Certified Blockchain Business Foundations (CBBF) Official Exam Study Guide v1.1
By: Kris Bennett and Chad Decker

Book is published by Blockchain Training Alliance, Inc.

Limit of Liability / Disclaimer of Warranty / Terms of Use
While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. There are no warranties which extend beyond the descriptions contained in this paragraph. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not apply or be suitable for your situation. You should consult with a professional where appropriate. The accuracy and completeness of the information provided herein and the opinions stated herein are not guaranteed or warranted to produce any particular results, and the advice and strategies contained herein are not suitable for every individual. By providing information or links to other companies or websites, the publisher and the author do not guarantee, approve or endorse the information or products available at any linked websites or mentioned companies, or persons, nor does a link indicate any association with or endorsement by the publisher or author.

This publication is designed to provide information with regard to the subject matter covered. It is offered or sold with the understanding that neither the publisher nor the author is engaged in rendering legal, accounting, investment, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought. This publication is no guarantee of passing this exam or other exam in the future. Neither the publisher or the author shall be liable for any loss or loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Contents

Chapter 1: What is Blockchain

Introduction

Welcome to the Blockchain Business Fundamentals course study guide. This guide is intended to help you identify key topics and subject areas related to the Blockchain Training Alliance's exam and certification for Blockchain Business Fundamentals. This guide is intended to present the reader with a variety of topics for self-study, with the intended outcome of helping the reader pass the exam and earn a CBBF certification.

What is Blockchain?

In order to properly understand blockchain, there are some key core concepts students should be familiar with. These key concepts include security, trustless-ness, decentralization, distributed ledgers, group consensus and immutability. In this section, and throughout this study guide, these topics will be presented and analyzed. In order to fully understand these key concepts and more, it's important to start with the basics.

At its most basic level, blockchain is an immutable record, or ledger.

The ledger is often used to track and manage asset ownership, however blockchain can be a simple record keeping device for any and all kinds of data – whether that data relates to asset ownership or not. Although blockchain is often described as a new and cutting-edge technology, the truth is blockchain is nothing more than a creative amalgamation of many old concepts, technologies, and methodologies. These components include ledgers, cryptography, group consensus, immutability and more.

At the core of blockchain is a ledger, a record keeping device which allows the keepers of a ledger to tell a story. This story usually revolves around the ownership and history of ownership of assets, although ledgers can be used to record just about any type of data imaginable. The earliest ledgers in human history appeared over 7,000 years ago and marked a key development milestone in human society, culture, and economics. Before this time ledgers were largely unnecessary; humans rarely owned more than they could carry around with them at any given time, and any trade, commerce, or exchange was largely limited to small tribal units and villages. Soon after humanity gave up a nomadic lifestyle to pursue an agrarian one the benefits became apparent.

It wasn't long before the average person had accumulated enough wealth that it was simply not practical or even feasible to be carried around all at once. At this point in history it became important to have a documented and permanent record of asset ownership. The introduction of ledgers into human society solved this problem and allowed people to trade across much larger groups; humans could now trade and

conduct commerce with others who shared vastly different languages, cultural values, and backgrounds. Small tribal units and villages gave way to large cities and empires – a new chapter of human history was being written.

Another core component of blockchain technologies is cryptography – the study of how to pass information back and forth in the presence of adversaries, bad actors, or simply audiences with no need to know. Although cryptography is often thought of as a cutting-edge discipline it is really quite ancient. As long as there have been two or more people on Earth who wished to keep a secret from someone else, there has been cryptography. In blockchain we use cryptography to protect anonymity, to provide ledger immutability, and to validate claims that people make against assets tracked and managed on the blockchain.

Finally, blockchain makes extensive use of existing computer networking technology, specifically peer-to-peer network architectures. The same technology that serves as the backbone of our modern internet also underlies blockchain. Adding a peer-to-peer (P2P) network architectures in the mix increases redundancy and fault tolerance by removing single points of failure commonly found in typical client / server network architectures.

If all of these concepts still seem a bit vague, don't worry. This guide will help introduce you to them in greater detail, and a wealth of information about each and every one of these topics can be found online for those wishing to get a deeper dive.

For right now, simply think of blockchain as the following simple process:

1. An announcement is made before multiple witnesses (nodes, miners, validators, etc).
2. Each participant documents the details of the announcement in their own personal copy of the ledger.
3. Announcements are grouped together in "blocks". Each participant regularly attempts to compare their current block with the current block of all the other participants on the network.
4. If there is a version of the current block which the majority of participants have in common, this version is considered to be the truth. Any participant that does not have the same data as the majority will simply discard their copy, obtain a copy from another participant, and move on.

Assets and Blockchain

Assets are a key component of any blockchain solution. Assets are simply the items that we're keeping records about, the items that 'matter' in the context of a given solution or use case. Assets can be defined as anything that requires a record of ownership. This can be monetary, non-monetary, or just information, like health records, tickets to an event, an auto title, or a patent.

Blockchain started as a record keeping system to record the transfer of digital "tokens" or "coins" such as Bitcoin and other cryptocurrencies. These coins and tokens required a way to keep a record of ownership. Out of the need to create a record of digital ownership, blockchain was born. In many ways blockchain seeks to supplement the internet of information we know today with the internet of value we're designing for the future.

Blockchains are important because they provide a safe and secure way for people to make any type of transaction without having to trust the other party. This concept in blockchain is known as "*trustlessness*" – as long as each participant in a transaction can trust in the accuracy and integrity of the ledger there is no additional requirement for trust between them.

Blockchains provide a digital immutable ledger that is widely distributed and peer-validated. It is critically important to note that a Blockchain does not require currency to function properly and most enterprise-level Blockchain applications require no special currency, coin, or token.

Blockchain can also be used as an event tracking system where announcements mark the occurrence of significant events and those events can be made actionable through the use of Smart Contracts/ Chaincode; software programmed to respond to certain types of these events.

By using Smart Contracts/Chaincode to handle meaningful events, Blockchain can also be a workflow/ BPM/BPA platform.

Blockchain History

The story of blockchain begins with a whitepaper published by an anonymous author a decade ago. Blockchain began as an idea documented by Satoshi Nakamoto. The ideas outlined in this whitepaper lead to the world's first and largest Blockchain – Bitcoin.

Bitcoin is a cryptocurrency that keeps its users highly anonymous through public key cryptography and cryptographic hashing. In public key cryptography users store their bitcoin in a digital wallet. This wallet contains the account's private key which is used to sign all transactions from that account. Any transactions presented by that account will be verified by the network using the corresponding public key for the account.

It is important to note that while common, anonymity is not a requirement of a blockchain platform. Many platforms, especially those aimed at business and enterprise use, replace anonymity with identity to allow solutions architects and administrators the ability to define and enforce permissions and role-based access. In many business scenarios, the anonymity and full-transparency that define public platforms are wholly undesirable but some sort of permanent append-only ledger is still required.

SIGNIFICANT BLOCKCHAIN DATES

- 2009 - First Bitcoin Block Created.
- 2010 - Satoshi Disappears in December – Date of last public post.
- 2015 - Ethereum and Hyperledger both go live.
- 2018 – Demand for blockchain increases, 14 Open Jobs for every blockchain developer.
- 2019 - Walmart requires produce suppliers to be using a blockchain solution.
- 2021 - Dubai hosts all government operations and record-keeping operations on blockchain as part of the Smart Dubai 2021 initiative.

Quiz: Chapter 1

1. Blockchain is primarily defined as a shared _____ ledger.
    a. Dynamic
    b. Immutable
    c. Single
    d. Updated

2. Which is NOT a technology used to create blockchain?
    a. Ledger
    b. Wifi
    c. Cryptography
    d. Computer networking technology

3. Blockchain as a ledger can best be described as a _____ entry ledger.
    a. Single
    b. Double
    c. Triple
    d. Dynamic

4. Nodes running on a blockchain must have _____ on ALL data stored.
    a. Consensus
    b. Hashes
    c. Ownership
    d. Certificates

5. Which is a type of data that can be stored on a blockchain?
    a. Medical records
    b. Ownership of a tangible asset
    c. Training certificates
    d. All of the above

6. _____ running on a blockchain allow actions to be taken on events/transactions.
    a. Nodes
    b. Smart contracts
    c. Networks sprinters

7. Data CANNOT be changed once it is committed to a blockchain.
    a. True
    b. False

8. The white paper that was released outlining Bitcoin was created by _____.
    a. Bill Gates
    b. Steve jobs
    c. Elon Musk
    d. Satoshi Nakamoto

9. What year was the first Bitcoin block created?
    a. 1998
    b. 2000
    c. 2005
    d. 2009

Answers: Chapter 1

1. B
2. B
3. C
4. A
5. D
6. B
7. A
8. D
9. D

Chapter 2: Cryptocurrency and Blockchain

Introduction

It is not uncommon to hear comparisons made between blockchain and the internet. Both are revolutionary technologies with the power to reshape the way we think, act, and view the world. Comparisons of the two platforms often invoke remembrances to the famous attage that "history does not repeat itself, but it often times rhymes". This due the many similarities that blockchain shows at this early stage to early stages of internet roll-out and adoption. Perhaps the biggest similarities between the two platforms exist in the first "killer app" to be built upon each.

When reflecting on the history of the internet, it's easy to see that the first truly consumer-grade application built on this new technological platform and deployed at scale was email. In other words, email was the introduction many early users had to the internet. Of course, as we all know, email is hardly the only use case for the internet and is far from the most interesting, dynamic, or impactful.

Similarly, the first consumer-grade application built on blockchain and deployed at scale has been cryptocurrency. For many early users, cryptocurrencies serve as the introduction and first hands-on experience with blockchain technology. However, just as the internet is far more than just email, blockchain is far more than just digital currencies.

Cryptocurrency and Blockchain

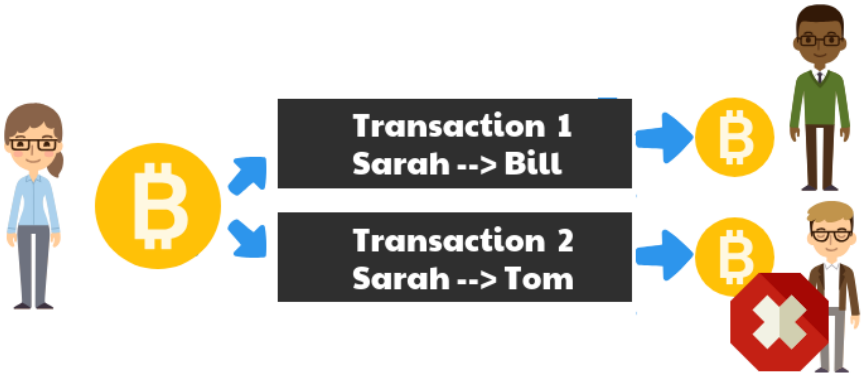
Bitcoin

If, up until this point in time, you were of the belief that Bitcoin was the world's first attempt at a digital currency which is disintermediated and trustless you would be mistaken - but you would hardly be the only one. The truth is, prior to Bitcoin many other attempts had been made to create a truly fungible digital currency. The reason we hear little about these prior attempts is that they all failed to solve one critical problem a currency must address - the double spend problem.

Double-spending

Double spending is a potential flaw in a digital cash scheme in which the same single digital token can be spent more than once. This is possible because a digital token consists of a digital file that can be duplicated or falsified. This problem was prominent when trying to create a decentralized currency but was solved by blockchain. Blockchain solved this by putting transactions in a block, verifying each transaction, then adding these blocks to the chain.

Double Spending Problem



Cryptocurrencies have some similar characteristics to fiat currency:

- Durable: Does this store of value persist well through time?
- Portable: Is this store of value easy to move around and transfer?
- Divisible: Is this store of value easy to divide into smaller sub-units for small payments & transactions?
- Fungible: Is each unit of this store of value equal in value to any other unit?
- Scarce: Is this store of value scarce enough to give it meaningful value?
- Accepted: How widely accepted is this store of value as a means of payment or settling a debt?

Blockchain is the underlying security and record keeping mechanism that manages and controls the Bitcoin network. It is simply a ledger that records the transfer of Bitcoin or other assets between people or entities. The records stay on the blockchain (they *are* the blockchain), what is transferred is the control or ownership of the underlying asset - Bitcoin.

Quiz: Chapter 2

1. Which of the following is NOT a quality of Bitcoin?
    a. It is digital
    b. It is decentralized
    c. It has no intermediaries
    d. It makes identity known

2. Bitcoin is a/an _____ that runs on blockchain.
    a. Application
    b. Fiat currency
    c. Chain code
    d. Database
    e. Scam

3. Blockchain is the underlying _____ software that manages and controls the bitcoin network.
    a. Security
    b. Database
    c. Derivative
    d. Dynamic

4. The blockchain is a ledger - it records the _____ of assets between people or entities.
    a. Value
    b. Transfer
    c. Number
    d. Dissolution

5. Control is enabled through _____.
    a. Cryptography
    b. Ownership
    c. TCP/IP
    d. Scientific constraints

Answers: Chapter 2

1. D
2. A
3. A
4. B
5. A

Chapter 3: Why Use Blockchain?

Introduction

A key concept in blockchain is the concept of decentralization. In order to properly understand decentralization, it is helpful to understand both centralized and distributed approaches. As we review each approach, it is critical to keep in mind that each new approach is NOT a replacement for the approaches that preceded it - they should be thought of as additional tools in the solutions design toolbox. In other words, just because you bought a screwdriver does not mean you go home and toss out all your wrenches; each approach offers value in uniquely different ways and it is not uncommon to use multiple approaches in the context of one solution.

The oldest and most well-known approach to systems architecture is a centralized approach. In a centralized solution there is typically a single owner or small group of owners of the solution, the data which the solution works with, and the infrastructure that delivers the solution. In other words, all layers and components of the solution are owned and managed by a central authority.

The next approach is a distributed or cloud approach. In a distributed solution, centralized control, ownership of the solution and the data which makes up the solution are retained. However, ownership of the infrastructure which delivers the solution is given up. Facebook is a great example of a distributed solution - Facebook owns the application as well as the data which goes into the application, but Facebook has largely given up ownership and management of the infrastructure that delivers the solution to hosting providers such as Microsoft, Amazon, or IBM.

A decentralized approach removes centralized ownership and control at all levels. In a truly decentralized solution the solution and its data are shared amongst all participants and the infrastructure can be shared by the solution owners or provided by the community at large.

Benefits of a Blockchain

As with any new tool, you will find there are good and bad use cases for blockchain. Blockchain provides many benefits, but it does have drawbacks as well. Understanding both is critical to applying the right technology to the problem set you're addressing. Before detailing the specific benefits and drawbacks, it's critical to understand that the benefits provided by blockchain always come at the expense of efficiency, speed, and performance.

Blockchain is, by design, an exceptionally inefficient solution. However, by embracing these inefficiencies we gain the benefits of security, redundancy, and massive fault tolerance. Embracing such an inefficient approach can seem very odd to those who have spent a career in traditional I.T. and have been conditioned to purge inefficiency whenever possible.

The benefits of blockchain solution include:

- Shared Infrastructure between Organizations in a Business Network
    - Your internal line of business (LOB) systems are the single source of truth for any question about your organization, but what is the single source of truth for processes that span multiple organizations in your business network?
- Publicly Verifiable
    - Accountability to customers and end-users (permission-less)
- Secure
    - Control who sees what data when (permissioned)
- Quality Assurance
    - Track origins of all supply chain components
        - Example: Food origin and/or safety recalls
    - Smart Contract as a replacement for middlemen operators
- Lower Transaction Costs
    - Removing middlemen reduces cost
- Tokenization
    - Create trade-able tokens backed by real-world value
    - Fractional Asset Ownership and Asset Digitization
        - Example- Own 1 car in 1 city, or own 100 cars in 100 cities
- Redundant and Highly Fault Tolerant
    - A distributed ledger is fault tolerant in that if a single node were to lose track of the ledger it would remain somewhere else on the network. To better understand fault tolerance, we can think of a group message. Everyone in the group message has a copy of the conversation, if someone wanted to delete something in the group chat, they would need to delete it on everyone's phone. Fault tolerance is especially useful when there are many people participating.
- Bring Clarity and Transparency to Business Processes
- No Centralized Authority
- Low Barrier to Entry
- Instant, Global Transactional Capabilities
- No Double Spending

Drawbacks of Blockchain

Blockchain is no different from any other technology - the benefits it provides come at a cost. There are some drawbacks to blockchain that must be properly considered in order to determine if blockchain is a good choice in an overall solutions architecture. These drawbacks are outlined below.

Here are some of the drawbacks blockchain faces:

- Extremely inefficient
- Very new technology
    - Constantly changing and evolving
    - Not very many trained resources
    - High Cost for trained resources
- Best practices, recommended patterns still being formed
- Scalability, transaction speed / cost, especially on public platforms

- No centralized ownership, no single authority
- Can be difficult (even impossible) to get a complete “God Mode” view of the solution and its data
- Many platforms and toolsets are still pre-production releases, and may not be ready to heavy applications development

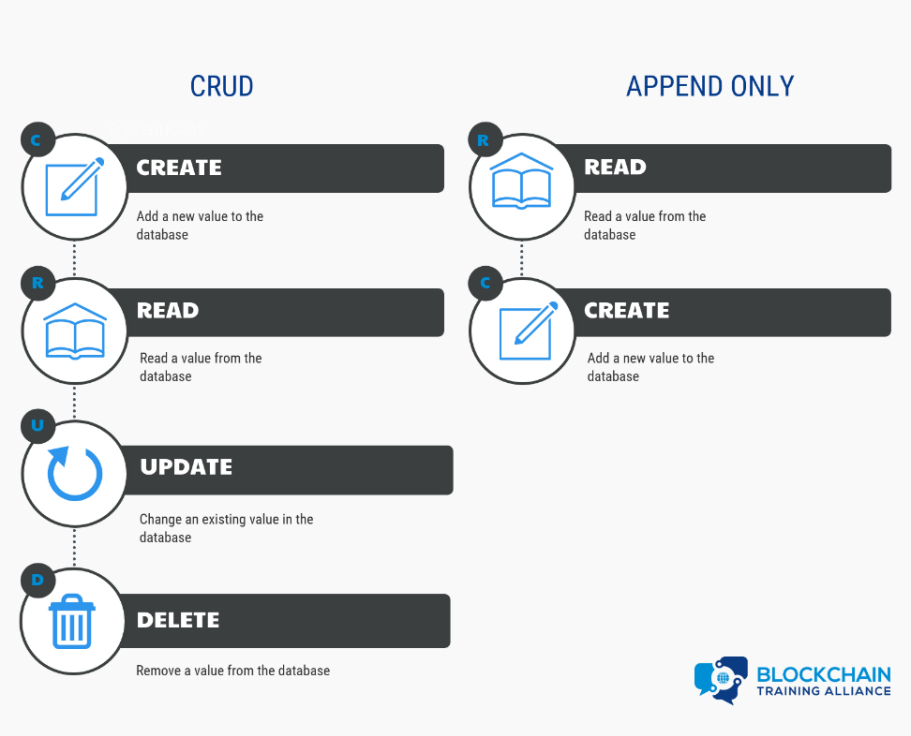
The Nature of an Append-Only Ledger

When listening to descriptions of blockchain it is not uncommon to hear that blockchain constitutes a "globally shared database". This is not a bad analogy, as long as one bears in mind several key differences. Databases have four primary operations or functions, commonly referred to as the CRUD functions. In a classical database, those functions are:

- **CREATE**
  - New records can be created and added to the database.
- **READ**
  - Existing records can be read from the database.
- **UPDATE**
  - Existing records can be updated in-place.
- **DELETE**
  - Existing records can be removed or purged from the database.

In blockchain, the last two of these functions have been intentionally removed. The only possible operations on a blockchain are:

- **CREATE**
  - New records can be created and added to the ledger.
- **READ**
  - Existing records can be read from the ledger.



Blockchain (by design) provides absolutely no ability to update or delete data on the ledger. This leads to the append-only and immutable properties of blockchain. If data is recorded on the blockchain, and that data later changes, that change must be recorded as an additional record on the ledger - no ability to update it in place exists. If data is no longer relevant, a new record must be added to the ledger indicating such - there is no ability to delete the record.

This append-only approach delivers the benefit of full version history of all data points within a blockchain solution. Databases, by contrast, excel at showing a 'snapshot' or current state of data.

Peer to Peer (p2p)

Centralized and Distributed system architecture solutions usually adopt a client / server network approach. Blockchain and decentralized applications platforms largely forego client / server to adopt a Peer-to-Peer (P2P) approach. In a P2P network, all nodes or computers are equal to all others. There are no servers, all nodes are clients and servers simultaneously. This allows for virtually unlimited fault-tolerance and built in failover abilities, as well as backups via data redundancy. All of this comes at the expense of performance and efficiency.

Quiz: Chapter 3

1. Which is NOT a quality of a decentralized solution architecture?
   a. There is no single owner
   b. There is no single authority
   c. There is no single truth
   d. There is no single administrator

2. Due to the invention of Distributed and Decentralized solutions there is no longer a need for centralized solutions.
   a. True
   b. False

3. One of the benefits of blockchain is that data can be _____.
   a. Always the same
   b. Always changing
   c. Editable
   d. Publicly verifiable

4. Blockchain is more secure than a traditional database because _____.
   a. There is no single point of failure
   b. The encryption code is more secure
   c. Miners are not trustworthy
   d. The data is always different

5. Blockchain is a great solution for tracking the origin of items and ensuring a certain level of quality exist.
   a. True
   b. False

6. Blockchain is a great solution because it still utilizes the functionality and need for intermediaries.
   a. True
   b. False

7. Which is NOT a drawback of implementing a blockchain solution?
   a. A lack of trained resources and talent
   b. Scalability
   c. It is a new and constantly changing technology
   d. Transaction speeds
   e. Cost
   f. None of the above

8. What function does a blockchain preform that a database does not?
    a. Fully distributed highly fault tolerant
    b. No centralized authority
    c. Low barrier to entry
    d. Global transaction capabilities
    e. No double spending
    f. All of the above

9. All nodes have and share the _____ copy of the ledger.
    a. Original
    b. Same exact
    c. Edited

Answers: Chapter 3

1. C
2. B
3. D
4. A
5. A
6. B
7. F
8. F
9. B

Chapter 4: Decentralized Networks and Ledgers

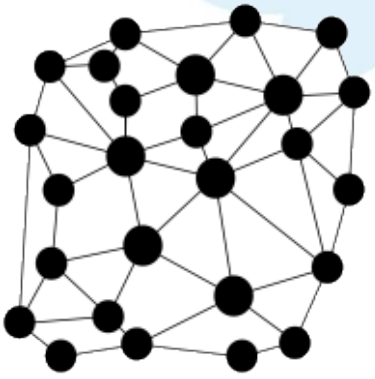
Introduction

In a blockchain the ledger is stored, updated, and maintained by a peer network. Each node in this network maintains its own individual copy of the ledger. It is the job of the network as a whole to come to a consensus on the contents of each update to the ledger. This ensures that each individual copy of the ledger is identical without requiring a centralized "official" copy of the ledger.

Why a Decentralized Network?

As mentioned, we assume right from the beginning that none of the participants will or have to trust one another. As long as they trust in the integrity and the accuracy of the blockchain itself they do not have to trust each other. The image below can be used to represent a blockchain network. Each dot on this picture is a node or a miner on the network, keeping a copy of the ledger.

Imagine if you were going to try to attack a network with this architecture, you could not perform a denial of service attack. The only true way to attack a network like this would be to take every single node offline. If you scale up this picture let's say 10x or 100x (adding nodes) you can see just how powerful and secure this network becomes.



Nodes can go online and offline as they choose, and the network continues to function seamlessly. When an offline node comes back online it can simply sync back up to the current state of the ledger with the other nodes online. This allows blockchain to not have a single point of failure or dependency that must be entrusted. This makes blockchain, and by extension, P2P architectures ideal for scenarios where network connectivity or uptime is not a guarantee – this is why there is so much interest and excitement around blockchain in parts of the world with developing infrastructure.

Quiz: Chapter 4

1. In blockchain, _____ has/have a copy of the ledger.
    a. Engineers
    b. Everyone
    c. Solution architects
    d. Developers

2. New transactions are broadcast and _____by the network.
    a. Recorded
    b. Scanned
    c. Changed
    d. Tagged

3. If everyone has a copy of the blockchain, when queried, everyone gets the _____.
    a. Secret code
    b. Future data
    c. Same answer
    d. Blind transaction data

4. With a decentralized ledger no one has to _____anyone else.
    a. Trust
    b. Blame
    c. Date
    d. Contract

5. One of the advantages of a distributed network is many nodes or peers that are connected in a network create no single point of failure or _____ control.
    a. Bilateral
    b. Centralized
    c. Dynamic
    d. Dual

Answers: Chapter 4

1. B
2. A
3. C
4. A
5. B

Chapter 5: Types of Blockchain

Introduction

Blockchain platforms are often described as being either public or private platforms. What do these terms mean, and how do you know which approach is the right approach for your solution or use case? In this section, each approach, as well as the respective benefits and drawbacks will be discussed.

Types of Blockchain

In order to properly describe a blockchain solution, additional terms must be entered into the conversation. A blockchain solution can be measured and described against the following three metrics:

- **Public vs. Private**
  - Who can write data to the blockchain? Public blockchains allow for large audiences or the public itself to add data to the ledger. Bitcoin is a great example of a public blockchain network – there are no rules or permissions around who can trade Bitcoin. Anyone can buy, sell, or send Bitcoin to anyone else. A blockchain solution used to track how charitable donations are used by a non-profit would be a great example of a private solution. In such a solution, only designated officers of the non-profit organization should be allowed to share metrics detailing how donations are allocated and spent.

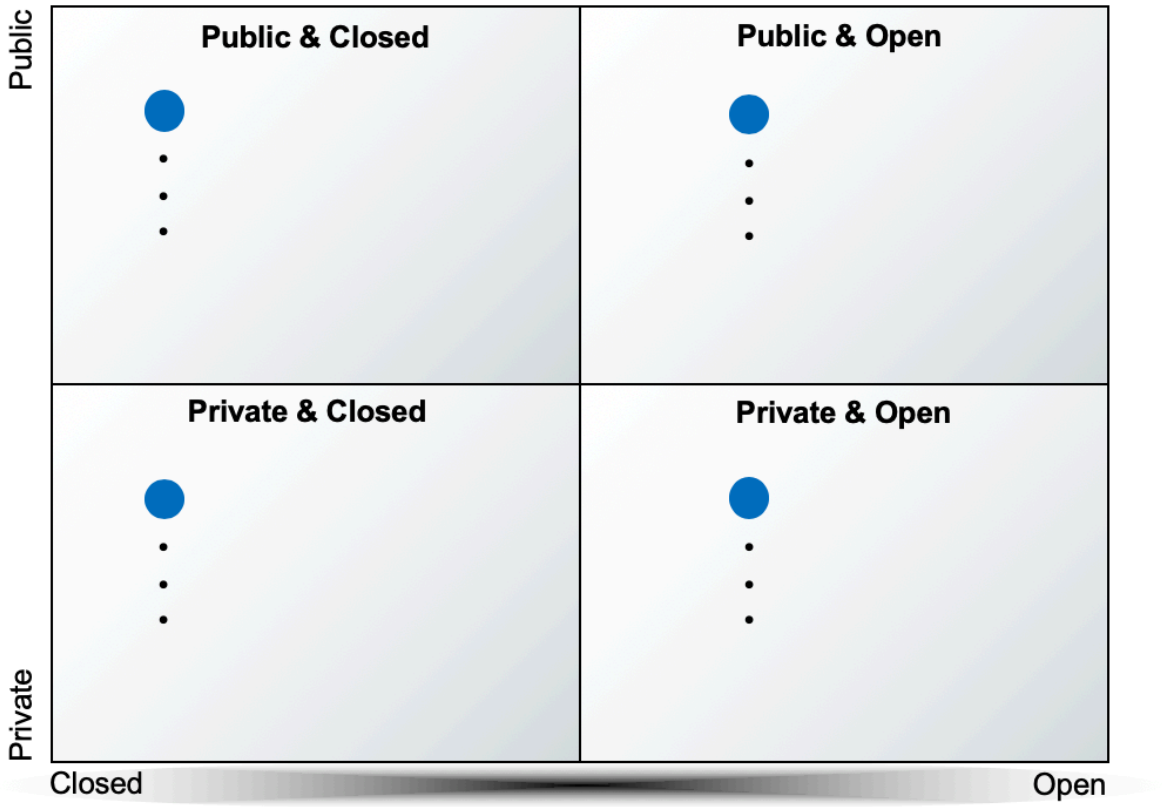
- **Open vs. Closed**
  - Who can read data from the blockchain? Open blockchains allow large audiences or the public itself to consume all the ledger data. Closed blockchains attempt to restrict read access. Once again, Bitcoin is a great example of an Open platform; anyone in the world can use a blockchain explorer to view the details of any Bitcoin transaction, whether they were a participant or not. An example of a closed blockchain solution might be a platform for managing elections. In such a solution it would be important that only election officials have access to election results and the individual votes cast by each voter – such information may not be well-suited for public consumption.

- **Permissoned vs. Permissionless**
  - Platforms or solutions which are open and public have little need for permissioning or role-based access. Such platforms are described as permissionless platforms because they do not have a native ability to track and manage identity, and subsequently define and enforce permissions based on that identity. This does NOT mean that you cannot build a permissioned solution on a permissionless platform, it simply means if you choose to do so you are responsible for designing and implementing a method to track and manage identity and draw permissions against that identity.

When designing a solution, a great way to determine what type of blockchain is needed is to determine if all participants are considered equal or should some have abilities or permissions that others do not? Answering this will help guide the solution to use a permissioned or permission-less blockchain technology.

It can sometimes be helpful to have a visual model when planning your blockchain solution. Feel free to use a quadrant such as the one below when mapping out a solution. For any envisioned use case, where does it fit on the model below? In other words, which combination best describes your desired solution?

- Public / Open
  - Anyone can write data, anyone can read data
- Public / Closed
  - Anyone can write data, only a few can read data
- Private / Open
  - Only a few can write data, many can read data
- Private / Closed
  - Only a few can write data, only a few can read data



Quiz: Chapter 5

1. Each block contains the hash of _____.
   a. The next block
   b. The previous block
   c. Of each block
   d. Of each fork

2. Only _____ of data can be made on or to the blockchain.
   a. Changes
   b. Deletions
   c. Additions

3. The blockchain provides a snapshot of the current state.
   a. True
   b. False

4. When looking at public vs private blockchains it is important to look at who can _____ data to the blockchain.
   a. Write
   b. Attach
   c. Edit
   d. Define

5. When looking at open vs closed blockchains it is important to look at who can _____ data from the blockchain.
   a. Read
   b. Write
   c. Define
   d. Download

6. When considering a permissioned vs permission-less blockchain it is important to ask: are all participants _____?
   a. Equal
   b. Trusted
   c. Liked
   d. Truthful

7. Any blockchain solution must be either public or private.
   a. True
   b. False

Answers: Chapter 5

1. B
2. C
3. B
4. A
5. A
6. A
7. B

Chapter 6: How Blocks Are Created

Introduction

Capturing transactions on blocks, and the subsequent validation process, can seem overwhelming to those new to the technology. Fortunately understanding the process is not that hard. In this section we'll review the process by which transactions are recorded, added to blocks, and validated using group consensus. This process is the heart of blockchain and a cursory understanding of the major steps is an important step in anyone's blockchain education.

How Blocks are Created

What is a "block"?

Perhaps the simplest analogy for understanding blocks in a blockchain is to think about sheets of paper in a notebook. Imagine an audience sitting in front of a stage. Each member in the audience has been given an identical notebook and a pen. Anytime a transaction is to be recorded on the ledger, the participants will walk up on the stage and announce their transaction to the audience. The audience will then record the transaction in their notebook, one transaction per line.

Eventually, an entire page in the notebook will be filled with transaction data. At this point, the audience will compare their current sheet of paper with the current sheet of paper held by all the other audience members. If the audience, collectively, finds a version of the data that more than 50% agree on or share in common, this data is considered to be the truth. If the audience is able to find a version of the transaction data shared by the majority of the audience then two things happen:

- Any participant who does not have the same data as the majority will discard their block and obtain a new copy from those in the majority, thus putting them back in sync with the rest of the participants.
- Once everyone is synced up, each participant will begin the process again by recording announced transactions on a fresh sheet of paper.

If this process makes sense, congratulations! You now understand a core concept of blockchain technology!

Two items of note:

- A block in a blockchain is just like a sheet of paper in the sense that neither has to know or care what type of data is recorded on it. Paper works equally well to store financial data, graphic data, musical data, weather data, etc. Data points of vastly different types with no relation to one another can happily co-exist on a block or on a piece of paper. The block or sheet of paper is just a simple record keeping device.
- In this example we made the assumption that transactions are recorded until the sheet of paper is full, then that sheet is validated by the entire audience. In reality, blocks are mined on a schedule. Imagine the same scenario as above, but in this revision there's a timer that buzzes every XX seconds. When this buzzer goes off the audience compares their sheets of paper.

Group Consensus

A critical concept to be familiar with in blockchain is that of group consensus. This is a simple concept which states that there's no way to know, without any room for doubt, what the absolute truth is. Therefore, we assume the truth to be whatever the majority of participants agree on. A great example of this is a police detective working to solve a crime. Imagine that you are that detective. One day the police chief asks you to investigate a bank robbery. Since you were not present when the bank was robbed, you don't know the actual truth of what happened. However, as a detective it is your job to try to determine what transpired. So, you do what any good detective would do in such a situation - you find witnesses to the event and ask them what they observed.

Imagine the following - you query ten witnesses about the robbery. Eight out of those ten witnesses tell you one version of the event - that four robbers ran out of the bank, jumped into a red sedan and drove away from the bank heading north. Two of your ten witnesses tell a much different story - that two robbers ran out of the bank, got into a white pickup truck and drove away from the bank heading south.

Which version is the truth? As a good detective you're likely to believe the version of the story told by the majority of the participants. When you provide a suspect description you'll most likely describe four robbers in a red sedan heading north.

This same principal is used extensively in blockchain - the truth is always assumed to be whatever the majority of participants agree on.

How are Blocks “Chained” Together?

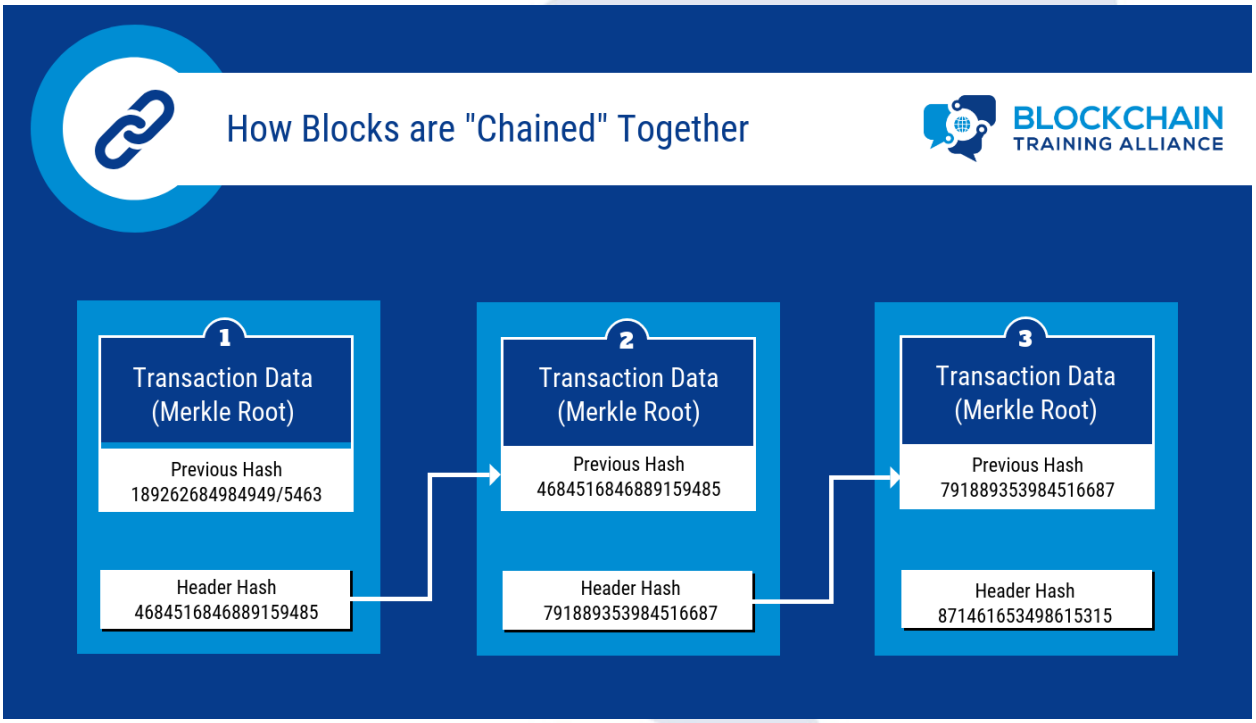
To link our sheets together we embed information from the previous sheet of paper into the new, recently validated sheet. In Blockchain, our sheet of paper is equal to a block. The act of embedding a previous block of information into the current block of information is called chaining. Hence, the name Blockchain.

To chain blocks together today, all data in a block is run through a special function called a "cryptographic hash". Cryptographic hashes create a unique output or identifier for a specific input.

Therefore, the hash of each block will always be unique based upon the inputs and attempting to change the data in a block will result in a hash or ID that no longer matches the original value recorded on the next block in the chain.

To link or chain blocks of data together the header of the current block contains the hash of the last (validated) block. Changing the data on any block in a Blockchain will result in a completely different hash and the new hash will not match the hash in the next block header thus breaking the Blockchain and invalidating all blocks linked to where the change was made. This gives Blockchain its property of immutability (can't be changed) and makes it highly censorship-resistant.

The height of a block simply refers to the number of blocks on the chain after the one in question. Block height is an indicator of the security of the data on the block; changing data in any block requires an attacker to change every subsequent block. The more of those blocks an attacker must alter, the more difficult it becomes to pull off an attack.



Quiz: Chapter 6

1. A block can be compared to _____.
    a. A cement block
    b. Wood block
    c. A piece of paper
    d. Car

2. The number of a block is the _____ of the block.
    a. Size
    b. Height
    c. Importance
    d. Weight

3. Blocks store _____.
    a. Name and financial information
    b. Numerical translations
    c. Digital data
    d. The future

4. The Block ID is the _____of the data on the block, and the _____ of that block.
    a. Hash, digital fingerprint
    b. Sum, total
    c. Representation, sign

5. The connection between blocks means that the Blockchain is much more _____ than a standard database.
    a. Dynamic
    b. Efficient
    c. Tamper-proof
    d. Private

Answers: Chapter 6

1. C
2. B
3. C
4. A
5. C

Chapter 7: Cryptography and Hashing

Introduction

Cryptography is used extensively in Blockchain to address concerns around privacy, ensure data integrity, and to help facilitate group consensus processes. Cryptography is the study of how to send information back and forth securely in the presence of adversaries.

There are a number of benefits to Blockchain solutions which include being publicly verifiable, secure, transparent, and cost-effective.

Blockchain also enables tokenization models that can enable organizations of all sizes to create truly digitized physical assets, provide fractional ownership solutions and create opportunities to decrease processing times while helping to remove unneeded intermediaries.

Some of the primary benefits of Blockchain are that it leverages a decentralized infrastructure, is a completely trustless environment, and provides immutability by cryptographically linking all blocks together. All blocks on the Blockchain are indexed using a Merkle Tree. A Merkle Tree is a lightweight digital fingerprint of all the transactions within a block which serves as an index to the blockchain.

Hashing

A hash function is a one-way function that takes any type of data as input and converts it to a unique 20-digit character code. For example, the letter ‘c’ could be given as the input, and through hashing, it would be converted to a 20-digit code. If the letter were to be changed to an ‘a’ the 20-digit code would be completely different. If the input were a 20 GB video file, the resulting hash would still be a 20-digit code that is completely unique. Hashing is especially useful in blockchain as blockchains need to constantly compare large amounts of data quickly with every other node on the network.

Merkle Trees

Blockchains use Merkle trees for fast and efficient validation of data. Merkle trees summarize the entire set of data in a block by creating a root hash of that data. The root hash is found by repeatedly hashing pairs of child nodes of data until only one node is left. The last remaining child node is known as the Merkle root.

Quiz: Chapter 7

1. Cryptography can be used to address the issue of _____.
    a. Privacy
    b. Efficiency
    c. Storage
    d. Global warming

2. _____ is a function for encoding or encrypting data to protect the contents from adversaries.
    a. A scientific function
    b. A quadratic function
    c. A cryptographic function
    d. A conjunction function

3. Public Key Cryptography provides _____ and transaction approval.
    a. Value
    b. Identity
    c. Decryption
    d. Democracy

4. _____verify the digital signature of a given key pair.
    a. Notaries
    b. Scanners
    c. Identification cards
    d. Public keys

5. _____sign/approve any transaction/action that might be made by the holder of the key pair.
    a. Public keys
    b. Private keys
    c. Notaries
    d. Presidents

6. Hashing is beneficial because it allows us to _____.
    a. Buy and sell things on the dark web
    b. Expand data into a digital format for reading purposes
    c. Instantly compare two or more large volumes of data to ensure they are the same

Answers: Chapter 7

1. A
2. C
3. B
4. D
5. B
6. C

Chapter 8: Mining a Block

Introduction

Blockchains are distributed when computers download the blockchain. These computers are known as nodes. When a block is filled up, it is validated through group consensus before it can be added to the chain of previously validated blocks. There are a number of Blockchain consensus mechanisms but regardless of the consensus type used, it is important to note that all transaction data on a chained block is assumed to be trustworthy and the chained data has not been tampered with due to the validation of data by group consensus.

Mining a Block

Consensus is a way to ensure the nodes on the network verify the transactions and agree with their order and existence on the ledger. In the case of applications like a cryptocurrency, this process is critical to prevent double spending or other invalid data being written to the underlying ledger, which is a database of all the transactions.

With consensus, there are different solutions that fit different situations. When deciding to use a specific consensus mechanism, you're taking on an opportunity cost (e.g. security, speed, etc.). The main difference between consensus mechanisms is the way in which they delegate and reward the verification of transactions. It's important to mention that most blockchain ecosystems have a hybrid of different consensus mechanisms. There is no need to choose one over the other.

When transactions are broadcast to the blockchain network it takes time for these transactions to be confirmed. It does this because transactions are verified by groups. When a transaction is initiated, it is sent to a pool with other unconfirmed transactions. Nodes group these transactions and then select blocks to be added to the chain. Each block is chained by including data from the previous block and the number of blocks in the chain is the block height. If two blocks were to be added to the chain at the same time the chain with the larger block height is selected to be the primary chain.

A blockchain gets more secure over time. If there are more blocks confirmed that means that there would be a smaller chance of a different chain to be selected as the primary one.

A fork is a change of protocol. There are two types of forks, a hard and soft fork. A hard fork is a fork where the data is not backward compatible. This results in a new blockchain being created. A soft fork occurs when data is backward compatible, resulting in a change that would not create a new blockchain.

Quiz: Chapter 8

1. Upgrades to the protocol can cause problems – but can be managed.
    a. True
    b. False

2. If the upgrade is backward compatible, it is a _____.
    a. Soft spoon
    b. Soft split
    c. Soft fork
    d. Hard fork

3. If the upgrade isn't backward compatible, it is a _____.
    a. Soft spoon
    b. Soft split
    c. Soft fork
    d. Hard fork

Answers: Chapter 8

1. A
2. C
3. D

Chapter 9: Types of Consensus

Proof of Work

Bitcoin implemented Byzantine Fault Tolerance through a validation system called Proof of Work. In Proof of Work consensus, when a block is validated each node competes to solve a guessing game problem to validate the block of data. This problem is non-computational and random guesses are most efficient. Nodes are called Miners and each miner attempts to guess a piece of data called the "nonce" to succeed in validating a block. All block data plus the current guess (nonce) are run through a cryptographic hash - if the resulting output matches the current level of "difficulty" (usually expressed as a fixed number of leading zeros) the miner has guessed the right answer.

This difficulty is adjusted by the network to correspond to load and to keep the average block mining time consistent with the schedule the platform defines (the buzzer from our example in chapter 6). A nonce is the random data that is combined with the block data which will produce a hash output matching the current difficulty level of the Blockchain. Any miner who thinks they have the correct answer will share it with all other miners. Miners will confirm the answer is correct by using the nonce with their block data to try to get a result that matches the difficulty setting. If 51% or more of the miners agree with the proposed nonce, the transactions on the winner's block are considered to be correct and the miner with the correct answer will be rewarded (reward is given in platform tokens). If the majority of miners do not agree with the nonce, no reward is given and the work performed is a sunk cost as validation did not occur.

Any nodes that do not have the correct block data will reconcile by copying the validated block from neighboring nodes. Proof of Work consensus creates a game theory incentive for each node to behave accurately and honestly; any dishonest participants will incur real-world costs in guessing the nonce for a zero percent chance of being rewarded with a payout.

Proof of Stake

Proof of Stake is a newer Blockchain consensus system that has been proposed as an alternative to Proof of Work consensus to overcome the scalability and cost concerns in PoW. Proof of Stake removes the guessing game from the validation of blocks so mining no longer requires powerful and specialized hardware. This vastly reduces the energy consumption of the network as well. Proof of Stake consensus uses a system where “validator” nodes each give or pay a stake in order to validate transactions. When it’s time for group consensus, all who wish to participate lock up funds in a stake.

A random node is selected and the hash of that node’s block data is shown to all other participants. All other nodes wager on the validity of the block transactions. If the majority agree with the proposed block, the random node is rewarded as are all who wagered on that node. If the majority disagree, the random node loses their stake, gets no reward, and a new node is randomly selected to share their block data. The game theory incentive toward honesty and accuracy is maintained, only the mechanics of how it's enforced are changed. The key difference with this consensus is that no computing is ever performed during consensus, only wagering and any kind of device can wager, regardless of computing power.

Other Consensus Mechanisms

Proof of Activity – is a hybrid of PoW and PoS. Empty template blocks are mined (PoW) then filled with transactions which are validated via PoS.

Proof of Burn – is where coins are "burned" by sending them to an address where they cannot be retrieved. The more coins burned, the better the chances of being selected to mine the next block.

Proof of Capacity – is where hard drive space is staked to participate. The most space 'staked', the better the odds of being selected to mine the next block. The consensus algorithm here generates large datasets called 'plots' which consume storage.

Proof of Elapsed Time – was created by Intel to run on their trusted execution environment. It is similar to PoW but far more energy efficient. The concern is this requires trust in Intel and can be viewed as a central authority.

Proof of Authority - uses a set of "authorities" which are nodes that are explicitly allowed to create new blocks and secure the Blockchain. This is a replacement for PoW but only for Private Blockchains. Nodes have to earn the right to become a validator/authority

Quiz: Chapter 9

1. With proof of work, when a block is full, each node competes to solve and guess the _____.
    a. Block number
    b. Block id
    c. Nonce
    d. Cryptographic Hash

2. With Proof of Work, when _____% of the miners confirm the nonce is correct, the transaction is added to the Blockchain.
    a. 25
    b. 50
    c. 51
    d. 100

3. With proof of stake no "computing" is ever preformed only _____.
    a. Contributing/collecting
    b. Staking wagering
    c. Blind betting/blind picking

4. Types of consensus include all EXCEPT _____.
    a. Proof of work
    b. Proof of stake
    c. Proof of burn
    d. Proof of space
    e. Proof of output

5. Proof of Stake is the most mature consensus mechanism.
    a. True
    b. False

6. The network is designed so that if some peers crash or attack the network maliciously, the network can still operate; this is known as _____.
    a. Byzantine fault tolerance
    b. Cyber defense
    c. Consensus
    d. Malware

Answers: Chapter 9

1. C
2. C
3. B
4. E
5. B
6. A

Chapter 10: Blockchain 2.0 and Ethereum

Introduction

When Bitcoin went live in 2009, blockchain was nothing more than a record keeping device, a place to permanently record data for future use. Bitcoin and other platforms which only offer the ability to store and retrieve data are often referred to as "blockchain 1.0" platforms.

In 2015 Ethereum introduced the concept of "blockchain 2.0" platforms by introducing the concept of Smart Contracts. The ability for developers to include custom logic and rules in their transactions now meant blockchain could do more than just data storage, it was now a fully-fledged application development platform. Business processes could be modeled and automated on the same platform that transaction data lived on.

Today, Ethereum is one of the most widely-used blockchain platforms. Smart Contracts, also known as chain code, are a way to program rules and decision points into transactions and processes on a blockchain. For those from a development background, a Smart Contract can be thought of a class in traditional programming terms. Smart Contracts are published to the blockchain directly and allow one to automate transactions and ensure they all follow the same rules. Each Smart Contract, along with the transactions it performs, exists as records or transactions on the blockchain. Therefore, Smart Contracts also live as permanent entities on the blockchain – this is an important point to keep in mind when evaluating a Smart Contract as a potential solution component.

Smart Contracts provide:

- Autonomy: Smart Contracts can be developed by anyone, no need for intermediaries such as lawyers, brokers, or auditors
- Backup: A Blockchain and Smart Contracts deployed to it provide a permanent record, allowing for auditing, insight, and traceability even if the creator is no longer in business
- Efficiency: Removing process intermediaries often results in significant process efficiency gains
- Accuracy: Replacing human intermediaries with executable code ensures the process will always be performed the same
- Cost Savings: Replacing intermediaries often provides significant cost reduction

Gas in Ethereum

Specific to the Ethereum Blockchain is the concept of gas. This concept was born out of a limitation the developers of Ethereum saw with Bitcoin, specifically its programming language called Bitcoin Script. One of the major limitations of Bitcoin Script is the inability to perform loops or iterations in the language.

This severely limits the types of functions developers can create in Bitcoin Script. This limitation was intentional – the developers of Bitcoin did not want to create a mechanism by which malicious or simply inexperienced developers could put the platform into an infinite loop. Ethereum developers introduced the concept of gas to allow for functionality lacking in Bitcoin Script in order to provide developers Turing complete Smart Contract development languages such as Solidity and Viper.

Gas is simply how users pay for the cost of a transaction to be processed or validated on the Ethereum Blockchain. Gas is a separate reward given to all miners independently of the consensus mining reward. Gas is used to compensate all nodes on the network for the cost incurred in recording a single transaction. Every transaction (write) on the Ethereum Blockchain must be submitted with gas, any unused gas is returned to the user.

Note that reading data from the Blockchain is not considered the transaction, and therefore does not incur a gas cost. The concept of gas not only pays for the cost of recording a transaction on their copy of the ledger, but it also prevents infinite loops and closes certain security vulnerabilities. An infinite loop would require infinite gas, and infinite funds with which to purchase that gas.

It is important to note that gas is only consumed when data is written to the Blockchain. Reading from the Blockchain consumes no gas.

A function (in a Smart Contract), which runs out of gas, will be terminated and no gas will be returned to the user. It is also important to note that the management of gas is handled at the protocol level – the protocol itself will remove Ether from a user's wallet, convert it to the requested amount of gas, and return any unspent gas to the wallet after converting it back into Ether. The user does not need to intervene or even be aware that this occurring. This also means developers only need to consider the gas costs of the transactions in their functions; they do not need to worry about managing the conversion of currency into gas and gas back into currency.

Finally, calculating the amount of gas needed to process a transaction is possible but a general rule of thumb is, the more write operations in a Smart Contract there are, the more gas required. Gas is decoupled from Ether so that real gas price costs remain constant while Ether prices can continue to be volatile. If NOT using an Ethereum Blockchain, it is important to determine how one will implement their own gas/fee/incentive system, or otherwise compensate nodes for the act of recording new individual transactions. Gas is also tied to the type of operation being performed – more complex operations will require more gas than simple ones. Online calculators, such as Eth Gas Station (available online at ethgasstation.info), are available to help developers and architects estimate gas costs based on the operations being performed.

Quiz: Chapter 10

1. Ethereum provides a decentralized _____ virtual machine, which can execute computer programs using a global network of nodes.
    a. Augmented
    b. Turing complete
    c. Scientific
    d. Dynamic

2. Smart Contracts are _____.
    a. Computer code
    b. Contracts written by people with the highest IQs
    c. Virtual contracts

3. Smart contracts perform all of the below except _____.
    a. Enforce rules
    b. Perform negotiated actions
    c. Make cognitive decisions

4. _____ is the unit in which Ethereum Virtual Machine (EVM) resource usage is measured.
    a. Inches
    b. Pounds
    c. Meters
    d. Gas

Answers: Chapter 10

1. B
2. A
3. C
4. D

Chapter 11: Blockchain Use Cases

Introduction

Newcomers to blockchain are often quick to ask, "*who is actually using blockchain technology and what value are they getting out of it?*" In this chapter, we take a look at several blockchain use cases and implementations.

Background Checks

Being able to verify and validate someone's transcripts, diplomas or education achievement claims. With a verification and immutable data on the blockchain, fraudulent achievements will be null and void. For instance, fake medical degrees is a real and urgent problem. A congressional committee over 25 years ago estimated there were about 5,000 fake doctors in the United States alone. That number is believed to have grown at a staggering pace since then due to the prevalence of the counterfeit degrees sold on the internet. People have and will continue to die at the hands of these counterfeit degrees. Blockchain presents a viable solution to this problem.

Personal Identification

Birth certificates, passports, identification cards and other forms of personal identification can become counterfeit lost and altered. Blockchain provides a potential solution for some of these problems.

Land Registries

It is estimated that at least one out of every three land titles contain an error. Title companies in the United States pay out billions of dollars in claims every year due to these errors. Blockchain could provide an immutable record of ownership and move the storage of ownership history from a paper record filed with a government building to a distributed and immutable ledger.

Financial Services – Securities Clearing

The banking, accounting, economic circles are enamored with the opportunity blockchain possess, for good reason. Its ability to provide bank-like services and also offer currencies that meet so many of the requirements of what a currency should do.

Global Supply Chain

Global Supply Chain is a huge area where many feel blockchain will see one of the most immediate impacts. In fact, in 2018, Walmart announced that they will be requiring all produce suppliers to be utilizing a blockchain solution by the Q3 2019. They have stated that they intend to issue the same requirement amongst all produce suppliers by 2020. Supply chain will also have a large impact on automotive, so much so that companies like Mercedes are spending hundreds of millions of dollars to just explore possible solutions. The automotive industry believes that there will be a large financial gain from the implementation of blockchain when it comes to recalls and even counterfeit items. It is estimated that nearly 30% of the air bags in the United States are Counterfeit. Being able to bring this number down significantly stands to save so many industries billions of dollars.

Healthcare

Healthcare is one of the first places people who learn about blockchain gravitate to immediately. The potential that blockchain has for impact in healthcare is astounding. It stands to not only save millions, curb counterfeiting, empower patients, but most of all save lives. This will affect EMRs, insurance claims, genome research and so much more.

Airlines

Airlines are looking at blockchain as a way to replace and/or enhance registration, rebooking, vouchers, and loyalty programs. Airlines are also looking at blockchain as the way to track the maintenance and upkeep of incredibly complex devices. The number of critical components inside a modern jet airliner and the amount of traceability and auditability that goes into any work, repair and adjustment of those complex machines is incredible and you can probably now begin to see why airline companies are making such an investment into blockchain.

Tokenized Economies

"Tokens" or digitalized assets have opened up a fascinating new world that has never before existed. A way to allow people to own, trade, buy, sell, track and maintain incredibly small ownership pieces of real-world assets. This tokenized fractional asset ownership is enabling many new business models.

Payment Channels

With complete and up to date micropayment and payment records, a business would foreseeably never have to stop and square up their books with any of their suppliers, venders, manufactures, lenders, etc. Instead all participants in a business network could know exactly where they stand at all times. This would give business leaders and decision makers greater clarity and insight into our business'. This could also simplify the maintenance upkeep and accounting process, allowing leaders to focus on activities with a high value add or return for time spent.

Quiz: Chapter 11

1. Which of the following industries is NOT implementing or exploring blockchain solutions?
    a. Healthcare
    b. Land registries
    c. Financial services
    d. Supply chain
    e. None of the above

2. It is estimated that nearly _____% of global airbags sold and installed are counterfeit.
    a. 10
    b. 30
    c. 75
    d. 90

3. Blockchain has the potential to affect nearly every industry in some way.
    a. True
    b. False

Answers: Chapter 11

1. E
2. B
3. A

Chapter 12: Blockchain Adoption

Blockchain is being considered by more than half of the world's fortune 500 companies according to a Juniper Market Research Survey. It is estimated that $2.3 billion were spent on blockchain by the end of 2018. What effect is this going to have? Blockchain is bringing us the internet of value.

Blockchain opens up entirely new business models, due to the fact blockchain is able to transcend physical and geographical barriers and uses math and cryptography to enable transactions globally. The uniqueness of blockchain lies in its ability to retain person to person transactions globally.

Blockchain today is often compared to the internet in the nineties. We are seeing the effects from blockchain that are similar to the effects the internet brought about in the nineties. We don't fully understand this technology and therefore cannot fully utilize its applications. Because we have the internet, we are seeing a much faster spread of blockchain, and blockchain is one step closer to web 3.0.

Quiz: Chapter 12

1. According to a Juniper market research survey in 2017, Blockchain (DLT) is being considered by more than _____% of the world's big corporations.
    a. 10
    b. 25
    c. 50
    d. 75

2. The internet brought us the age of information, and Blockchain is bringing us the internet of _____.
    a. Streaming
    b. Value
    c. Augmented reality
    d. Virtual reality

3. Blockchain transcends all physical and geographical barriers and uses _____ and _____ to enable transactions globally.
    a. Internet connections, Fiat currency
    b. Cell towers, Gps
    c. Math, Cryptography
    d. Cell phones, GPS

4. The uniqueness of blockchain lies in its capacity to store and retain _____ transactional history so that chances of fraud, hacking, and third-party interference are greatly reduced.
    a. Person to person
    b. Future
    c. Public or private
    d. Cash

5. Blockchain today has been likened to _____.
    a. Landing on the moon
    b. The internet
    c. The Atari
    d. Virtual reality

6. Blockchain is moving very fast, but we still have a lot to learn and new opportunities exist on many levels.
    a. True
    b. False

7. Blockchain investments are extending to the _____ countries and _____ areas of the world quickly, providing a way to do personal business, as well as commerce.
    a. Underdeveloped, underbanked
    b. Diverse divided
    c. Wealthiest, smartest

Answers: Chapter 12

1. C
2. B
3. C
4. A
5. B
6. A
7. A

Chapter 13: Web 3.0

In order to understand Web 3.0, it is important to first understand what web 1.0 and 2.0 were. Web 1.0 is the first integration of the internet. This took place in the nineties and was led by the visionary, Sir Tim Berners-Lee. Berners-Lee had a vision of decentralizing content. He wanted people to be able to access content without the need of a third party.

Web 2.0 is the current age of the internet and is considered the age of social media. Web 2.0 decentralized people. People now do not have to go through a third party to communicate with each other.

Web 3.0 is the Internet of Value

Web 3.0 plans to decentralize finance. We saw this first with Bitcoin, but it is continuing to evolve and will soon make all assets decentralized. There are things we need to accomplish before reaching the goal of web 3.0 and the primary problem needing attention is transaction speed. Many solutions are being worked on and one of these solutions is off-chain protocol. Off-chain works by having multiple transactions verified and added to a chain separate from the main before being added to the main chain.

One thing is for certain about web 3.0, it will not look anything like web 2.0 or web 1.0. All of the previous web components will still be critical pieces, but entirely new business models will open up with web 3.0. Individual consumers will be able to do things that were previously reserved for only the richest and most powerful organizations on earth. The effects this will have are going to be profound and transformative.

Quiz: Chapter 13

1. New Blockchain Networks are failing to evolve and improve upon the original creation of blockchain.
    a. True
    b. False

2. Web 1.0 is considered the Internet of _____.
    a. Static information
    b. The future
    c. Web surfing
    d. Gaming

3. Web 2.0 brought us _____.
    a. Virtual reality
    b. World news
    c. Social engagement
    d. The millennial generation

4. Web 3.0 brought us the internet of _____.
    a. Value
    b. Augmented reality
    c. Fake news
    d. Virtual reality

5. Digital Identity is an extremely exciting use case for most blockchain enthusiasts.
    a. True
    b. False

Answers: Chapter 13

1. B
2. A
3. C
4. A
5. A

Chapter 14: Blockchain Implementation

Introduction

Bitcoin used blockchain to store financial transactions, but the data can be anything from a vote in an election to an entire book. This is important when considering practical use cases for blockchain. As we know, blockchain is a distributed, immutable, highly secure database and many industries could take advantage of the transparency that blockchain provides. For example, blockchain technology could change how voting works. Blockchain would allow for voters to be 100% certain their vote is being counted. A good use case will do one of two things: It will either allow for new possibilities that have never been possible before or improve certain aspects of an existing process.

Blockchain is not always a better alternative to a database.

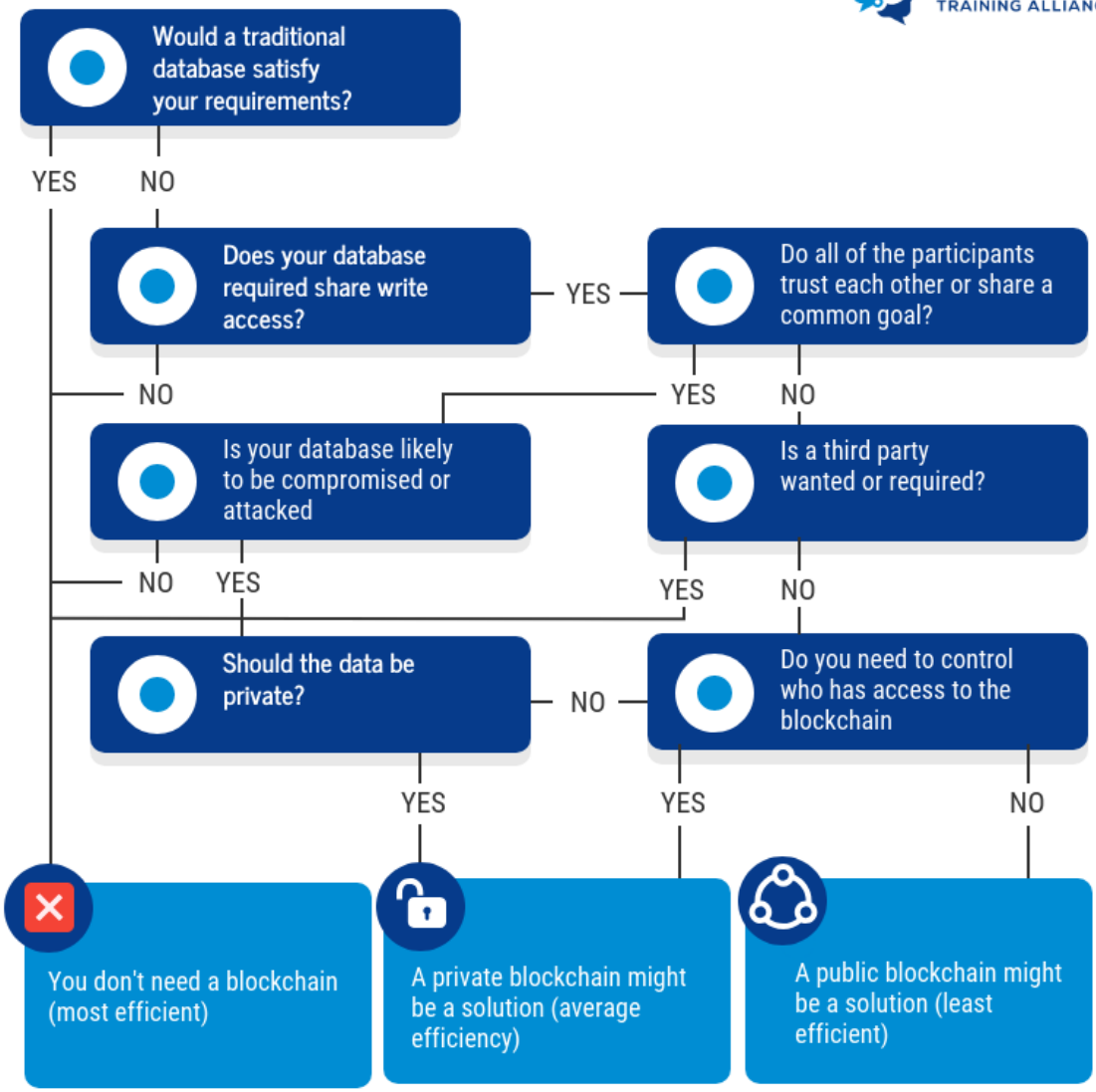
Blockchain has a few drawbacks that need to be considered when attempting to implement it. Starting with how new blockchain is, to the stigma of its use originating in the Dark Web. The creation of blockchain is also a mystery that tends to put people on edge. ICO/ITO scams and the misperception that blockchain is just another name for cryptocurrency are also drawbacks that aren't technical but do impact the adoption of blockchain itself.

More tangible challenges with blockchain today include the fact that blockchain technology is still changing and evolving, best practices and recommended patterns for implementation are still being formed. There are not very many trained resources and therefore, the cost of trained resources is high. Finally, scalability is a core concern when it comes to blockchain. Blockchain prioritizes security over speed. Therefore, solutions that require high transaction speeds are not good candidates for Blockchain. Different group consensus methods beyond Proof of Work are currently being proposed to overcome current scalability limitations. Today, most major public blockchain are able to process 10-20 transactions per second worldwide.

Data Sovereignty is another factor to consider when comparing blockchain solutions versus traditional ones. In a centralized system, all data is owned by the system owner. In scenarios where one must demonstrate they own and control the data as well as demonstrate where it is and is not stored, blockchain may not be a good solution (although private blockchains can still be a viable option here).

Transaction times are very high in blockchain, but solutions are being investigated. One such solution includes using off chain transactions to lower transaction times.

Blockchain Decision Chart



Quiz: Chapter 14

1. Blockchain is always the solution.
    A. True
    B. False

2. Which of the following use case implications is NOT a reason to explore a blockchain solution?
    A. Large Business network
    B. Can't be solved with a database
    C. Need multiple ledgers
    D. Intermediaries are wanted

3. What is an obvious way a blockchain solution can deliver a customer value?
    A. Less planning needed
    B. No board members needed
    C. Financial Incentives
    D. All of the Above

Answers: Chapter 14

1. B
2. D
3. C