissioned or enterprise blockchains.
- Can be Open Sourced, Consortium or privately developed
- Transactions are processed by select nodes in the blockchain
- Transactions are not publicly viewable(transparent) in the blockchain
- Locally distributed.

CBSA Exam Crash Course

Private Blockchains



CBSA Exam Crash Course

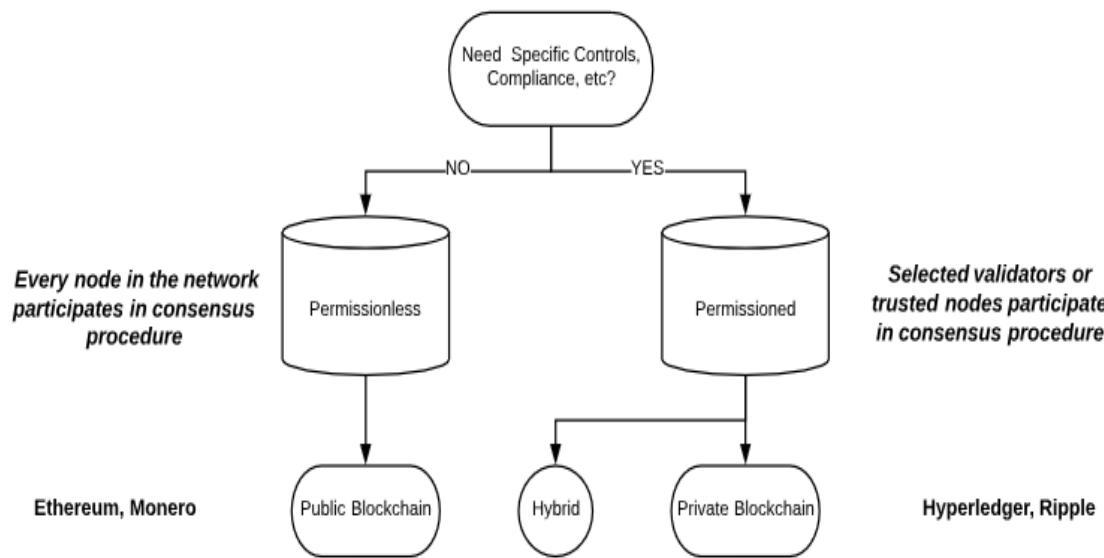
Private Blockchain Benefits

Some Private Blockchains Benefits Are

- Enterprise Permissioned
 - Faster Transactions
 - Better Scalability
 - Compliance Support
 - Consensus more efficient (Less nodes)
-

CBSA Exam Crash Course

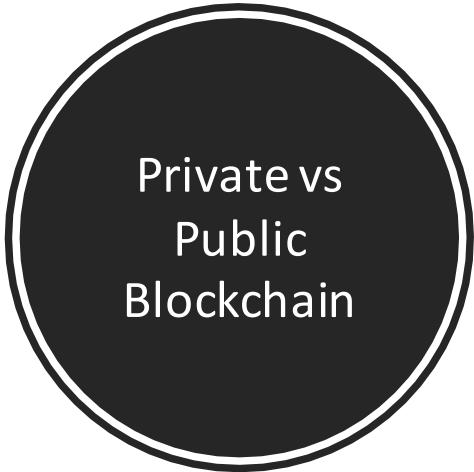
Blockchain types and decision flow



Blockchains Were originally developed as permissionless such as BTC

- **Permissionless (Public) or Permissioned (Private)**
- **Decide based on your enterprise privacy and security requirements**

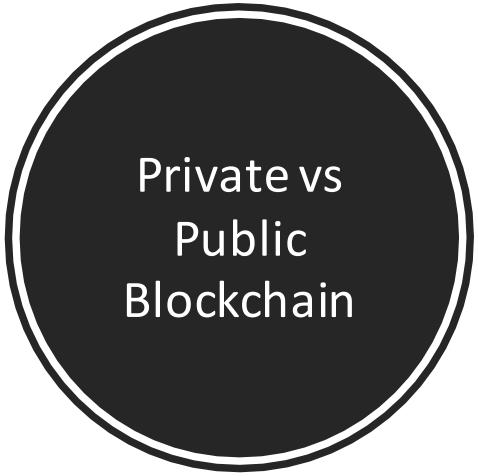
CBSA Exam Crash Course



	Public (Permissionless)	Private (Permissioned)
Access to Ledger	Open Read/Write	Permissioned Read/Write
Identity	Anonymous	Known Identities
Security and Trust	Open Network (Trust Free)	Controlled Network(Trusted)
Transaction Speed	Slower	Faster
Consensus	POW/POS	Proprietary or Modular
Open Source	Yes	Depends on Blockchain
Code Upkeep	Public	Consortium or Managed
Examples	Ethereum, Multichain	R3 Corda, Quorum

- Blockchains
- Permissionless (Public) or Permissioned (Private)

CBSA Exam Crash Course



	Ethereum	R3 Corda	Quorum	Hyperledger	Ripple
Industry	Cross-Industry	Financials	Cross- Industry	Cross Industry	Financial
Ledger	Permission-less	Permissioned	Permissioned	Permissioned	Permissioned
Consensus	Proof of Work (PoW)	Pluggable	Majority Voting	Pluggable	Probabilistic Voting
Smart Contract Support	Yes	Yes	Yes	Yes	No
Cryptocurrency	Ether (Eth)	N/A	N/A	N/A	Ripple (XRP)

- Comparing Enterprise Blockchains

CBSA Exam Crash Course

Considerations on permissioned vs permissionless blockchain?

Governance

Industry Vertical

Smart Contract Functionality

Cryptocurrency Requirement

Consensus Algorithm

Costing Model

Integration

Practice Questions

Which of the following blockchains are not permissionless?

- a. Hyperledger
- b. Ethereum
- c. Bitcoin
- d. Monero

Practice Questions

Which of following is a benefit of a permissionless blockchain?

- a. Transparency
- b. Compliance Support
- c. Efficient Consensus
- d. Faster Consensus

Practice Questions

Which of following is not a benefit of a permissioned blockchain?

- a. Transparency
- b. Compliance Support
- c. Efficient Consensus
- d. Faster Consensus

Practice Questions

Which of following is a benefit of a permissioned blockchain?

- a. Censorship Resistant
- b. Compliance Support
- c. Secure due to mining
- d. Distributed Ledger

CBSA Exam Crash Course

Objective

How blocks are written to the blockchain

Hashing

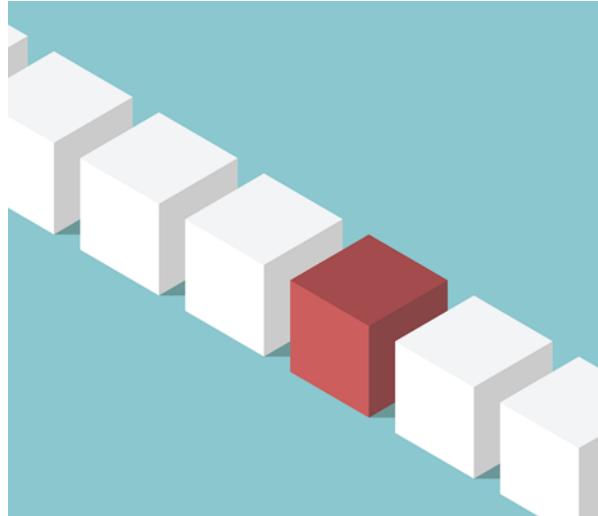
Block

- A block contains data of the transaction, hash of the block and hash of the previous block.
- The structure of the block is:

Block 1
Data
Previous Hash
Hash Hash

CBSA Exam Crash Course

- **Block** An ordered set of transactions that is cryptographically linked to the preceding block(s) on a channel.
- **Chain** The ledger's chain is a transaction log structured as hash-linked blocks of transactions.



CBSA Exam Crash Course

Blocks

Block metadata contains:

- version - the current version of the block structure
- previous block header hash - the reference this block's *parent block*
- merkle root hash - a cryptographic hash of all of the transactions included in this block
- time - the time that this block was created
- nBits - the current *difficulty* that was used to create this block
- nonce ("number used once") - a random value that the creator of a block is allowed to manipulate

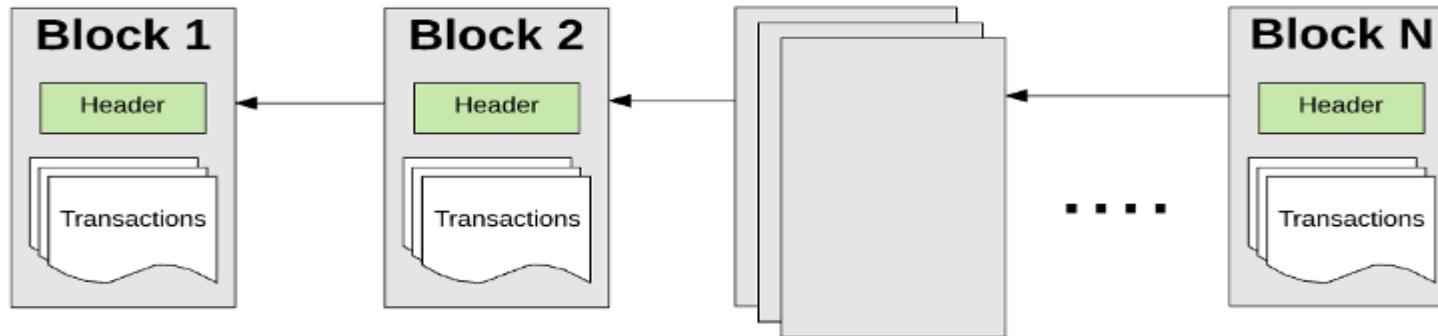
Blockchain Architectures

A genesis block is the first block of a block chain and then come the branches

- Block Categories
- Main branch blocks
- Side branch blocks
- Orphan blocks

CBSA Exam Crash Course

- For a transaction to be considered valid it will be processed by a validation process known as blockchain mining.
- Mining is when a group of nodes use their computing resources to create a block of valid transactions.



CBSA Exam Crash Course

- For a transaction to be considered valid, it will be processed by a validation process known as **blockchain mining**.
- Mining is when a group of nodes use their computing resources to create a block of valid transactions.



AntMiner S7



Avalon6

CBSA Exam Crash Course

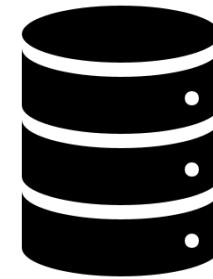
- Legacy Architectures in databases.
- SQL or NoSQL
- Whether centralized or distributed
- Traditional databases use client-server network architecture.
- Database processing is quicker

SQL Statement:

```
SELECT Orders.OrderID, Customers.CustomerName, Orders.OrderDate  
FROM Orders  
INNER JOIN Customers  
ON Orders.CustomerID=Customers.CustomerID;
```

CBSA Exam Crash Course

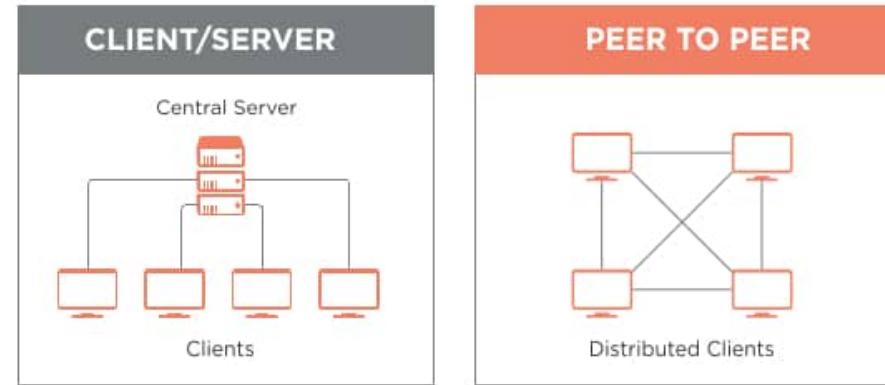
- Traditional databases use client-server network architecture.
- Control of the database remains with a designated authority
- If security of the authority is compromised then the data can be modified, or even deleted.
- (CRUD) Create, Read, Update, and Delete . More flexible than blockchain.



CBSA Exam Crash Course

Databases maintain

- Disintermediation
- Centralization
- Performance
- Agility
- Privacy



CBSA Exam Crash Course

The blockchain allows for two specific functions:

- 1. Validation of a transaction
- 2. Writing of a new transaction



CBSA Exam Crash Course

Blockchain Properties

- Trustlessness—network participants help secure the network so there is no need for a centralized third party to be employed.
- Replication – Blockchain stores a copy on every computer in the network.
- Immutable – Once a piece of information is appended to the blockchain, it can never be edited.
- Time-stamp – A timestamp is a sequence of characters or encoded information identifying when a certain event occurs.

CBSA Exam Crash Course

Database Properties ACID and BASE

- Atomicity – means that either all of the operations in a transaction execute successfully and take the system to a different consistent state or nothing happens at all.
- Consistency –means that integrity constraints must be maintained so that the database is consistent before and after the transaction.
- Isolation – this property ensures that multiple transactions can occur concurrently with no inconsistency of the database state.
- Durability – This property ensures that once the transaction has completed execution the updates are written to disk.

CBSA Exam Crash Course

Objective

Where cryptography fits into blockchain and the most commonly used systems

CBSA Exam Crash Course

- A **wallet** is a program which allows you to gain access to, send and receive bitcoins on the blockchain.
- Several types of bitcoin wallets: Hardware, software, paper and web.
- Software wallets are programs that you download and run on your PC.

CBSA Exam Crash Course

- A **web wallet** is hosted on a website of a company which provides bitcoin wallet services.
- These wallets are easier to set up and use, but you have to rely on the hosting company to provide sufficient security measures, which can sometimes be a dangerous trade-off.
- Least secure

CBSA Exam Crash Course

- A hardware wallet maintains high levels of security to protect your coins by storing your coins offline.
- Offline storage keeps your coins out of reach from hackers because they are not on the Internet.
- It is more expensive than a software or web wallet.
(\$100.00)

CBSA Exam Crash Course

- A paper wallet is offline and is considered the safest
- Print out basically
- Static, not on network



CBSA Exam Crash Course

Wallet Security

- **Restrict unsupervised access.** Strong passwords and close all ports and maintain a strict firewall.
- **Frequently change address.** Use a different address for every transaction.
- **Multiple Signatures (Multi-sig).** Multiple private keys to deter breaches.

CBSA Exam Crash Course

Ethereum Wallets

- **MyEtherwallet**
- **Jaxx**
- **Metamask**



Practice Questions

Which of following types of wallet is considered the most secure?

- a. Coinbase
- b. Paper
- c. Hardware
- d. Web

Practice Questions

Which of following types of wallet is considered the least secure?

- a. Coinbase
- b. Paper
- c. Hardware
- d. Web

CBSA Exam Crash Course

Objective

The Common use cases for public blockchains

CBSA Exam Crash Course

- Use cases can be very different between permissionless and permissioned blockchains
- Blockchains are growing in use cases
- Major Vendors sponsoring



THERE MANY USES CASES FOR THE BLOCKCHAIN EVEN THOUGH THE TECHNOLOGY ADOPTION HAS REALLY JUST STARTED.



BLOCKCHAIN IS DOMINANT AND PROMISING TECHNOLOGIES OF THE PAST FEW YEARS



BLOCKCHAIN IS CONSIDERED A DISRUPTIVE TECHNOLOGY

CBSA Exam Crash Course

Financial such
as Audit trails

Retail
Logistics

Government
programs

Real estate
titles

Supply Chains

Tokenization

Digital
Identity

Compliance
in markets

CBSA Exam Crash Course

Industry

Financials - banking and insurance

Government

Retail

Logistics

Legal

Manufacturing

Telcom

Many others

Practice Questions

Blockchain is considered to be a disruptive technology? True or False

- a. False
- b. True

CBSA Exam Crash Course

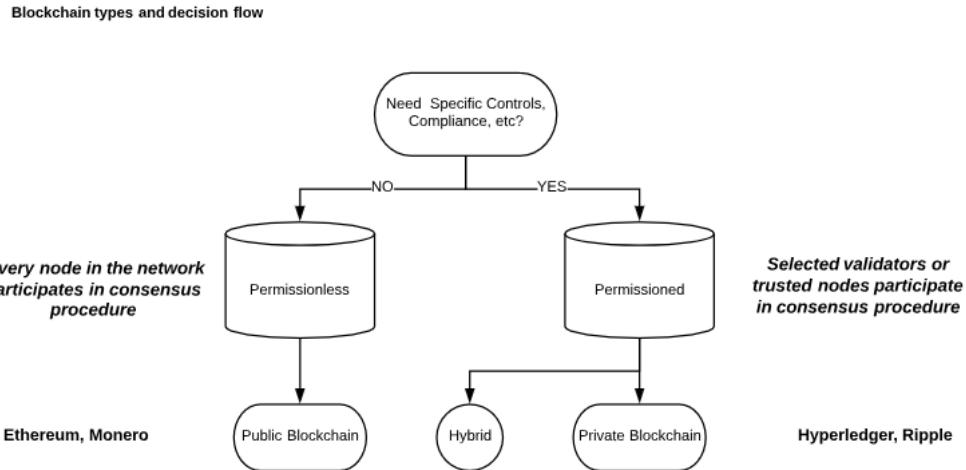
Objective

Common use cases for private & permissioned blockchains

CBSA Exam Crash Course

Blockchains

- Were originally developed as permissionless such as BTC
- Permissionless (Public) or Permissioned (Private)



CBSA Exam Crash Course

Blockchains

- Permissionless (Public) or Permissioned (Private)

	Public (Permissionless)	Private (Permissioned)
Access to Ledger	Open Read/Write	Permissioned Read/Write
Identity	Anonymous	Known Identities
Security and Trust	Open Network (Trust Free)	Controlled Network(Trusted)
Transaction Speed	Slower	Faster
Consensus	POW/POS	Proprietary or Modular
Open Source	Yes	Depends on Blockchain
Code Upkeep	Public	Consortium or Managed
Examples	Ethereum, Multichain	R3 Corda, Quantum

CBSA Crash Course

Considerations on permissioned vs permissionless blockchain?

- Governance
- Industry Vertical
- Smart Contract Functionality
- Cryptocurrency Requirement
- Consensus Algorithm
- Costing Model
- Integration

CBSA Exam Crash Course

A business model describes the rationale of how an organization creates, delivers, and captures value in economic, social, cultural, or other contexts. Investopedia



CBSA Exam Crash Course

- There are many use-cases for the blockchain, even though the technology adoption has really just started.
- Blockchain is one of the several dominant and promising technologies of the past few years that is driving companies to innovate and change how value is delivered.

CBSA Exam Crash Course

- Business - to - Business (B2B)
- Business - to - Consumer (B2C)
- Consumer - to - Consumer (C2C)
- Consumer - to - Business (C2B)
- Business - to - Government (B2G)
- Government - to - Business (G2B)
- Government - to - Citizen (G2C)

CBSA Exam Crash Course

Blockchain Technology is already disrupting:

- Financial Services
- Government Services
- Healthcare
- Real Estate
- And many more industries on a smaller scale

CBSA Exam Crash Course

Blockchain Technology is already evolving to where an organization has to consider its effects to the business model in three main ways(approaches):

- Technical
- Business
- Legal

CBSA Exam Crash Course

The use of Blockchain Technologies in several industries is effecting how services are delivered and how many people are involved in the delivery of that service.

Essentially a “disruption” in the business model is occurring.



B2C Use Case

Verticals that are heavily exploring blockchain for transparency are:

- Financials
- Logistics
- Charity Funding
- Agriculture Tracking
- Precious Metals
- Numerous other verticals

B2C Use Case

The jewelry industry is an industry that has been known for fraud, child labor issues, false metal mining and a clear lack of transparency. A precious metals consortium with IBM has established a blockchain initiative around how transparency can be brought to the consumer.

- The “TrustChain Initiative” tracks and authenticates diamonds and precious metals through every stage of the supply chain as it becomes a piece of finished jewelry.
- It provides digital verification, physical product and process verification, and third-party oversight.

B2C Use Case

- The collaboration's goal is to instill trust in the origin and ethical sourcing of jewelry by bringing together a community of responsible and ethical organizations across the complex and multi-tiered jewelry supply chain.
- Consumers will see that "TrustChain" establishes a trusted product with documented provenance and brings together quality assurance, social and environmental responsibility and authenticity spanning the entire jewelry ecosystem – from miners, manufacturers, wholesale suppliers and retailers – on a single digital platform.

B2C Use Case

The Benefits to the consumer from a blockchain solution is clear and established.

- Transparency to the consumers
- Responsibility from the suppliers
- Ethical Sourcing validation
- Labor verification
- Immutable shared view

Practice Questions

Blockchain Technology is already evolving to where an organization has to consider its effects to the business model in three main approaches. Which of the following is not approach?

- a. Technical
- b. Business
- c. Legal
- d. Performance

CBSA Exam Crash Course

- Feeling like this guy?
- It's a Crash Course!



CBSA Exam Crash Course

Objective

What is needed to launch your own blockchain

CBSA Exam Crash Course

Steps to building a Blockchain:

- Establish Use-Case
- Platform (Consensus)
- Design the Nodes
- Design the Services
- Determine APIS
- Determine Testing
- Release to Production

Practice Questions

Which of following steps would be considered the first step in the design process for a blockchain?

- a. Implementation
- b. Platform
- c. Nodes
- d. Use Case

CBSA Exam Crash Course

Objective

Common problems & considerations in working with public blockchains

CBSA Exam Crash Course

Blockchains

- Permissionless (Public) or Permissioned (Private)

	Public (Permissionless)	Private (Permissioned)
Access to Ledger	Open Read/Write	Permissioned Read/Write
Identity	Anonymous	Known Identities
Security and Trust	Open Network (Trust Free)	Controlled Network(Trusted)
Transaction Speed	Slower	Faster
Consensus	POW/POS	Proprietary or Modular
Open Source	Yes	Depends on Blockchain
Code Upkeep	Public	Consortium or Managed
Examples	Ethereum, Multichain	R3 Corda, Quantum

CBSA Exam Crash Course

- A **fork** is a change to the software of the digital currency that creates two separate versions of the blockchain with a shared history (One Dominant)
- Can be permanent or temporary
- There is a snapshot date, where a snapshot of the ledger is captured
- The snapshot happens at a block number and a new currency is a result



CBSA Exam Crash Course

Blockchain Hard Fork

- A hard fork is a term that describes a major change to the blockchain protocol which makes previously invalid blocks or transactions valid.
- This can be used to keep the same coin with major changes to the blockchain or to create a new coin.
- This requires all nodes to upgrade to the latest version of the protocol software if they want to use the new coin or blockchain.

CBSA Exam Crash Course

Soft Fork

- A soft fork is a change that's backward compatible. For example, instead of 1MB blocks, a new rule might only allow 500K blocks.
- A change to the software protocol where only previously valid blocks/transactions are made invalid.
- Soft forks need a majority of hash power in the network.

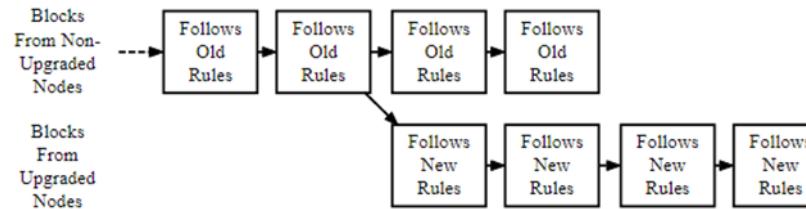
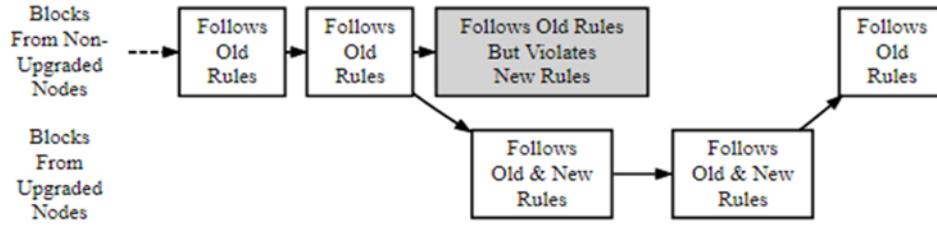
CBSA Exam Crash Course

Soft vs Hard Forks

Soft Fork	Hard Fork
Tightening the rules (eg, 1MB -> 0.5MB)	Expanding the rules (eg, 1MB -> 2MB)
Backwards compatible	Not backwards compatible
Old nodes accept new blocks	Old nodes don't accept new blocks

CBSA Exam Crash Course

Soft vs Hard Fork



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

Diagrams - Investopedia

CBSA Exam Crash Course

Hard Fork Examples

- **Ethereum Classic** is a split from an existing cryptocurrency, Ethereum after a hard fork
- **Monero** is a hard-fork to introduce an upgrade to its network by implementing a feature called Ring Confidential Transactions (RCT) to improve its privacy and security
- **Bitcoin Cash** is a hard fork orchestrated by a portion of the community that wanted Bitcoin to scale by increasing its block size from the current 1MB to 8MB.

CBSA Exam Crash Course

Soft Fork Examples

- **BIP 66:** Soft fork on Bitcoin's signature validation
- **P2SH:** Soft fork that enabled multi-signature addresses in Bitcoin's network



CBSA Exam Crash Course

SegWits

- SegWit = Segregated Witness - Segregated Witness in short, means to separate transaction signatures.
- Is the process by which the block size limit on the BTC blockchain is increased by removing signature data from Bitcoin transactions.
- By removing signatures, it frees up capacity to add more transactions to the chain.

CBSA Exam Crash Course

Segwit is Segregated Witness

- Segwit removes signatures.
- Creates efficiency but increases security threats.

How is a Segwit coin different?

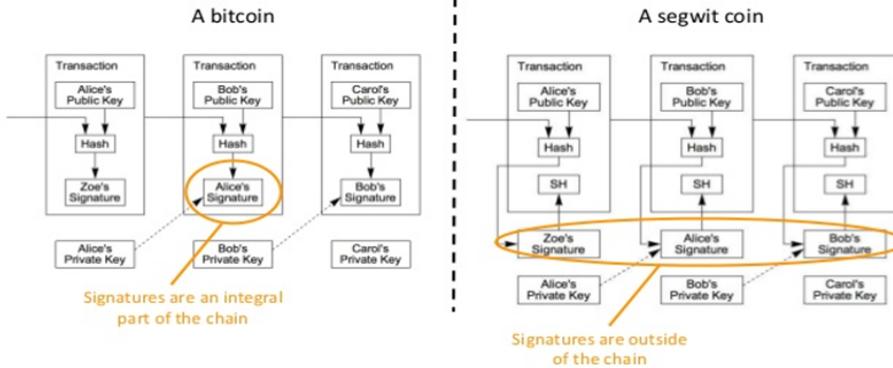


Diagram – Peter Rizen

CBSA Exam Crash Course

Segwits benefits:

- Improve Scalability (UTXO)
- Reduces transaction times by skipping calculation for signatures.
- Enables off chain protocols (P2SH256)
- Can improve transaction security thru reducing malleability



Pre Test Questions

What type of fork describes a major modification to the blockchain protocol which makes previously invalid blocks or transactions valid?

- a. Hard fork
- b. Soft fork
- c. Either hard or soft forks
- d. Segwit Fork

Pre Test Questions

What type of fork is a change that's backward compatible?

- a. Hard fork
- b. Soft fork
- c. Either hard or soft forks
- d. Segwit Fork

Pre Test Questions

What type of fork process removes signatures and thereby frees up capacity to add more transactions to the chain?

- a. Hard fork
- b. Soft fork
- c. Either hard or soft forks
- d. Segwit Fork

CBSA Exam Crash Course

Objective

When is mining needed and when it is not

CBSA Exam Crash Course

- For Example in Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger.
- This ledger of past transactions is called the block chain as it is a chain of blocks.
- The blockchain serves to confirm transactions to the rest of the network as completed
- Bitcoin nodes use the blockchain to distinguish legitimate Bitcoin transactions from attempts to re-spend coins that have already been spent.

CBSA Exam Crash Course

- Bitcoin mining is so called because it resembles the mining of other commodities
- Requires exertion and it slowly makes new currency available at a rate that resembles the rate at which commodities like gold are mined from the ground.
- Bitcoin uses the Hashcash proof of work



CBSA Exam Crash Course

- A reward *is given when* a block is discovered, the discoverer may award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network.
- Currently this bounty is 25 bitcoins but this value will halve every 210,000 blocks.
- The miner is awarded the fees paid by users sending transactions.
- The fee is an incentive for the miner to include the transaction in their block.

Pre Test Questions

A reward is given to a miner when a block is_____?

- a. Forked
- b. Printed
- c. Mined
- d. Discovered

CBSA Exam Crash Course

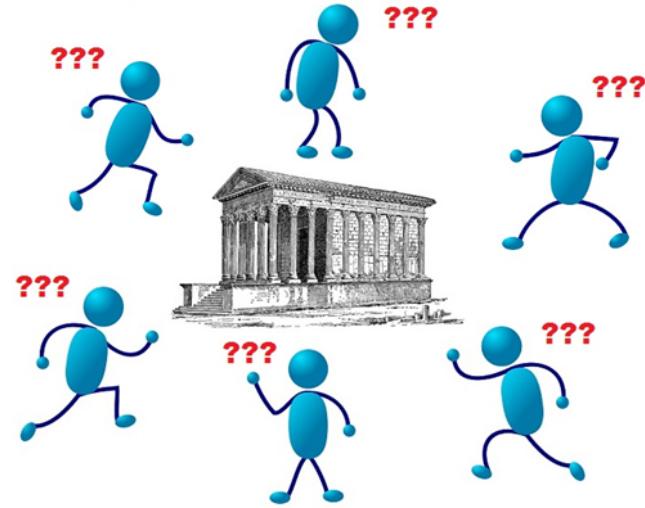
Objective

Byzantine Fault Tolerance

CBSA Exam Crash Course

The Byzantine Generals Problem

- A number of generals have surrounded a walled city on all sides.
- The balance of power is such that if all generals attack at the same time, they will take the city.
- Generals must coordinate attack or they could lose the city and their campaign.



CBSA Exam Crash Course

The Byzantine Generals Problem with computers

- “Byzantine Generals’ Problem” states that no two node on a decentralized network can entirely and irrefutably guarantee that they are displaying the same data.
- Satoshi Nakamoto solved the issue with the BTC POW Consensus algo.



CBSA Exam Crash Course

Byzantine Fault Tolerance (BFT)

- Classic problem in distributed computing and is explained with Byzantine generals
- Pre-selected generals and meant for a private blockchain
- PBFT runs incredibly efficiently.
- High transaction throughput BUT Centralized/permission based.
- Hyperledger, Ripple and Stellar

CBSA Exam Crash Course

The Byzantine Generals Problem with computers

- Essentially a “Byzantine” node is a node that can be rogue by not forwarding packets or perhaps mislead other nodes involved in the P2P Consensus network.
- Hyperledger Fabric out of the box does not provide PBFT, but offers its users to add this consensus mechanism modularly.

CBSA Exam Crash Course

- IBM backed Hyperledger uses this consensus algorithm.
- (Indy) Plenum Byzantine Fault Tolerance and for Iroha BFT consensus algorithm called Sumeragi
- In PBFT each node maintains an internal storage.
- When a node receives a message, it is signed by the node to verify its format.
- Once enough of the same responses are reached, then a consensus is met that the message is a valid transaction.

Pre Test Questions

Who is credited with solving the Byzantine General Problem in computing?

- a. Bill Gates
- b. Andreas Antonopoulos
- c. Central Intelligence Agency
- d. Satoshi Nakamoto

Pre Test Questions

A Byzantine failure is the loss of a system service due to a Byzantine fault in systems that requires _____. What is required?

- a. Replication
- b. Availability
- c. Bandwidth
- d. Consensus

CBSA Exam Crash Course

Objective

Consensus among blockchains

CBSA Exam Crash Course

- Consensus is a dynamic way of reaching agreement in a group.
- While voting just settles for a majority rule without any thought for the feelings and well-being of the minority.
- Consensus makes sure that an agreement is reached which could benefit the entire group as a whole

CBSA Exam Crash Course

Blockchain Consensus Algos

- *Proof of Work*
- *Proof of Stake*
- *Delegated Proof-of-Stake (DPoS)*
- *Byzantine Fault Tolerance (BFT)*
- *Directed Acyclic Graphs (DAGs)*
- *Other Algos*

CBSA Exam Crash Course

Proof of Work was the first blockchain consensus algorithm.

- Satoshi Nakamoto created for the Bitcoin blockchain
- PoW, *miners* solve hard problems to create blocks.
- PoW runs on a system of “the longest chain wins.”
- Expensive both cost and environmentally
- Bitcoin, Ethereum, Litecoin

CBSA Exam Crash Course

Proof of Stake the blocks aren't created by miners doing work

- Instead by *minters staking* their tokens to “bet” on which blocks are valid.
- In the case of a fork, minters spend their tokens voting on which fork to support.
- Attacks costly but more environmental
- Peercoin and Ethereum will go to.

CBSA Exam Crash Course

- In the DPoS participants who hold tokens are able to cast votes to elect block producers
- Votes are weighted by the voter's stake, and the block producer candidates that receive the most votes are those who produce blocks.
- In DPoS you can think as stakeholders as notaries and block producers as witnesses

CBSA Exam Crash Course

- The benefits
- Separation of concerns
- Stakeholder (token) control
- Scalability
- On Chain Governance
- Avoids the “Nothing at Stake” problem

CBSA Exam Crash Course

DPoS divides the consensus model in two fundamental parts

1. Electing a group of block producers
 2. Scheduling production.
- Not everyone in a DPoS network can produce blocks to validate a transaction

CBSA Exam Crash Course

- Avoids the “Nothing at Stake” problem by addressing the famous Nothing-at-Stake problem in PoS networks in which a small group of validators can take control of the network.
- The fixed number of token validators in DPoS as well as the dynamic election model prevents this issue from happening.

CBSA Exam Crash Course

Consensus Method	Used in	Primary Pros	Primary Cons
Proof of Work (PoW)	BTC, ETH, LTC	Widely Tested	Slow and Resource Intensive
Proof of Stake (PoS)	Peercoin, ETH Casper	Energy Efficient	Nothing at Stake
Proof of Elapsed Time (POET)	Hyperledger Sawtooth	Participation Cost	Specialized Hardware(Intel)
Delegated Proof of Stake (DPoS)	Steemit, EOS, LISK	Fast and Efficient	Centralized
Delegated Byzantine Fault Tolerance (DBFT)	NEO	Fast and Scalable	Root Chain control
Practical Byzantine Fault Tolerance (PBFT)	Hyperledger Fabric	Transaction Throughput	Centralized
Federated Byzantine Fault Tolerance (FBFT)	Ripple, Stellar	Low Cost and High Throughput Transactions	Centralized

CBSA Exam Crash Course

Proof of Elapsed Time

- Created by Intel to run on their trusted execution environment
- Similar to Proof of Work but more energy efficient
- Major Issue – requires trust in Intel, places power back in the hands of a central authority
- Hyperledger Sawtooth (Lottery Based) The current implementation of Hyperledger Sawtooth builds on a Trusted Execution Environment (TEE) provided by Intel's Software Guard Extensions (SGX).

CBSA Exam Crash Course

Proof of Authority

- Uses a set of “authorities” – nodes that are explicitly allowed to create new blocks and secure the blockchain
- Replacement for PoW - Private blockchains only
- Earn the right to become a validator/authority

CBSA Exam Crash Course

Proof of Burn

- Coins are “burned” by sending them to an address where they cannot be retrieved
- The more coins you burn, the better your chances of being selected to mine the next block
- Eventually, you must stake more by burning more coins

CBSA Exam Crash Course

Proof of Activity

- Hybrid of PoW and PoS
- Empty template blocks are mined (PoW), then filled with transactions which are validated via Proof of Stake

CBSA Exam Crash Course

Proof of Capacity

- Pay to play with hard drive space
- The most space you ‘stake’ the better your odds of being selected to mine the next block
- Consensus algorithm generates large data sets called ‘plots’ which consume storage
- Major criticism – this method has no real deterrent for bad actors

Practice Question

What consensus algorithm uses miners to validate transactions?

- a. Proof of Stake
- b. Proof of Elapsed Time
- c. Proof of Work
- d. Proof of Capacity

Practice Question

What application is used by Hyperledger Fabric to communicate with the network?

- a. JSON
- b. Binary
- c. SDK
- d. RPC API

CBSA Exam Crash Course

Objective

What is hashing

CBSA Exam Crash Course

Hashing means taking an input string of any length and giving out an output of a fixed length.

- In the context of cryptocurrencies like Bitcoin, the transactions are taken as an input and run through a hashing algorithm which gives an output of a fixed length

CBSA Exam Crash Course

- No matter how big or small your input is, the output will always have a fixed 256-bits length
- Even if slight changes are made to the input the changes get reflected in the hash. Unison
- Blockchain hash functions makes it immutable.
- Integrity and Tamperproof

CBSA Exam Crash Course

<https://anders.com/blockchain/hash.html>

The screenshot shows a web application titled "Blockchain Demo". The navigation bar includes links for Hash, Block, Blockchain, Distributed, Tokens, and Coinbase. The main content area is titled "SHA256 Hash". It displays two input fields: "Data:" containing "hello person hyperledger course" and "Hash:" containing "91c6cb0457e49182229f12204c4fe0880ec85814588fac338f918c68f28bf14a".

Data:	Hash:
hello person hyperledger course	91c6cb0457e49182229f12204c4fe0880ec85814588fac338f918c68f28bf14a

Practice Question

Blockchain's use of cryptographic hashing provides for

- a. the maintaining of data integrity
- b. making data blocks tamper proof
- c. network security to work in unison
- d. All of the above

CBSA Exam Crash Course

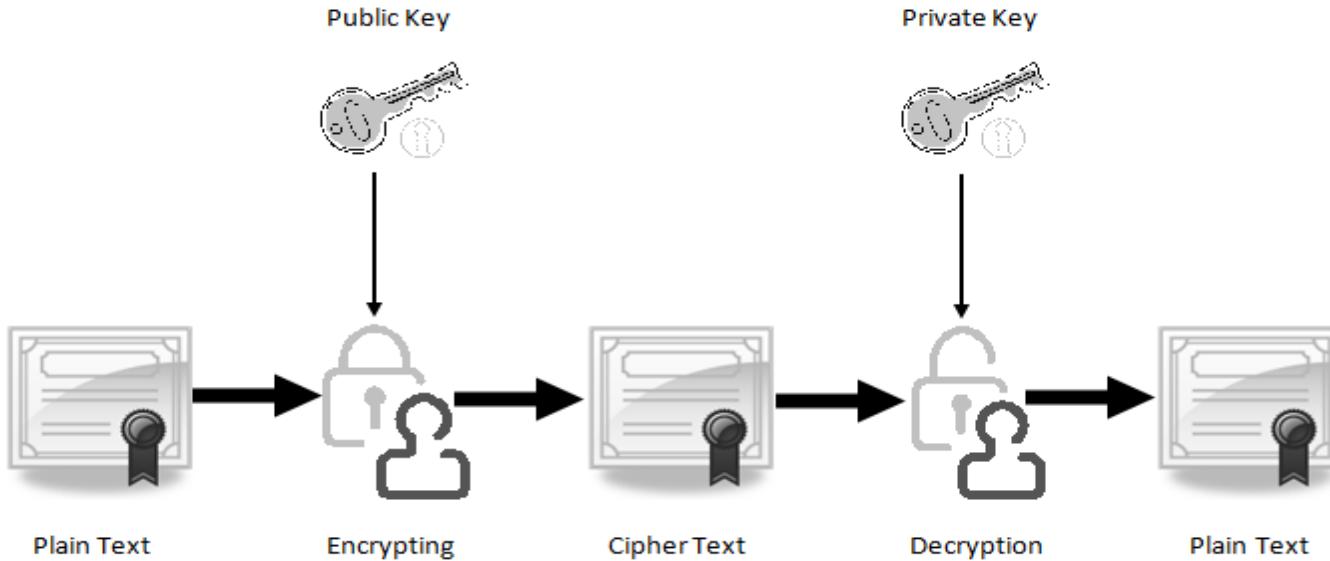
Objectives

**Security in Blockchain
How addresses, public keys, and private keys work**

CBSA Exam Crash Course

- Private Key and public key are a part of encryption that encodes the information. Both keys work in two encryption systems called symmetric and asymmetric.
- Symmetric encryption (private-key encryption or secret-key encryption) utilize the same key for encryption and decryption.
- Asymmetric encryption utilizes a pair of keys like public and private key for better security where a message sender encrypts the message with the public key and the receiver decrypts it with his/her private key.

CBSA Exam Crash Course



SSL2Buy.com

CBSA Exam Crash Course

- Public key uses asymmetric algorithms that convert messages into an unreadable format.
- A person who has a public key can encrypt the message intended for a specific receiver.
- The receiver with the private key can only decode the message, which is encrypted by the public key.
- The key is available via the public accessible directory.

CBSA Exam Crash Course

- The private key is a secret key that is used to decrypt the message and the party knows it that exchange message.
- In the traditional method, a secret key is shared within communicators to enable encryption and decryption the message, but if the key is lost, the system becomes void.

CBSA Exam Crash Course

- A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption.
- The purpose of a PKI is to facilitate the secure electronic transfer of information
- Confirms identity

CBSA Exam Crash Course

An X.509 certificate is any certificate under the X.509 specification standard for public key infrastructure and Privilege Management Infrastructure (PMI).

The X.509 provides standardized formats for:

- Attribute certificates
- Public key certificates
- Certificate revocation lists
- Certification validation algorithms

CBSA Exam Crash Course

- These certificates are used for identity validation and for transmission of encrypted data that only the owner (person, organization or software) of a specific certificate is able to decrypt and read.
- X.509 certificates act as secure identifiers, digital passports which contain information about the owner.
- The certificate is tied to a public key value which is associated with the identity contained in the certificate.

CBSA Exam Crash Course

Objective

What is a smart contract and dapps

Smart Contract

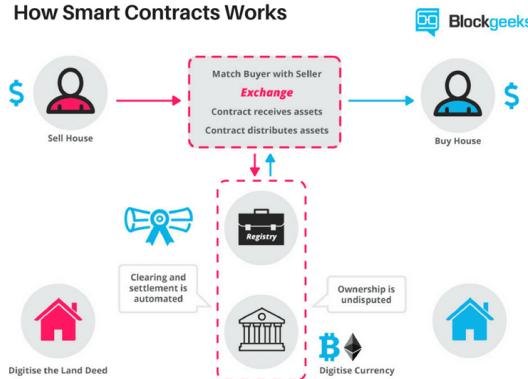


- Smart contract is a term used to describe computer program code that is capable of facilitating, executing, and enforcing the negotiation or performance of an agreement using Blockchain technology. (Contract)
- The entire process is automated can act as a complement, or substitute, for legal contracts.
- Terms of the smart contract are recorded in a computer language as a set of instructions
- Aka - Chaincode

CBSA Exam Crash Course

Image Blockgeeks

How Smart Contracts Works



Smart Contracts

- Smart Contracts provide:
- **Autonomy**
- **Trust**
- **Backup**
- **Safety**
- **Speed**
- **Savings**
- **Accuracy**

CBSA Exam Crash Course

Contracts versus Smart Contracts

<i>Traditional contracts</i>	<i>Smart contracts</i>
 1-3 Days	 Minutes
 Manual remittance	 Automatic remittance
 Escrow necessary	 Escrow may not be necessary
 Expensive	 Fraction of the cost
 Physical presence (wet signature)	 Virtual presence (digital signature)
 Lawyers necessary	 Lawyers may not be necessary

Courtesy - PWC

CBSA Exam Crash Course



Smart Contracts :



Smart contracts define the rules and penalties around an agreement in the same way that a traditional contract does



Automatically enforce those obligations.



Several smart contracts can make up a dapp generally

CBSA Exam Crash Course



Types of functions which are required in a smart contract:



Constructor Function - The function which is called only once, when you deploy the smart contract. For example it can be used to receive the initial Ether sent to it, at the time of deployment.



Fallback Function - The function without a name (literally no name, defined as `function (){ code... }`) which is invoked when someone sends Ether to the address of your smart contract. In the lack of this function, Ether sent to the smart contract will be rejected.

CBSA Exam Crash Course

Smart contracts provide security that is better to traditional contracts.

Cut transactional costs associated with traditional contracting.

Smart contracts on Ethereum network run on something called Ethereum Virtual Machine (EVM)

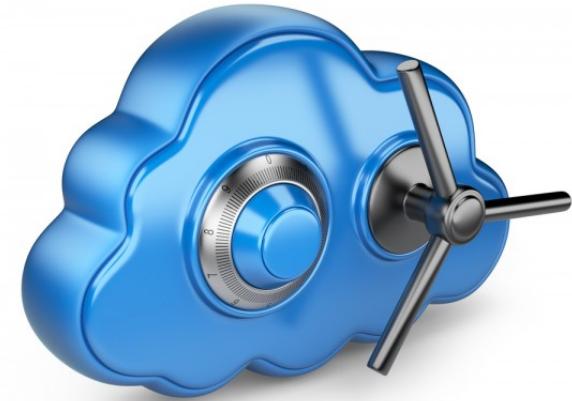
The Decentralized Applications (DApps) running on the Ethereum network are basically complex Smart Contracts.

Smart Contracts Enforcement

Basics of Ethereum states that all modifications to a contract's data must be performed by its code.	Modification of a contract's data requires a blockchain user to send requests to its code. This process kickoff determines whether and how to fulfill those requests.	A traditional database uses an "enforced stored procedure".	Think of this approach as "pre defined rules"
--	---	---	---

Smart Contracts Legal Enforcement

- Smart Contracts may not be legally enforceable. Especially across borders.
- Could be used as evidence
- Think of a vending machine where you put in the required funds to get the drinks or food...



CBSA Exam Crash Course



Smart Contract

Ethereum Account Type (Just like User Account)



Address



Balance

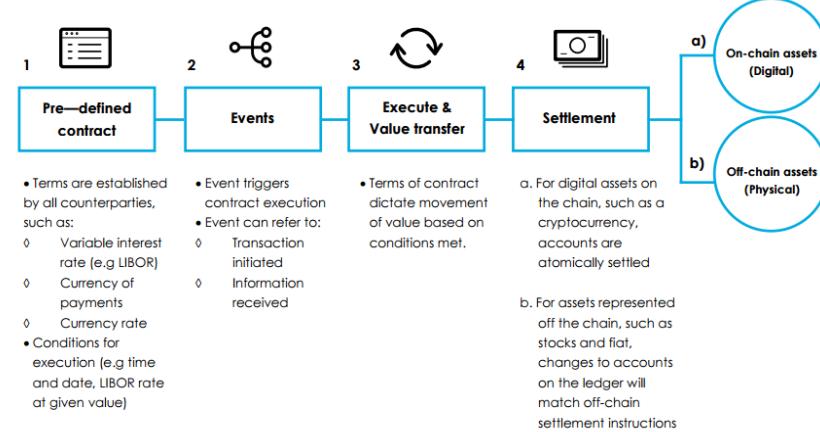


Code



State

```
0x16E0022b17B...
0 Ether
contract Counter {
    uint counter;
    function Counter() public {
        counter = 0;
    }
    function count() public {
        counter = counter + 1;
    }
}
```



Smart Contracts

Smart Contracts workflow ([Blockgeeks.com](https://blockgeeks.com))

CBSA Exam Crash Course

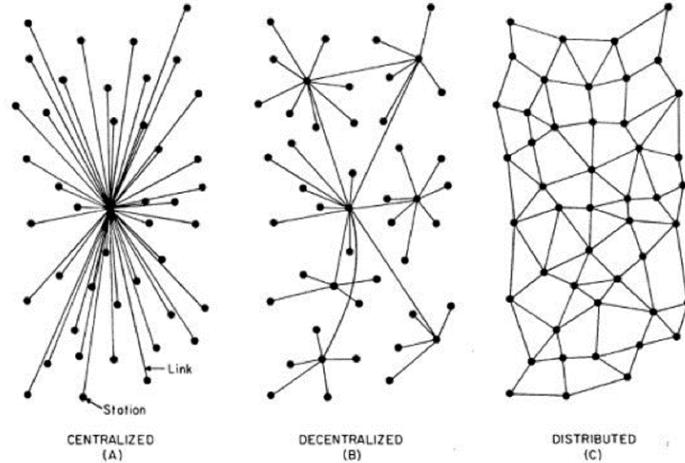


Image Blockgeeks

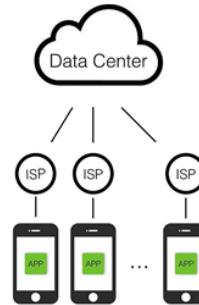
dApps 101

- Dapps are “decentralized applications” - These applications run on a P2P network of computers, instead of a one computer.
- One or more Smart contracts.
- Not Centralized

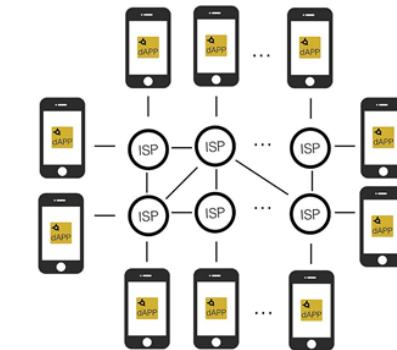
Dapps

- Open-source
- Data & the records of operation of application to be cryptographically stored on ledger
- Uses cryptographic token
- Generate tokens
- Decentralized P2P Network

Apps



dApps



dapps

dApps



Dapps

- Open-source
- Access with Mist Browser
(Ethereum)
- Collection of Smart Contracts

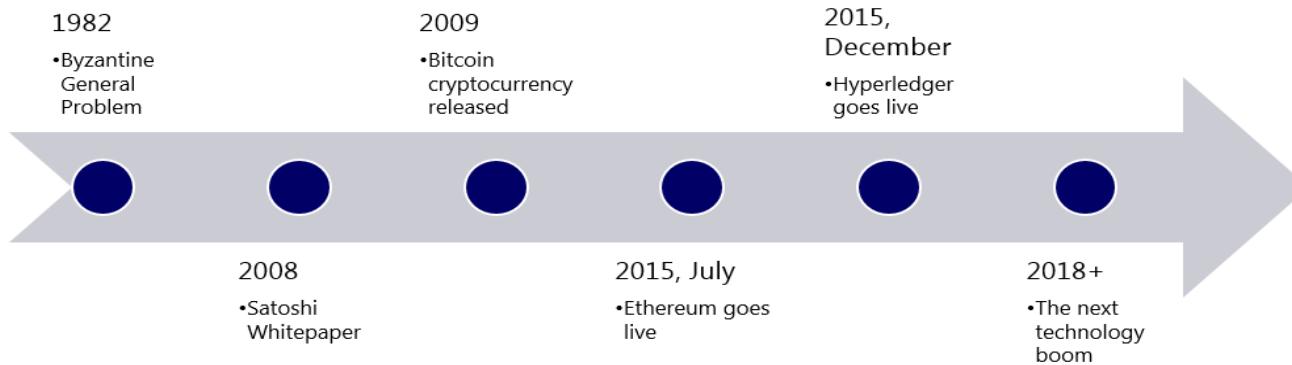
CBSA Exam Crash Course

Objective

Brief history of blockchain

CBSA Crash Course

- History of Blockchain

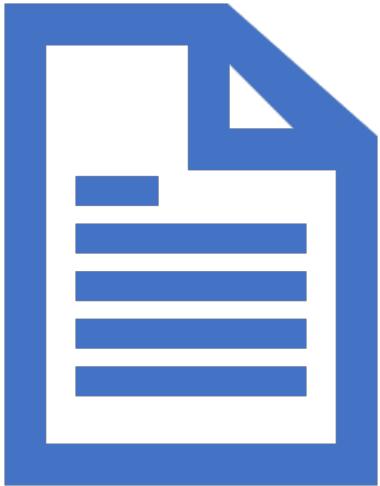


CBSA Exam Crash Course

Objective

**The programming languages of the most common
blockchains**

Go and Solidity



CBSA Exam

- Solidity – Ethereum
- Go – Hyperledger

CBSA Exam Crash Course

*Estimated Stats

PROGRAMMING LANGUAGES SUPPORTED BY BLOCKCHAIN-BASED PROJECTS



Courtesy Freecodecamp

<https://medium.freecodecamp.org/the-most-popular-programming-languages-used-in-blockchain-development-5133a0a207dc>

CBSA Exam Crash Course

Objective

**Common testing and deployment practices for blockchains
and blockchain-based apps**

CBSA Exam Crash Course

SDLC:

- SDLC or the Software Development Life Cycle is a process that produces software with the highest quality and lowest cost in the shortest time.
- SDLC includes a detailed plan for how to develop, alter, maintain, and replace a software system.

CBSA Exam Crash Course

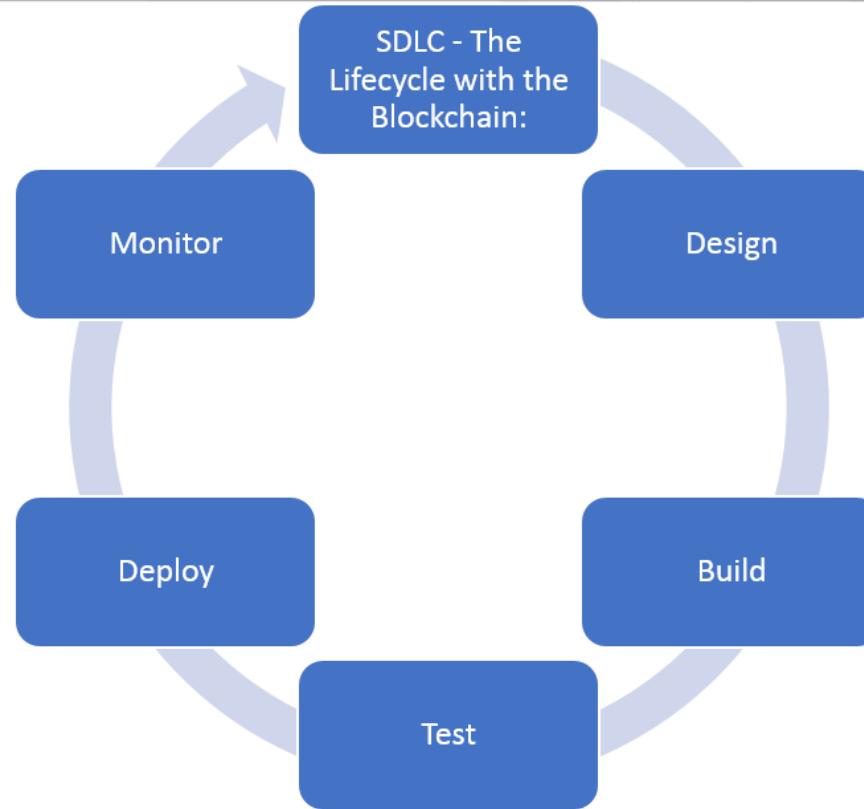
Some SDLC models are:

- Agile
- Waterfall
- Spiral

Note that you can build a dAPP, for example, using SDLC

SDLC

SDLC



CBSA Exam Crash Course

Design:

- Design for Peer to Peer (P2P)
and not Client Server
- Plan for Security (Algos,
encryption, etc)

CBSA Exam Crash Course

Build on Languages

- Java
- Python
- Solidity
- Go (Golang)
- PHP
- C++

Build on Frameworks

- PHP:
- Symphony
 - Fuel PHP
- Ethereum Solidity:
- Embark
 - Open Zeppelin

CBSA Exam Crash Course

Test Networks:

- Jasmine
- Carmine
- PhantomJS
- Truffle (Ethereum)
- Metamask (Ethereum)

CBSA Exam Crash Course

Deploying:

- Jenkins
- Docker
- Terraform
- Kubernetes
- Vagrant
- Truffle (Ethereum)
- Parity (Ethereum)

CBSA Exam Crash Course

Monitoring your resources:

- Nagios
- New Relic
- Bitnama
- Azure Monitor (Azure)
- Stackdriver (GCP/AWS)
- Etherscan (Ethereum)
- Etherstats (Ethereum)

CBSA Exam Crash Course

Value Creation

Value Creation

- Value Creation of the blockchain technology
- **Costing**
- **Security**
- **Privacy**
- **Efficiency**
- **Open source**



CBSA Exam Crash Course



VALUE CREATION OF THE
BLOCKCHAIN
TECHNOLOGY WITH
SMART CONTRACTS



SMART CONTRACT IS A
TERM USED TO DESCRIBE
COMPUTER PROGRAM
CODE THAT IS CAPABLE OF
FACILITATING,
EXECUTING, AND
ENFORCING THE
NEGOTIATION OR
PERFORMANCE OF AN
AGREEMENT USING
BLOCKCHAIN
TECHNOLOGY.
(CONTRACT)



THE ENTIRE PROCESS IS
AUTOMATED CAN ACT AS
A COMPLEMENT, OR
SUBSTITUTE, FOR LEGAL
CONTRACTS, WHERE THE
TERMS OF THE SMART
CONTRACT ARE
RECORDED IN A
COMPUTER LANGUAGE AS
A SET OF INSTRUCTIONS

CBSA Exam Crash Course



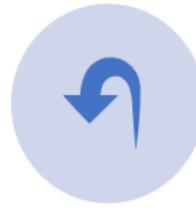
VALUE CREATION OF THE
BLOCKCHAIN TECHNOLOGY
WITH TOKENS



TOKENS ARE USED AS A STORE
OF VALUE AS ENTRIES ON A
BLOCKCHAIN LEDGER.



YOU OWN THESE 'TOKENS'
BECAUSE YOU HAVE A KEY
THAT LETS YOU CREATE A NEW
ENTRY ON THE LEDGER, RE-
ASSIGNING THE OWNERSHIP
TO SOMEONE ELSE.



YOU DON'T STORE TOKENS ON
YOUR COMPUTER, YOU STORE
THE KEYS THAT LET YOU
REASSIGN THE QUANTITY.



THESE ARE DIGITAL
RESOURCES WHICH YOU
CONTROL AND YOU CAN
REASSIGN CONTROL TO
SOMEONE ELSE.

CBSA Exam Crash Course



VALUE CREATION
OF THE
BLOCKCHAIN
TECHNOLOGY
SMART CONTRACTS
PROVIDE:



AUTONOMY



TRUST



BACKUP



SAFETY



SPEED



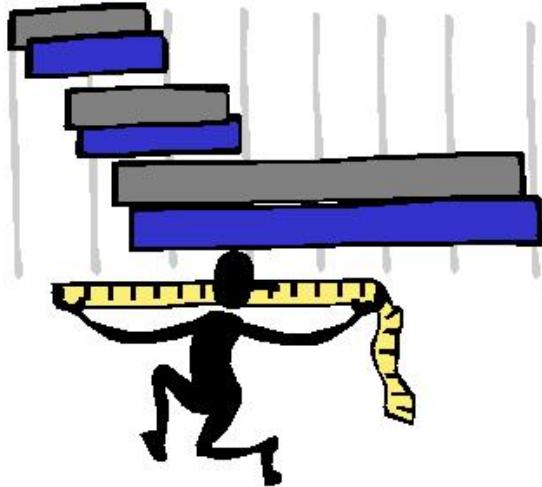
SAVINGS



ACCURACY

Value Creation

CBSA Exam Crash Course



End Results Benefits Could Be?

- Benefits of the Value Creation of the blockchain technology should end in?
- **CAPEX Reduction.**
- **OPEX Reduction**
- **Permissioned Access (Security)**
- **Increased Privacy**
- **Efficiency by reducing intermediaries. (Less accountants, Attorneys, Custom Agents, Lenders, etc.)**
- **Risk Reduction(Less Human Error)**
- **Numerous other value added benefits**

CBSA Exam Crash Course

Blockchain Key Components

CBSA Exam Crash Course

Blockchain Key Components



CRYPTOGRAPHY



P2P NETWORK



SHARED
DIGITAL LEDGER



CONSENSUS
ALGORITHM



VALIDITY RULES



VIRTUAL
MACHINE

CBSA Exam Crash Course

Blockchain Key Components

- Cryptography for transactions.
- Recorded, encrypted and secured between peers in blockchain.
- No need for a centralized authority.

CBSA Exam Crash Course

Blockchain Key Components

- P2P Network connect the blockchain nodes
- All computers share responsibility on the network
- Workloads are shared

CBSA Exam Crash Course

Blockchain Key Components

- Shared Digital Ledger is a data structure managed inside the node application.
- Distributed Database held and updated independently by each participant (or node) in a large network.



CBSA Exam Crash Course

The Consensus algorithm is implemented as part of the node application for how the ecosystem comes to a single view of the ledger.

- Different ecosystems have different methods for attaining consensus
- Determines method for “World State”

CBSA Exam Crash Course

Blockchain Key Components

- Validity Rules (validation) state how the user and the transactions will be validated.



CBSA Exam Crash Course

Blockchain Key Components

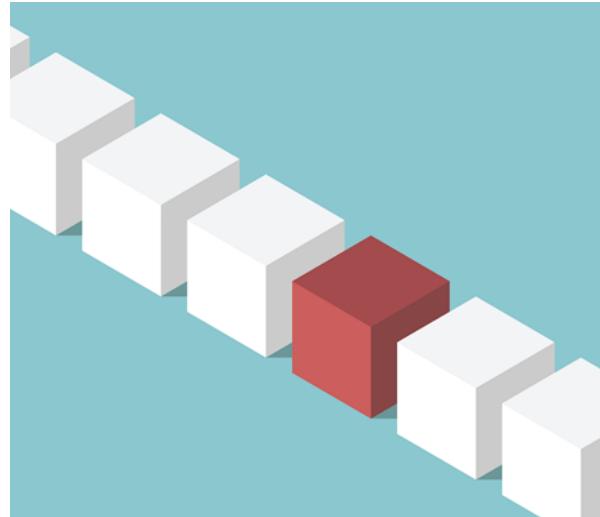
- Virtual Machines are a representation of a server created by a computer program and operated with instructions embodied in a language.
- Ethereum and Bitcoin use VMS. We will discuss Hyperledger shortly
- For Example the virtual machine lives in the Ethereum node applications

IBM Blockchain as a Service

Blockchain Terminology

Hyperledger Terminology

- **Block** An ordered set of transactions that is cryptographically linked to the preceding block(s) on a channel.
- **Chain** The ledger's chain is a transaction log structured as hash-linked blocks of transactions.

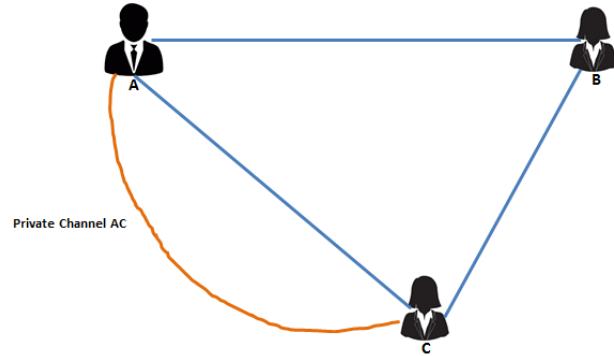


Hyperledger Terminology

- **Chaincode** - A smart contract is code – invoked by a client application external to the blockchain network – that manages access and modifications to a set of key-value pairs in the World State
- Chaincode services are secured and lightweight.
- The environment is a “locked down” and is a secured container with a set of signed base images which contains secure OS and Chaincode language, runtime and SDK images for Golang, Java, and Node.js.

Hyperledger Terminology

- A channel is a private blockchain overlay which allows for data isolation and confidentiality.
- A channel-specific ledger is shared across the peers in the channel, and transacting parties must be properly authenticated to a channel in order to interact with it.



Hyperledger Terminology

- Endorsement refers to the process where specific peer nodes execute a chaincode transaction and return a proposal response to the client application.



Hyperledger Terminology

- Membership services provide identity, privacy, and confidentiality to the network.
- Reputation Manager enables auditors to view transactions pertaining to a participant, providing that each auditor has been granted proper access authority, based on the role of the participants.
- Blockchain services manages the distributed ledger through a peer to peer protocol that is built on HTTP/2.

Hyperledger Terminology

- A **Participant** is an actor in a business network. A participant might represent an individual or an organization.
- A participant can create assets and share assets with other participants.
- A participant can interact with assets by submitting transactions
- A participant has an identity set that can be validated to prove the identity of that participant.

Hyperledger Terminology

- World State is also known as the “current state”, the world state is a component of the HyperLedger Fabric Ledger
- The world state represents the latest values for all keys included in the chain transaction log.



IBM Blockchain as a Service

Blockchain Architecture 101

Blockchain Architectures

Architecture perspective

- Blockchains are decentralized generally.
- Notable exceptions like Ripple
- Peer to Peer networks
- Security is built in

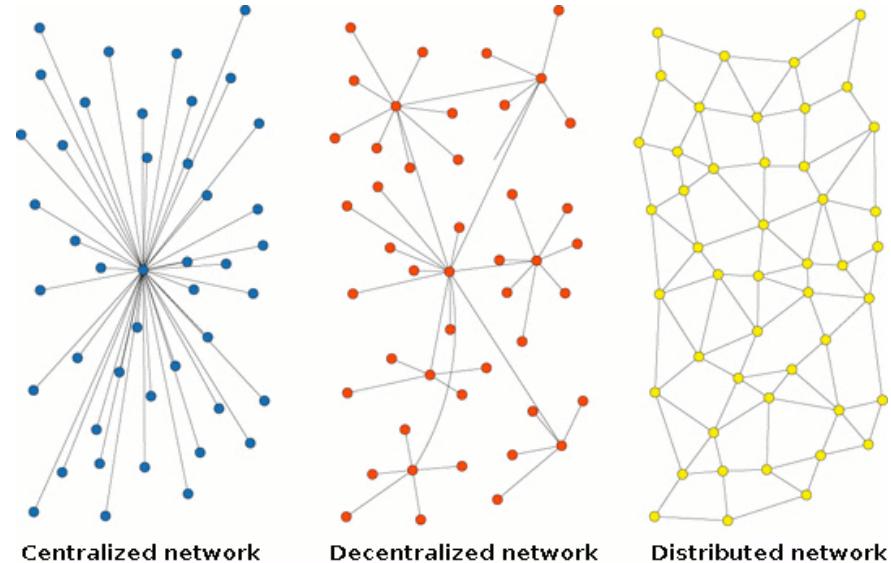
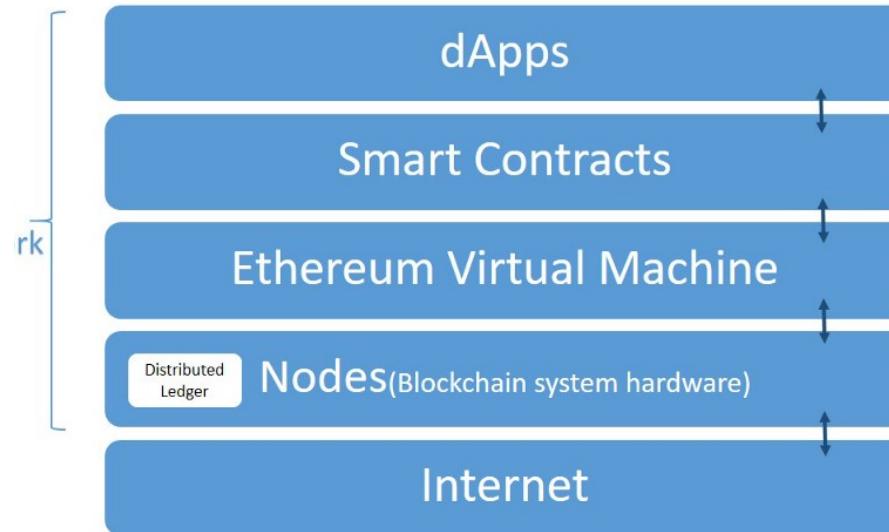


Diagram - Wallstreet Technologist

Blockchain Architectures

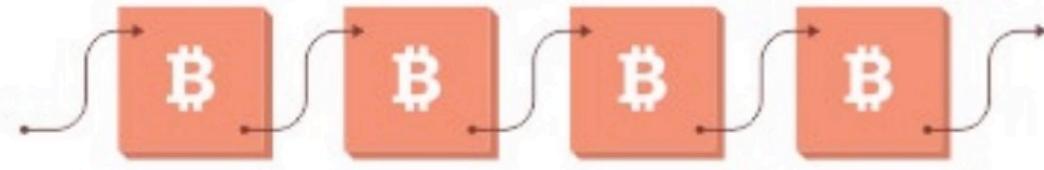
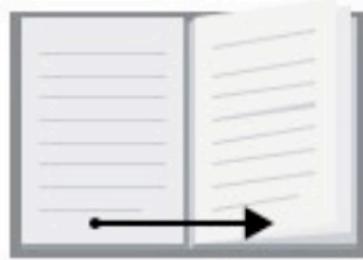
- Blockchain
- A decentralized distributed ledger (like a data structure) where data is being stored inside blocks in the form of transactions.
- Peer to Peer resources distributed
- Most blockchains scale horizontally.
- Transaction processing can be dependent on Consensus algo...



Blockchain Architectures

Blockchain

- A decentralized distributed ledger (like a data structure) where data is being stored inside blocks in the form of transactions.
- Most blockchains scale horizontally.
- Transaction processing can be dependent on Consensus algo...



Blocks in a chain refer to previous blocks, like page numbers in a book.

Blockchain Architectures

- Distributed Ledgers ...
- Removes the dependency on the trusted third party for recording the data in blocks.
- Complex algorithms are required to avoid malicious activities.
- Each block is built on top of the previous Block which allows the immutability to be achieved.

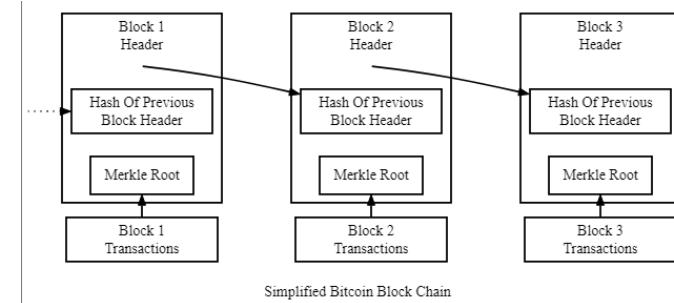


Diagram – [Bitcoin.org](https://bitcoin.org)

Blockchain Architectures



Distributed Ledgers ...



Immutability means, very difficult to fake/alter a block & very easy to detect the tampering.



This all exist in the memory of the computers and runs as a computer process.



Every participant of the Blockchain contains almost same copy of the Blockchain ledger.

Blockchain Architectures

Block metadata contains:

- version - the current version of the block structure
- previous block header hash - the reference this block's *parent block*
- merkle root hash - a cryptographic hash of all of the transactions included in this block
- time - the time that this block was created
- nBits - the current *difficulty* that was used to create this block
- nonce ("number used once") - a random value that the creator of a block is allowed to manipulate

Blockchain Architectures

A genesis block is the first block of a block chain and then come the branches

- Block Categories
- Main branch blocks
- Side branch blocks
- Orphan blocks

Blockchain Architectures

Blockchain Scalability Dilemma

Blockchains do not scale well.

Why.. Because it's a consensus protocol.

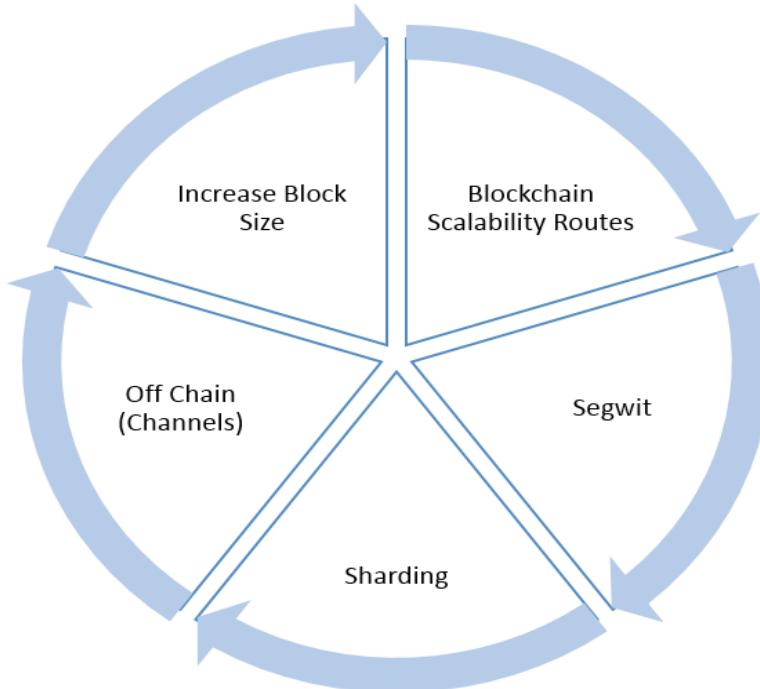
Every node needs to process the transaction

For Scalability = tradeoff is needed –

low transaction throughput vs high level of decentralization.

Blockchain Architectures

Scaling



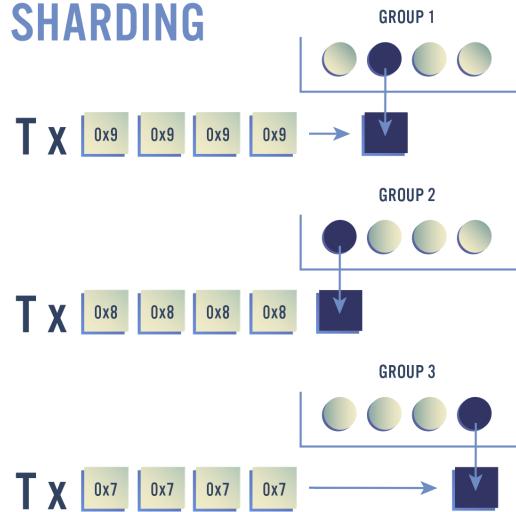
Blockchain Architectures

SegWits

- SegWit = Segregated Witness - Segregated Witness in short, means to separate transaction signatures.
- Is the process by which the block size limit on the BTC blockchain is increased by removing signature data from Bitcoin transactions.
- By removing signatures this frees up capacity to add more transactions to the chain.

Blockchain Architectures

SHARDING



Sharding

- The processing of the blockchain is separated into different shards and each part of the state would be stored by different nodes in the network. Nodes only processes shards
- Increases Processing
- Increases Security concerns

Blockchain Architectures



OFF CHAIN (STATE CHANNEL)



STATE CHANNELS ARE A ROUTINE BY WHICH BLOCKCHAIN PROCESSES THAT COULD BE PROCESSED ON THE BLOCKCHAIN INSTEAD GET CONDUCTED OFF OF THE BLOCKCHAIN.



Increase Block Size



With forking generally the block size has been increased. The goal of the increase of block size is to



Allow larger transaction size. (eg 1MB to 8MB)



Increase network efficiency



Could affect mining profitability



Example Bitcoin Cash is a hard fork orchestrated by a portion of the community that wanted Bitcoin to scale by increasing its block size from the current 1MB to 8MB.

CBSA Exam Crash Course

Enterprise Blockchain Comparison

Blockchain Feature Comparison

	Ethereum	Hyperledger	Corda	Ripple	Quorum
Industry	Cross	Cross	Financials	Financials	Cross
Governance	Developers	Linux Foundation	R3 Consortium	Ripple Labs	Developers and JP Morgan
Ledger Type	Permission-less	Permissioned	Permissioned	Permissioned	Permissioned
Consensus	PoW PoS TBD	Pluggable	Pluggable	Probabilistic Voting	Majority Voting
Smart Contracts	Yes	Yes	Yes	No	Yes
Crypto \$	Ether	NA	NA	XRP	NA
					HFS Research

Hyperledger Overview

BIPs – Bitcoin Improvement Proposals

CBSA Exam Crash Course

- A Bitcoin Improvement Proposal (BIP) is a design document for introducing features or information to Bitcoin.
- The BIP should provide a concise technical specification of the feature and a rationale for the feature.



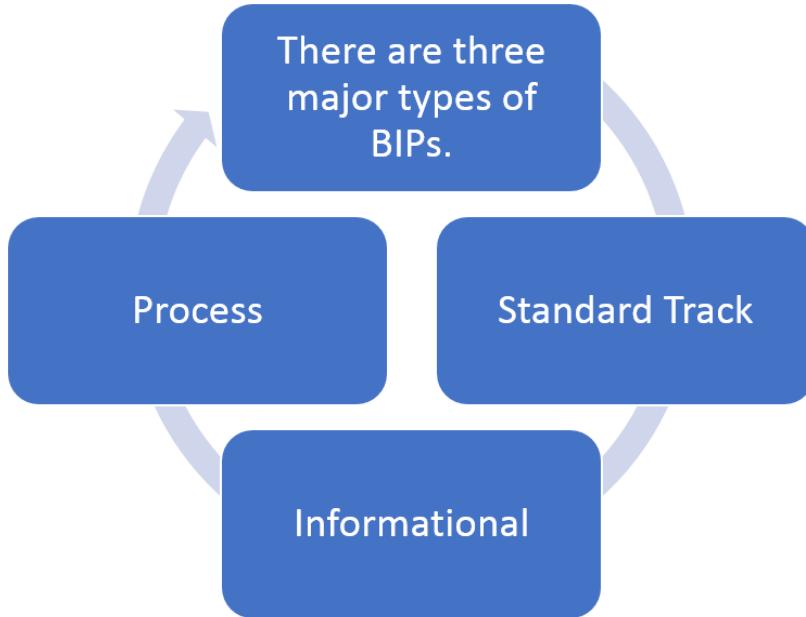
CBSA Exam Crash Course

- This is the standard way of communicating ideas since Bitcoin has no formal structure.
- Any developer or anyone from anywhere in the world can propose a BIP.
- The whole Bitcoin community of users, miners, developers, and investors to vote on it.



CBSA Exam Crash Course

Learn these BIP types..



CBSA Exam Crash Course



Standard Track BIPs entail making changes to the network protocol, block, or transaction validation method.



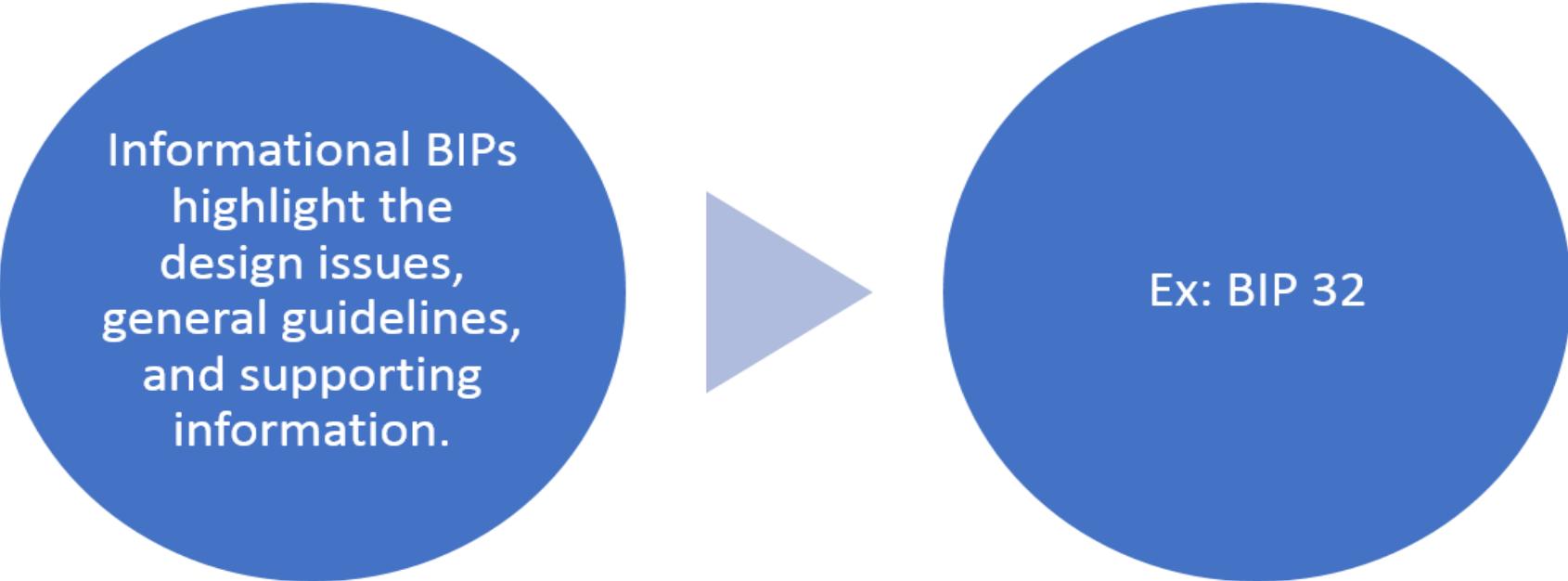
It also intends to affect the interoperability of the two versions of BIPs or Bitcoin.



Requires community consensus.

Ex= BIP 91

CBSA Exam Crash Course



Informational BIPs highlight the design issues, general guidelines, and supporting information.

Ex: BIP 32

CBSA Exam Crash Course

Process BIPS describe and or propose a change in the process.

Similar to Standards
Track BIPs and require community consensus.

Ex: BIP 2

CBSA Exam Crash Course

Hyperledger Project Overview

CBSA Exam Crash Course

- Hyperledger is an open source project that came out of the Linux Foundation and was created in order to help advance cross-industry blockchain technologies.
- It is essentially a global open source collaboration involving leaders from numerous industries.



HYPERLEDGER PROJECT

CBSA Exam Crash Course

- Hosted by the Linux Foundation which provides a governance structure and oversight to the Hyperledger community.
- Open Source
- Uses a modular umbrella approach to enterprise blockchains



CBSA Exam Crash Course

The Hyperledger Project consists of the following

- Infrastructure - Ecosystems that accelerate open development and commercial adoption
- Frameworks – A portfolio of differentiated approaches to business blockchain frameworks developed by a growing community of communities



CBSA Exam Crash Course

The Hyperledger Project consists of the following

- Tools - Typically built for one framework, and through common license and community of communities approach, ported to other frameworks



CBSA Exam Crash Course

Hyperledger Portfolio

Hyperledger Portfolio

Hyperledger Modular Umbrella Approach

Infrastructure

Technical, Legal,
Marketing, Organizational

Ecosystems that accelerate
open development and
commercial adoption



Cloud Foundry

Node.js

Hyperledger

Open Container
Initiative

Frameworks

Meaningfully differentiated approaches
to business blockchain frameworks
developed by a growing community of
communities

Hyperledger
Fabric

Hyperledger
Iroha

Hyperledger
Sawtooth

Hyperledger
Burrow

Hyperledger
Indy

Tools

Typically built for one framework, and through
common license and community of communities
approach, ported to other frameworks

Hyperledger
Explorer

Hyperledger
Composer

Hyperledger
Cello

Hyperledger
Quilt



6

CBSA Exam Crash Course

Hyperledger Framework

CBSA Exam Crash Course

Framework	Application
Indy	Distributed ledger and utility library
Iroha	DLT, Smart Contract Engine, Utility Libraries (Mobile)
Sawtooth	DLT, Smart Contract Engine
Burrow	Permissioned smart contract application engine
Fabric	DLT, Smart Contract Engine

CBSA Exam Crash Course

Framework	Smart Contract Technology	Smart Contract Type	Language(s) for Writing Smart Contracts
Hyperledger Burrow	Smart contract application engine	On-Chain	Native language code
Hyperledger Fabric	Chaincode	Installed	Golang (> v1.0) or Javascript (> v1.1)
Hyperledger Indy	None	None	None
Hyperledger Iroha²	Chaincode	On-chain	Native language code
Hyperledger Sawtooth	Transaction families	On-Chain and Installed	C++, Go, Java, JavaScript, Python, Rust, or Solidity (through Seth)

CBSA Exam Crash Course

- **Hyperledger Fabric:** Intended as a foundation for developing applications or solutions with a modular architecture
- Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play



HYPERLEDGER PROJECT

CBSA Exam Crash Course

Hyperledger Features

CBSA Exam Crash Course

- Hyperledger Fabric is a blockchain implementation that is designed for deploying a modular and extensible architecture.
- It has a modular subsystem design so that different implementations can be plugged in and implemented over time.
- Hyperledger Fabric is essentially enterprise driven and supports the enterprise fully

CBSA Exam Crash Course

Modular and extensible

- This means modularity in all components of all frameworks.
- Consensus layer
- Smart contract layer
- Communication layer



CBSA Exam Crash Course

Modular and extensible (cont)

- Communication layer
- Data store
- Identity services (root of trust—to identify the participants)
- APIS
- And more components

CBSA Exam Crash Course

Interoperability

- This principle is around backward interoperability and not focused on the interoperability between the various Hyperledger project-powered blockchain systems or business networks.
- API Suite

CBSA Exam Crash Course

Secure Solutions

- Enterprise and therefore business network security is paramount.
- The focus is on the interaction between components and the structure that governs the permissioning nature of permissioned blockchains.
- Enterprise prefer permissioned blockchains

CBSA Exam Crash Course

Token or CryptoCurrency Agnostic

- Hyperledger projects do not use crypto-assets, cryptocurrency, tokens, or coin-like constructs as incentive mechanics to establish trust systems.
- *Behlendorf and the team at Hyperledger remain "sympathetic" to the interest in ICOs, but don't see a future where Hyperledger itself issues a crypto token.*

CBSA Exam Crash Course

Rich APIS

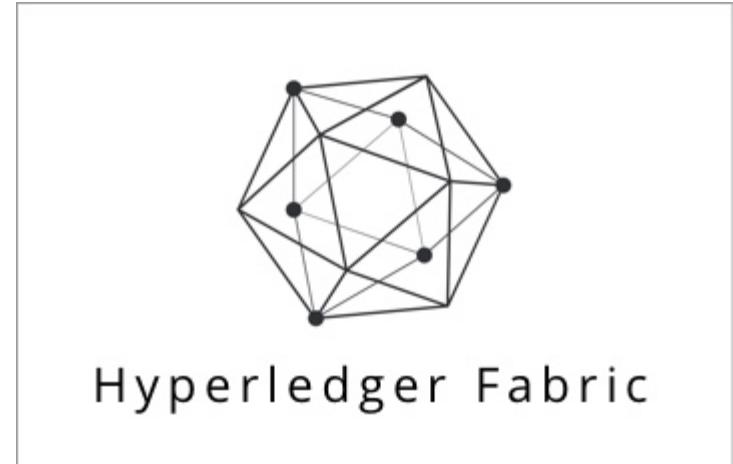
- The focus here is to ensure that blockchain systems have not only enterprise middleware access but instead access to business networks, existing participants, and new systems without exposing the details of blockchain powered business networks.
- Check Github for latest APIs

CBSA Exam Crash Course

Hyperledger Fabric

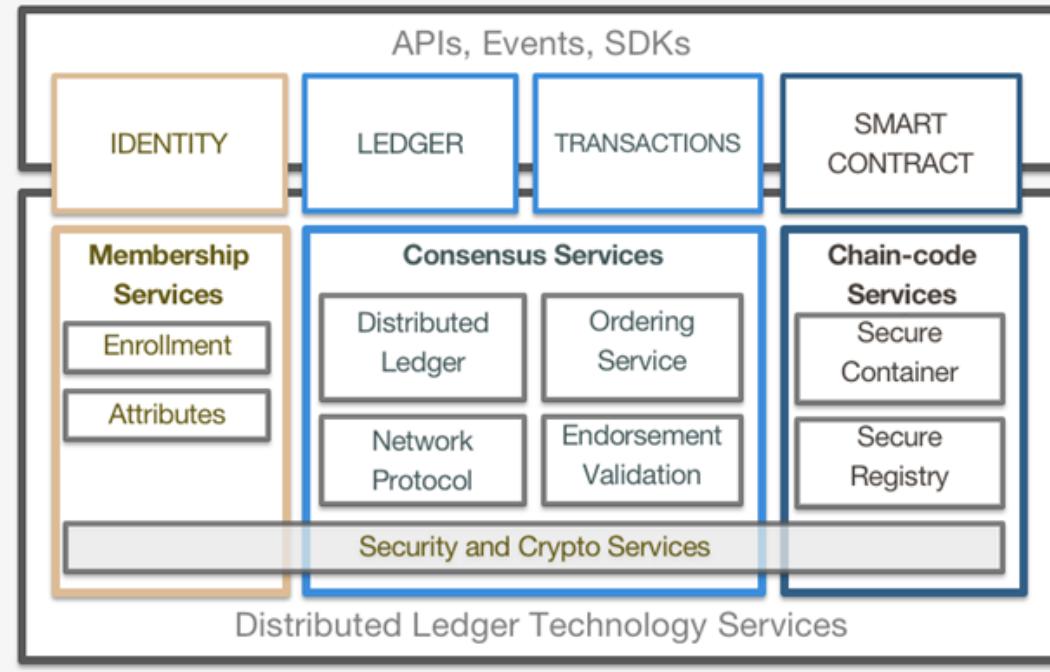
CBSA Exam Crash Course

- Hyperledger Fabric follows a modular design, and the following are some of the possible components or modules that can be plugged in and implemented.
- Lets discuss some of the main modules



CBSA Exam Crash Course

Reference Architecture



IDENTITY

Pluggable, Membership, Privacy and Auditability of transactions.

LEDGER | TRANSACTIONS

Distributed transactional ledger whose state is updated by consensus of stakeholders

SMART CONTRACT

“Programmable Ledger”, provide ability to run business logic against the blockchain (aka smart contract)

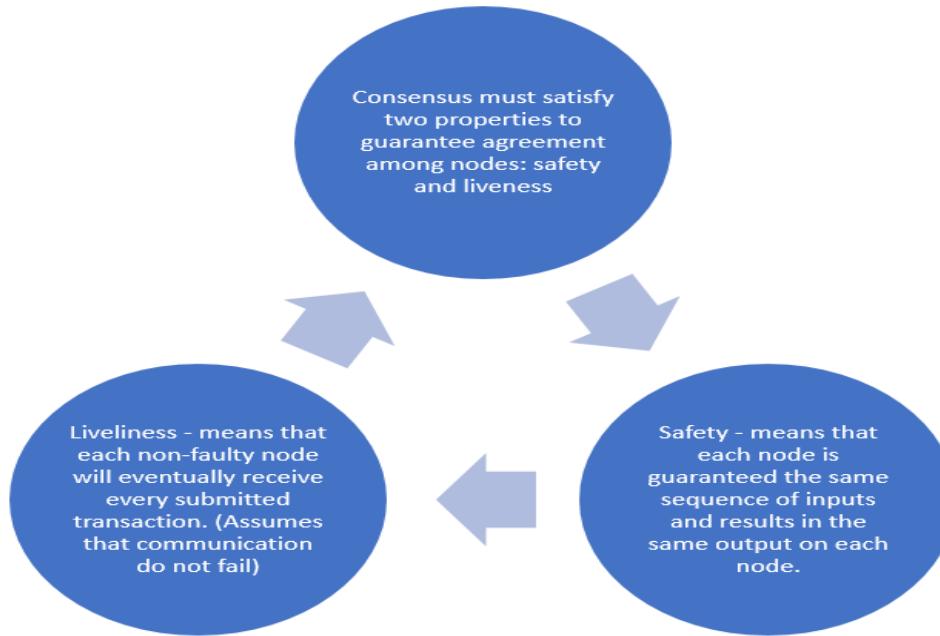
APIs, Events, SDKs

Multi-language native SDKs allow developers to write DLT apps

CBSA Exam Crash Course

Hyperledger Fabric Consensus

CBSA Exam Crash Course



CBSA Exam Crash Course

- Hyperledger makes use of the permissioned voting-based consensus from the pool of other consensus named the **lottery-based consensus**. (Kafka in Hyperledger Fabric Ordering Service)
- Voting-based algorithms are advantageous in that they provide low-latency finality.
- More Nodes = More Time to reach Consensus...
- Trade off between Scalability and Performance

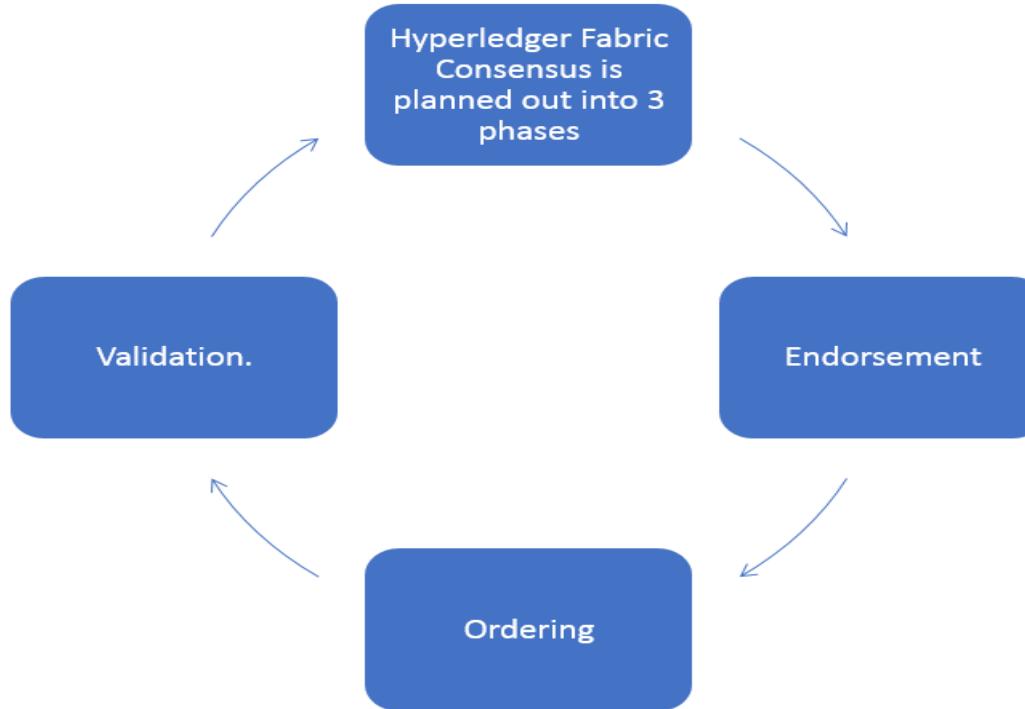
CBSA Exam Crash Course

Endorsement is driven by policy (m out of n signatures) upon which participants endorse a transaction.

Ordering phase will get the endorsed transaction and agrees to the order to be committed to the ledger.

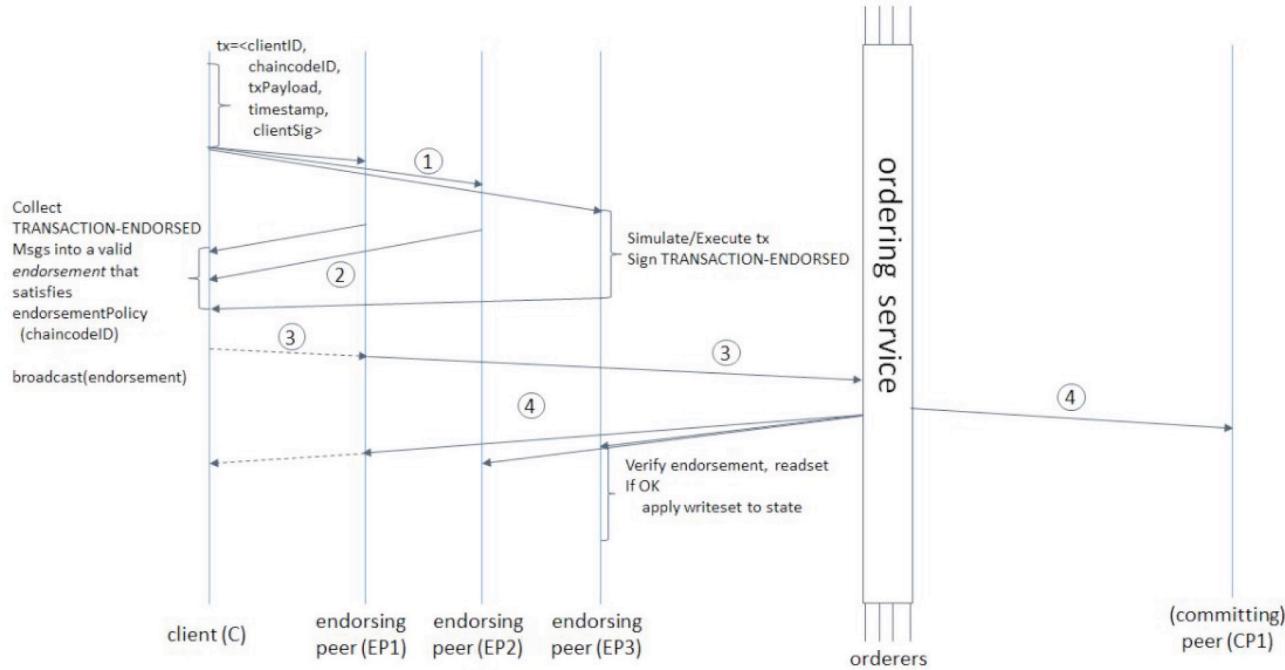
Validation takes a block of ordered transactions and validates the correctness of the result.

CBSA Exam Crash Course



CBSA Exam Crash Course

- Transaction Flow (Linux Foundation)



Review Question

Voting-based algorithms are advantageous because they provide _____

- A) low-latency finality
- B) high-performance
- C) low-latency consensus
- D) high-security

Review Question

Hyperledger Fabric Consensus is planned out into 3 phases.
Which one is NOT a phase?

- A) Endorsement
- B) Ordering
- C) Validation
- D) Segregation

CBSA Exam Crash Course

Hyperledger Ledger Basics

CBSA Exam Crash Course

Ledger Basics

- The ledger is the sequenced, tamper-resistant record of all state transitions.
- State transitions are a result of chaincode invocations (“transactions”) submitted by participating parties.
- Each transaction results in a set of ***asset key-value pairs*** that are committed to the ledger as creates, updates, or deletes.

CBSA Exam Crash Course

Fabric Ledger has two parts:

State data: Representation of current state of the assets. Asset state data can be changed upon changes to the state of the data.

Transaction Logs: Record of all the transactions (in the order they are received) which modified the state data, and once the data is written it is immutable and cannot be modified.

CBSA Exam Crash Course

What DB is used?

The ledger system in Hyperledger fabric uses levelDB. By definition, LevelDB allows concurrent writers to safely insert data into the database by providing internal synchronization

State database options include LevelDB and CouchDB.

LevelDB is the default key-value state database embedded in the peer process.

CouchDB is an optional alternative external state database.
(Binary data)

CBSA Exam Crash Course

What DB is used for Where and Why?

	Transaction Logs	State Date (World)
Type	Immutable	Mutable
Operations	Create, Retrieve	ALL-CRUD
DC	levelDB	levelDB/CouchDB
Attitude	Embedded in peers	Key-Value Paired(JSON, Binary)
Query	Simple	Couch DB for Complex

CBSA Exam Crash Course

Hyperledger Composer

CBSA Exam Crash Course

- Hyperledger Composer
Playground is a tool which provides an environment that quickly models and tests a blockchain network.
- The composer has a simple Graphical UI to edit and test the business blockchain network.



<https://composer-playground.mybluemix.net/login>

CBSA Exam Crash Course

Hyperledger Composer(Fabric Composer):

- Fabric Composer is a newer open-source application development framework, which simplifies the creation of Hyperledger Fabric blockchain applications, thus reducing the time and complexity of development.
- The tool aims at helping users to create blockchain applications based on Hyperledger Fabric without needing to know the low-level (Go Programming) details involved in blockchain networks

CBSA Exam Crash Course

- If you want to build your blockchain application directly on Hyperledger Fabric you have to write your Chaincode in ***GO or Java Programming Language*** which is comparatively different than JavaScript because its composer is quite easy to code smart contract using Model file (.cto) and angular JavaScript.
- Hyperledger Composer primarily uses JavaScript for ***chaincode*** development.

CBSA Exam Crash Course

Hyperledger Composer has following main components

- Business Network Archive: Capturing the core data in a business network including the business model, transaction logic, and access controls, the Business Network Archive packages these elements up and deploys them to a runtime.
- Stored as “.bna” files.

CBSA Exam Crash Course

Hyperledger Composer has following main components

- Composer Playground: This web-based tool allows developers to learn Hyperledger Composer, model out their business network (domain), test that network, and deploy that network to a live instance of a blockchain network
- CRUD Capacity
- Templates

CBSA Exam Crash Course

- Composer uses what's called connection profiles to define the system to connect to.
- A connection profile is a JSON document that acts as part of a business network card.
- The connection profile is most often provided by creators of the system they refer to

CBSA Exam Crash Course

- You can use queries to get data about the state of the blockchain. Queries are defined within a business network, and can include variable parameters. Queries are sent using the Composer API.
- Events in Composer are defined in the business network definition in the same way as participants or assets. Events are emitted by the transaction processor function once it has been defined. An event indicates to external systems that something important has occurred on the ledger. Applications subscribe to emitted events using the composer-client API

CBSA Exam Crash Course

Developers of the business network can create a set of access controls.

Access controls are rules that determine which assets participants have access to in the business network and the conditions in which they can access them.

A historian is a specialized type of registry that records successful transactions conducted on the business network

CBSA Exam Crash Course

Hyperledger Composer consists of the following high-level components:

- Execution Runtimes
- JavaScript SDK
- Command Line Interface
- REST Server
- LoopBack Connector
- Playground Web User Interface
- Yeoman code generator
- VSCode and Atom editor plugins

Hyperledger Composer

Hyperledger Composer modeling language, an object-oriented modeling language that defines the domain model for a business network definition.

- The modeling language is saved as a .cto file.

The CTO file contains:

- A single namespace, in which all resource declarations are implicitly.
- A set of resource definitions that includes assets, transactions, participants, and events
- The option to import resources from other namespaces

CBSA Exam Crash Course

Namespace

There is a system namespace which contains base definitions of asset, event, participant, and transactions. These base definitions are abstract types that are implicitly extended by all new assets, events, participants, and transactions

- Events and transactions in the system namespace are defined by an eventID or transactionID and a timestamp.
- The system namespace also includes definitions of registries, historian records, identities, and system transactions

Hyperledger Composer



PARTICIPANTS REPRESENT ACTORS THAT INTERACT WITH THE BLOCKCHAIN APPLICATION THROUGH TRANSACTIONS.



ASSETS MODEL THE ITEMS TO BE STORED IN THE BLOCKCHAIN.
(REFERENCE VALUE)



TRANSACTIONS REPRESENT THE ACTUAL TRANSACTION REGISTERED ON THE BLOCKCHAIN LEDGER, INITIATED FROM A PARTICIPANT, RELATED TO ONE OR MORE ASSETS.



TRANSACTION PROCESSORS ARE USED WHEN A TRANSACTION IS INITIATED ON THE BLOCKCHAIN AND ALL NODES OF THE BLOCKCHAIN VALIDATE IT AND PERFORM SIDE EFFECTS

CBSA Exam Crash Course



IN COMPOSER,
RESOURCES ARE:



- ASSETS, PARTICIPANTS,
TRANSACTIONS, AND
EVENTS



- ENUMERATED TYPES



- CONCEPTS

CBSA Exam Crash Course

Resource definitions all have the following inherent properties. A namespace defined by the namespace of its parent file

- A name and an identifying field
- An optional super-type that the resource definition extends
- An optional “Abstract” declaration to indicate that this type cannot be created.
- A set of named properties defined. Properties and data are owned by each resource
- A set of relationships to other Composer types that are not allowed by the resource but may be referenced from the resource.

CBSA Exam Crash Course

Here is an example of Vehicle as a super-type, and a Car being considered an asset with a set of parts:

```
asset Car extends Vehicle {  
    o String model  
    --> Part[] Parts
```

CBSA Exam Crash Course

In composer, concepts are abstract classes that are not considered an asset, participant, or transaction

- Concepts do not have an identified by field because concepts cannot directly abstract concept Address {

- o String street
 - o String city default ="New York"
 - o String country default = "US"
 - o Integer[] counts optional

}

concept CanadaAddress extends Address {

- o String zipcode

}be stored in registries or referenced in relationships

CBSA Exam Crash Course

Other supported
programming
areas

Arrays

Primitive

Field Validators

Relationships

Imports

Decorators

Review Questions

The primary purpose of Hyperledger Composer is:

- a) Allowing blockchain applications to run on computers with slow processing power
- b) Accelerate the time to develop a blockchain application
- c) Make it easy to integrate blockchain technology into legacy systems
- d) Both B and C

Review Questions

The connection profile:

- a) Defines the participants that can connect to each other
- b) **Defines the system to connect to**
- c) Defines the systems to avoid
- d) Defines connections between assets in a network

Review Questions

Composer modeling language files are saved with which extension?

- a) .EXE
- b) .CTO
- c) .CML
- d) .CMP

Review Questions

A historian is:

- a) A specialized business network that only allows certain participants
- b) A specialized type of registry that records errors on the business network
- c) A specialized type of registry that records all successful transactions
- d) A specialized type of registry that records all participants on the network

Review Questions

Hyperledger Fabric business network is divided into three categories.

- a. Sawtooth, Fabric, and Indy
- b. Composer, Fabric, and Chaincode
- c. **Blockchain, Chaincode, and Membership**
- d. Blockchain, Registration, Identity

Review Questions

What application is used by Hyperledger Fabric to communicate with the network?

- a. JSON
- b. Binary
- c. SDK
- d. RPC API

CBSA Exam Crash Course

Hyperledger Fabric Playground

CBSA Exam Crash Course

- Playground makes the highly complex blockchain network easy for running blockchain testing.
- There is an online and offline version of Playground
- Online playground runs the business network in browser memory
- Local playground is deployed in Hyperledger Fabric instances.



HYPERLEDGER
COMPOSER

CBSA Exam Crash Course

- Playground is located here
- It will let you know if your running a supported version

x

Invalid version!



It looks like you've used an older version of Composer Playground before!

Clear local storage

CBSA Exam Crash Course

- Playground is a “sandbox”
- Use it to develop, test, validate, etc.
- Deploy a new Business Network
- Not a live blockchain

Welcome to Hyperledger Composer Playground!



In this web sandbox, you can deploy, edit and test business network definitions. Have a play and learn what Hyperledger Composer Playground is all about.

Let's Blockchain!

Not sure where to start? View our Playground tutorial.

CBSA Exam Crash Course

- Deploy a “Model”

```
/**  
 * My Pearson Student Training network  
 */  
namespace org.example.mynetwork  
asset Commodity identified by tradingSymbol {  
    o String tradingSymbol  
    o String description  
    o String mainExchange  
    o Double quantity  
    --> Trader owner  
}  
participant Pearson identified by tradeld {  
    o String tradeld  
    o String firstName  
    o String lastName  
}  
transaction Trade {  
    --> Commodity commodity  
    --> Trader newOwner  
}
```

CBSA Exam Crash Course

Hyperledger Chaincode

CBSA Exam Crash Course

- Chaincode writing you will want to make sure that you have the Go programming language installed and setup.
- Make sure that a directory is created for your chaincode application as a child

```
// Extract the function and args from the transaction proposal
fn, args := stub.GetFunctionAndParameters()
var result string
var err error
if fn == "set" {
    result, err = set(stub, args)
} else {
    result, err = get(stub, args)
}
if err != nil {
    return shim.Error(err.Error())
}
// Return the result as success payload
return shim.Success([]byte(result))
}
```

CBSA Exam Crash Course

- We can then implement the init function. **Init is called during chaincode instantiation, and it will initialize any data.**

Chaincode:

```
// Init is called during chaincode instantiation to initialize any data.  
func (t *SimpleAsset) Init(stub  
shim.ChaincodeStubInterface)  
peer.Response  
{  
}
```

CBSA Exam Crash Course

- Now our example chaincode application implements two functions that can be invoked via the **invoke function**.

```
// Set stores the asset (both key and value) on the ledger. If the key exists,  
// it will override the value with the new one  
func set(stub shim.ChaincodeStubInterface, args  
[]string) (string, error) {  
if len(args) != 2 {  
return "", fmt.Errorf("Incorrect arguments.  
Expecting a key and a value")  
}  
err := stub.PutState(args[0], []byte(args[1]))  
if err != nil {  
return "", fmt.Errorf("Failed to set asset: %s",  
args[0])  
}  
return args[1], nil  
}
```

Review Questions

The chaincode's interface implements the following functions

- a. open and close
- b. query and update
- c. init and run
- d. **invoke and init**

Review Questions

The “init” method is called when:

- a) there is an error in the code
- b) a chaincode receives an invoke function
- c) a chaincode receives an “instantiate” or “upgrade” transaction
- d) an asset is created

Review Questions

The “invoke” method is called in response to:

- a) receiving an transaction to process transaction proposals
- b) receiving an asset
- c) sending a transaction
- d) receiving an instantiate transaction

Review Questions

Every chaincode program must implement the:

- a) Chaincode panel
- b) **Chaincode interface**
- c) Chaincode policy
- d) Chaincode parameters

CBSA Exam Crash Course

Ethereum

CBSA Exam Crash Course

The total supply of ether and its rate of issuance was decided by the donations gathered on the 2014 presale of the currency.

- 60 million ether created to contributors of the presale
- 12 Million (20% of the above) were created to the development fund (early contributors and developers) and the remaining to the Ethereum Foundation
- 5 ethers are created every block (about 15 seconds) to the miner of the block
- 2-3 ethers may be sent to another miner (Uncle)

CBSA Exam Crash Course

- Most widely used Open Source Blockchain-based distributed computing application platform
- Mainly used for building & implementing smart contracts functionality
- It offers a Decentralized Virtual Machine aka Ethereum Virtual Machine (EVM)
- Initiated by Vitalik Buterin in 2013
- Ethereum's live Blockchain was launched on 30 July 2015

CBSA Exam Crash Course

- **Ether** is the native token of the Ethereum blockchain which is used to pay for transaction fees, miner rewards, and other services on the network.
- **Ethereum** is an open software platform based on blockchain technology that enables developers to write smart contracts and build and deploy decentralized applications.

CBSA Exam Crash Course



Ethereum Tokens

Usage Tokens

- These are tokens in specific blockchain that are similar to their own native currency in their DAPPS.
- Example is Golem

Work Tokens

- These are the tokens that identify you as a sort of shareholder in the DAPP.
- As a shareholder you generally have some voting rights.
- Dash is a good example

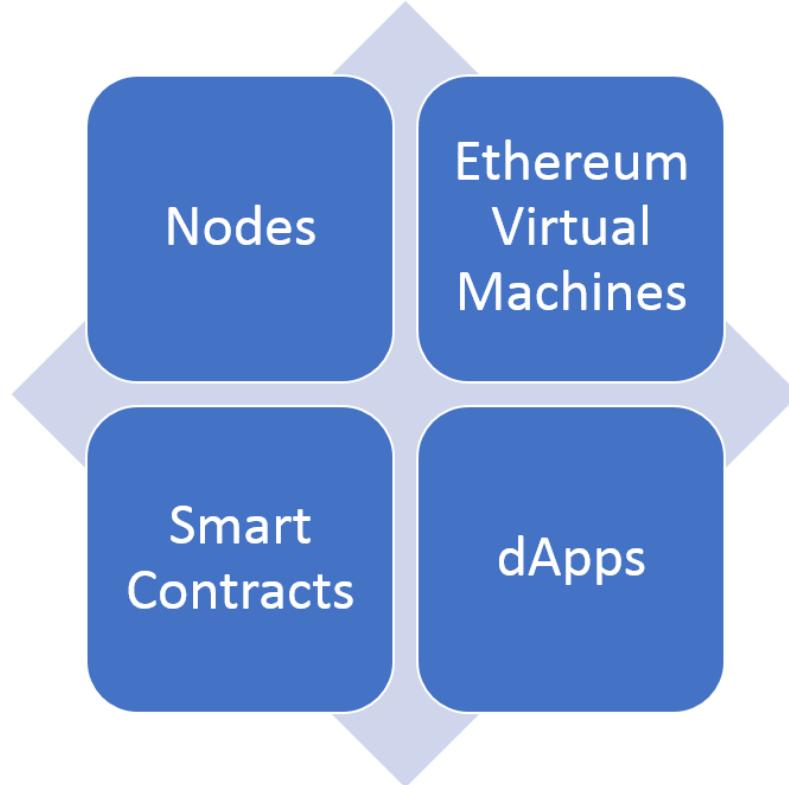
Ethereum Tokens

- **ERC20** defines a common list of protocols that an Ethereum token has to implement.
- Allows developers the ability to program behavior of new tokens within the Ethereum ecosystem.
- Common with crowdfunding companies via Initial Coin Offerings (ICO).



CBSA Exam Crash Course

Ethereum has four main components:



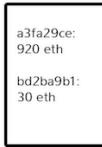
CBSA Exam Crash Course

Ethereum transaction workflow

Ethereum App



data



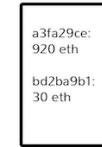
value



EVM



value



data



Distributed Network

Courtesy - Ethereum Stack Exchange

Practice Questions

Ethereum has four main components. Which one of the following is NOT a component?

- a. Gas
- b. EVM
- c. Dapps
- d. Nodes

Practice Questions

Ethereum has a native token that is utilized to pay for transaction fees, miner rewards, and other services on the network. What is it called?

- a. Ether
- b. EVM
- c. Ethereum
- d. Gas

CBSA Exam Crash Course

Ethereum EVM

CBSA Exam Crash Course

- **Ethereum Virtual Machine (EVM)** is built into the software running on the Ethereum protocol. It executes smart contracts - Ethereum programs written in the Solidity language.
- The EVM is contained in the full nodes of the Ethereum network, inside of which it executes these Ethereum-user-written programs.

CBSA Exam Crash Course

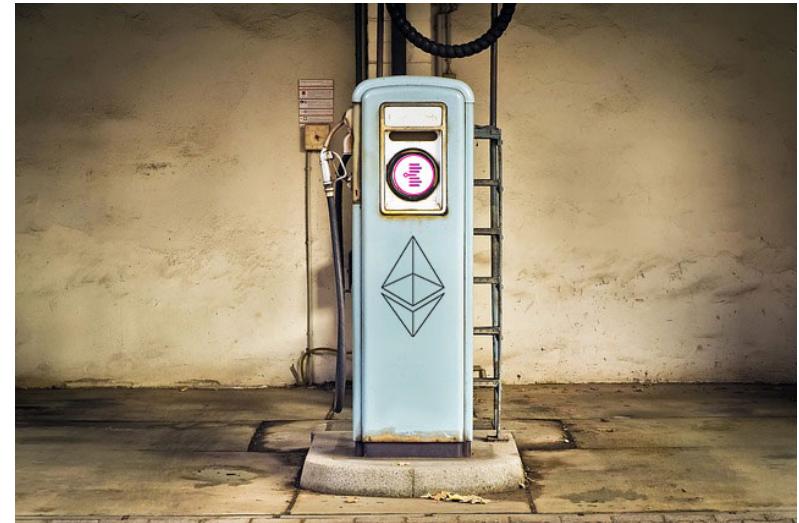
- **EVM code** is the programming language in which accounts on the Ethereum blockchain can contain code.
- The EVM code associated with an account is executed every time a message is sent to that account, and has the ability to read/write to the storage and then send messages.

CBSA Exam Crash Course

- Contracts can call other contracts or send Ether to non-contract accounts by the means of message calls.
- Message calls are similar to transactions, in that they have a source, a target, data payload, Ether, gas and return data.
- Every transaction consists of a top-level message call which in turn can create further message calls.

CBSA Exam Crash Course

- **Gas** is a measurement roughly equivalent to computational steps for Ethereum.
- Every operation has a gas expenditure on an EVM.
- Gas was implemented to help alleviate issues with Ether price fluctuations.



CBSA Exam Crash Course

- The Ethereum blockchain is a transaction-based state machine.
- In computer science, a *state machine* refers to something that will read a series of inputs and, based on those inputs, will transition to a new state.
- Genesis State is the beginning state and then to the final state.

CBSA Exam Crash Course

- The EVM is a Ethereum Virtual Machine is a computer software which runs at an abstraction layer straight above the underlying hardware.
- Ethereum uses a Semi Turing Complete Virtual Machine for running and compiling the codes.
- The term “Turing Complete” states that this software is agile enough to run any code defined by the developer or user.

CBSA Exam Crash Course

- The only limitation the EVM has that a typical Turing complete machine does not is that the EVM is intrinsically bound by gas.
- Power of the EVM is limited by the amount of “Gas”
- Stack based VM last-in -first-out stack to hold temporary values.
- The implementation can be in Python, Ruby, C++, and other languages.
- Fully Isolated from network.

Practice Questions

Ethereum Smart contracts are written in what development language?

- a. Solidity
- b. Python
- c. PHP
- d. Cobal

Practice Questions

A limitation of the EVM not associated with other types of virtual state machines is that the EVM is intrinsically bound by which variable parameter ?

- a. Gas
- b. CPU
- c. Code Base
- d. Location

Practice Questions

Ethereum is a programmable blockchain. What is one of the following reasons is NOT correct regarding Ethereum programmability ? Select One

- a. Does not allow users to create their own operations of any complexity
- b. It serves as a platform for many different types of decentralized blockchain applications
- c. Ethereum also includes a peer-to-peer network protocol
- d. Uses a semi Turing complete EVM

CBSA Exam Crash Course

Ethereum Browsers

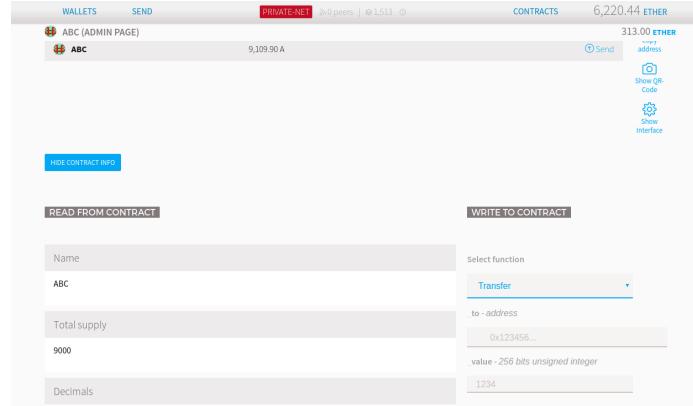
CBSA Exam Crash Course

- **Mist** is the browser for decentralized web apps (Web 3.0)
- IE or Google Chrome are for Web 2.0
- Mist is still in heavy development and may not support untrusted dApps

CBSA Exam Crash Course

- Mist is a full node, so you download the blockchain.
- Mist integrates with Swarm.
- Mist is a flexible desktop hybrid electron application with a web interface.

<https://github.com/ethereum/mist>



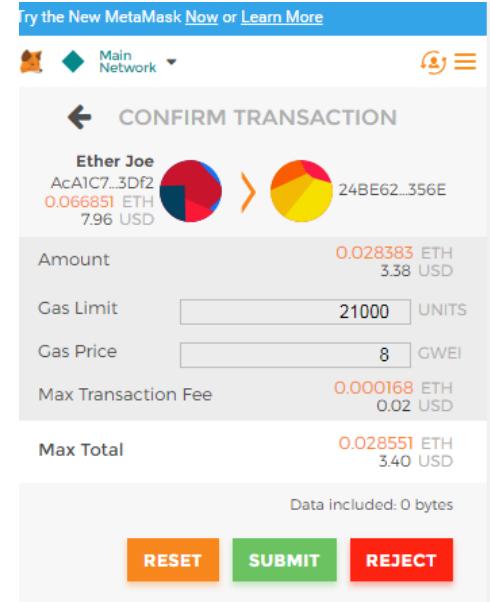
CBSA Exam Crash Course

- MetaMask is a bridge that allows you to visit the distributed web of tomorrow in your browser today.
- It allows you to run Ethereum dApps right in your browser without running a full Ethereum node.
- MetaMask includes a secure identity vault, providing a user interface to manage your identities on different sites and sign blockchain transaction.

CBSA Exam Crash Course

- Metamask is the best ERC20 compatible wallet , it provides you extra layer of security from phishing sites.
- Download via Browser extension in Chrome.

<https://metamask.io/>



CBSA Exam Crash Course

- Parity is another lightweight browser-based wallet that gives users access to decentralized applications and currencies on Ethereum.
- Parity comes with an extensive, in-built Ethereum Wallet and dApp environment.
- Web3 dApp Browser

<https://www.parity.io/>

CBSA Exam Crash Course

Ethereum Development

CBSA Exam Crash Course

Tools with Ethereum

- Languages – Solidity, Serpent, Mutan
- IDE – Solidity Browser, Ethereum Studio
- Clients – geth, eth, parity, Etherum Wallet
- Storage – IPFS, Swarm and Storj
- Dapp Browsers – Metamask or Mist
- Testing – Testnet, TestRPC

CBSA Exam Crash Course

Frontend Tools used with Ethereum:

- HTML
- CSS
- JavaScript

Backend Tools used with Ethereum:

- Solidity
- Serpent

Download Solidity or compile with your browser.

CBSA Exam Crash Course

- Solidity, the language behind Ethereum, is specifically designed to utilize the Ethereum Virtual Machine or EVM.
- Ethereum-based applications and Smart Contracts are written in Solidity.
- Solidity was proposed in August 2014 by Dr. Gavin Wood for Ethereum
- It has similarities to JavaScript and C.

CBSA Exam Crash Course

Solidity uses a whole new framework but it is very similar to the popular JavaScript.

Solidity vs JavaScript

- Solidity is kind of an Object Oriented language just like C++ and C# whereas JavaScript is based on HTML.
- Solidity is designed specifically for Ethereum applications and it runs only on the Ethereum blockchain.
- JavaScript is a universal language for the web and is being used in a large number of applications.

CBSA Exam Crash Course

APIs

- JSON is a lightweight data-interchange format. It can represent numbers, strings, ordered sequences of values, and collections of name/value pairs.
- To talk to an Ethereum node from inside a JavaScript application, use the web3.js library, which gives an convenient interface for the RPC methods.

Practice Questions

When discussing Ethereum with your customers, what would be the best statement to use when comparing to cryptocurrencies?

- a. Ethereum is the platform and Ether is its cryptocurrency.
- b. Ether is a platform and Ethereum is the cryptocurrency for Ether.
- c. Ethereum is a platform and Ether is the test platform. Bitcoin is used as the cryptocurrency for Ethereum.
- d. None of the above.

Practice Questions

Which of the following would NOT be true about what a smart contract gives your organization?

- a. Autonomy
- b. Trust
- c. Legal assurance
- d. Savings

Practice Questions

Ethereum has four main components. Which of the following components executes smart contracts?

- a. EVM
- b. Node
- c. Smart Contract code
- d. dApps

Practice Questions

In the Ethereum EVM there are two types of memory areas. Select Two

- a. Database
- b. Persistent
- c. Memory
- d. Storage

Practice Questions

Regarding Ethereum contracts..... The contracts can call (perform) two specific message calls. The message calls are either _____ or _____? Select Two

- a. BTC Nodes
- b. dapps
- c. Other Contracts
- d. Send Ether to Non Contracts Accounts

CBSA Exam Crash Course

Resources on Pearson

CBSA Exam Crash Course

Taking the Exam

Taking the CBSA Exam

- The Certified Blockchain Solution Architect (CBSA) exam is a professionally delivered exam which is proctored thru Pearson.
- Passing this certification will distinguish you as one that is knowledgeable from a pre sales perspective



Taking the CBSA Exam

Taking the Certified Blockchain
Solution Architect (CBSA) exam
Register for the exam

- Exam cost is \$300.00
- This exam is a 70 question
multiple-choice exam that lasts
1.5 hours (90 minutes)
- Performance Based



Passing the CBSA Exam

- To pass you need to score 70%
- Results will be immediately displayed.
- If you fail please review the exam retake policy for confirming when you can retake.



Obtaining and Maintaining your CBSA

- Upon passing you will receive in 2-4 weeks your training package, including certification token.
- Your certification expires two years to the date you take and pass the exam and will need to be renewed by retaking updated exam



CBDH Course on Pearson

https://learning.oreilly.com/videos/certified-blockchain-developer-hyperledger/9780135435458

The screenshot shows a Pearson learning platform interface. On the left, a sidebar menu includes: Browse, Recommended, Playlists, History, Topics, Learning Paths, Newsletters, Highlights, Settings, Support, and Sign Out. The main content area displays a video course titled "Certified Blockchain Developer--Hyperledger Fabric (CBDH)" by Joseph Holbrook. The course cover art features a play button icon and the text "Complete Video Course", "Certified Blockchain Developer", "Hyperledger Fabric (CBDH)", "Joseph Holbrook", and "SNEAK PEEK". Below the cover are sections for "Estimated time to complete: 5h 43m", "Topics: Windows", and "Published by: Pearson IT Certification 2019". A large red "Start" button is prominent. To the right, a "Contents" sidebar lists the course structure:

- Certified Blockchain Developer--Hyperledger Fabric (CBDH)**
 - Introduction**
 - Certified Blockchain Developer--Hyperledger Fabric: Introduction (1m 52s)
 - Module 1: Introduction to Blockchain**
 - Module introduction (33s)
 - Lesson 1: Certified Blockchain Developer Hyperledger**
 - Learning objectives (30s)
 - 1.1 What Is a CBDH (1m 27s)
 - 1.2 Audience for the Certification (2m 10s)
 - 1.3 Skillsets Required for Success (4m 3s)
 - 1.4 Objectives of the Exam (5m 57s)
 - 1.5 Certification Value (3m 2s)
 - Lesson 2: How a Blockchain Works**
 - Learning objectives (27s)

CBSA Course on Pearson

The screenshot shows a web browser displaying a course page for 'Certified Blockchain Solution Architect (CBSA)' on the Pearson O'Reilly platform. The left sidebar contains navigation links for 'Browse', 'Recommended', 'Playlists', 'History', 'Topics', 'Tutorials', 'Newsletters', 'Highlights', 'Settings', 'Support', and 'Sign Out'. The main content area features a large thumbnail for the 'Certified Blockchain Solution Architect (CBSA) livelessons video' by Joseph Holbrook. The thumbnail includes the 'livelessons' logo, the course title, author name, and a 'video' label. To the right of the thumbnail, details about the course are listed: 'Estimated time to complete: 5h 12m', 'Topics: Blockchain', and 'Published by: Pearson IT Certification 2018'. A red 'Continue' button is at the bottom of the thumbnail. Below the thumbnail, a section titled '5+ Hours of Video Instruction' describes the course as preparing viewers for the CBSA exam and its applications. A welcome message from the author is also present. On the right side of the page, a 'Contents' sidebar lists the course structure, including 'Introduction' (100% complete), 'Module 1: The Certified Blockchain Solutions Architect Exam Overview', and 'Lesson 1: Certified Blockchain Solutions Architect' (58% complete). Each lesson item includes a thumbnail, title, and duration.

O'REILLY®

Find a solution

Filter by: All

Search

VIDEO

Certified Blockchain Solution Architect (CBSA)

by Joseph Holbrook

Estimated time to complete:
5h 12m

Topics:
Blockchain

Published by:
Pearson IT Certification 2018

Joseph Holbrook

video

Continue

5+ Hours of Video Instruction

More than 5 hours of video instruction preparing viewers to take the Certified Blockchain Solutions Architect (CBSA) Exam, or desire the knowledge in using Blockchain, Ethereum, and Hyperledger for application in their day-to-day work.

Welcome to the *Certified Blockchain Solutions Architect (CBSA) LiveLessons* Course. This course is ideal for technology-focused engineers, application developers, IT administrators, or anyone wanting to obtain the Blockchain Training Alliance Certified Blockchain

Contents

Certified Blockchain Solution Architect (CBSA)

by Joseph Holbrook

Introduction

100% of section complete

Certified Blockchain Solution Architect (CBSA): Introduction

1m 49s

Module 1: The Certified Blockchain Solutions Architect Exam Overview

Lesson 1: Certified Blockchain Solutions Architect

58% of section complete

Learning objectives

21s

1.1 What is a Certified Blockchain Solutions Architect

56s

1.2 Audience for the Certification

1m 27s

1.3 Skill Set Required for Success

1m 9s

1.4 Objectives covered in the exam

1m 31s of 4m 11s

1.5 Certification Value

1m 15s

Hyperledger Course on Pearson

https://learning.oreilly.com/live-training/courses/understanding-hyperledger-fabric-blockchain/0636920199007/

LIVE ONLINE TRAINING

Understanding Hyperledger Fabric Blockchain

Get to know Hyperledger



JOE HOLBROOK



September 18 & 19, 2018
10:00am – 2:00pm EST

This course has ended.

[What you'll learn](#) [Instructor](#) [Schedule](#)

This training is focused on preparing IT professionals in Hyperledger Fabric 1.1 foundations and providing use cases with demos. It will introduce you to the need for Blockchain applications, use cases, and about Hyperledger Fabric, which is the open source framework for developing Blockchain applications and solutions with a modular architecture.

What you'll learn-and how you can apply it

Next Course March 28 and 29th

CBSA Exam Crash Course

Thank you

Course Closeout



Thank you

