Blockchain 101 Guide

for

Blockchains Demonstration

Project 9

Version 1.0 approved

Prepared by Vanessa Soares, David Mistretta, Daniel Champagne, and Ian Eichorn

University of Massachusetts Dartmouth

1 November 2017

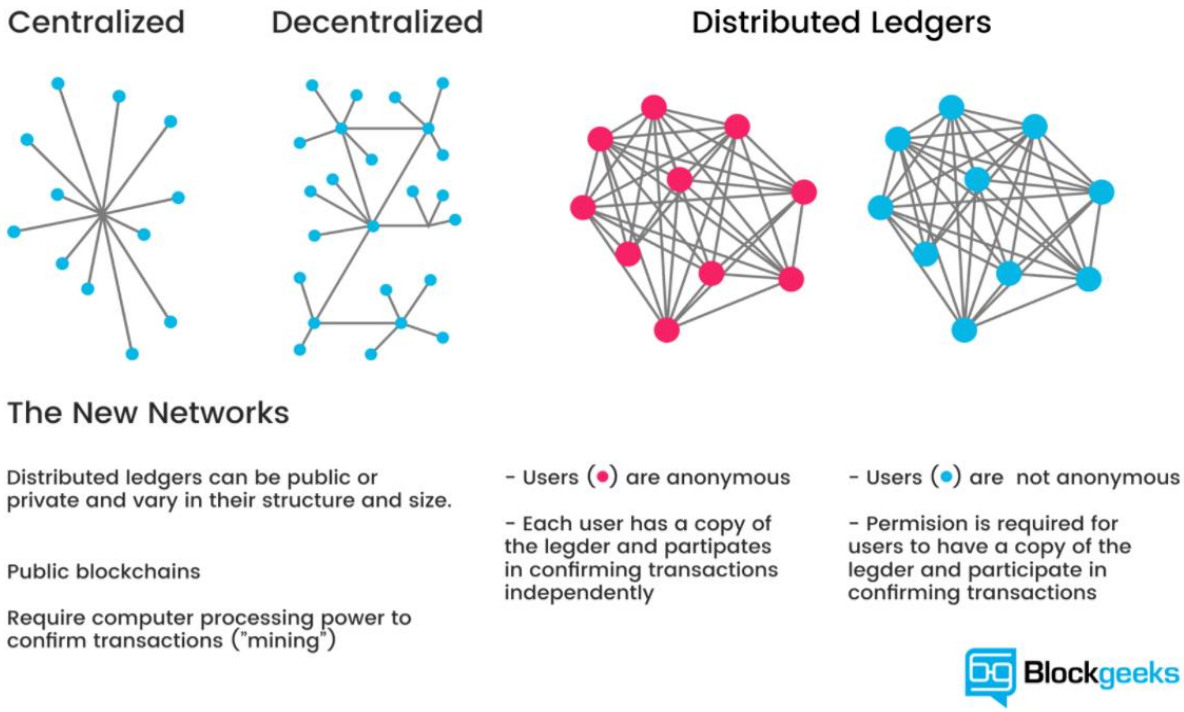
Table of Contents

Chapter 1: What is a Blockchain?

A blockchain is a shared distributed ledger that allows for the recording of transactions and asset tracking on a network. An asset can be anything from a house, a car, land, or even patents, copyrights, or branding. Anything of value can be tracked and traded on a blockchain network. This reduces the risk and cuts costs for anyone involved in the tracking process. In terms of Bitcoin and the blockchain, think of the blockchain as the operating system and Bitcoin as the application that is running on the operating system. Bitcoin is only the first use case for the Blockchain [5].

Blockchains are a new and developing technology that may further protect against data breaches. They are defined as incorruptible digital ledgers of economic transactions that have the ability to be programmed to record everything of value. Blockchains have created the backbone of a new internet system by allowing the distribution of digital information but not allowing that digital information to be copied. Blockchains are defined as incorruptible digital ledgers of economic transactions that have the ability to be programmed to record everything of value. Blockchains have created the backbone of a new internet system by allowing the distribution of digital information but not allowing that digital information to be copied [1].

They were originally devised for Bitcoin, the digital currency, but the technology community is finding other potential uses for them. Blockchains allow digital information to be distributed but not copied. Information shared on a blockchain exists as a shared and continually updated database. Information is public, easily verifiable, and is not stored in one single location. Therefore, it makes it extremely difficult for hackers to corrupt the data since no centralized version of this information exists. Since blockchains store blocks of information that are identical across the network, the blockchain can't be controlled by one single entity and it has no single point of failure. Therefore, data breaches may be prevented by potentially storing user information or any other confidential information on a blockchain. A blockchain can be viewed as a spreadsheet that is duplicated across a network of computers that's designed to regularly update this spreadsheet [1].



Chapter 2: Basic Concepts and Benefits of a Blockchain

I. Decentralization

Decentralized technology lets us store data on a network that can be accessed over the Internet [4]. Through the decentralized technology, the owner of the data has direct control through their private key which is directly linked to the data [4].

Anything that happens on the blockchain network is a function of the network as a whole [1]. Therefore, the blockchain is managed by all nodes on its network instead of a single entity. Decentralization is defined as the networking operating on a user-to-user/peer-to-peer basis [1].

Blockchains are defined as public ledgers of all transactions and communications that have ever been executed on the network [3]. They are comprised of a network of nodes that get a copy of the blockchain that is automatically downloaded once they join the blockchain network [1]. A block is the "current" part of the blockchain that records some or all of the recent communications [3]. Once the communication or transaction is completed, the block goes into the blockchain as a permanent database [3]. Once a block is completed, a new block is generated [3]. These blocks are linked

together in the form of a chain in linear chronological order with every block containing a hash of its previous block [3].

Since blockchains store blocks of data that are identical across the network, blockchains cannot be controlled by a single entity and they have no single point of failure [1]. The blockchain network operates on a consensus mechanism that automatically checks in with itself every 10 minutes and reconciles every transaction that happens in these 10 minute intervals [1].

Reasons for Decentralization [4].
Empowered Users: allows users to keep control of their information and transactions.
Fault Tolerance: less likely to fail accidentally since they rely on many separate components that are not likely to fail.
Durability and Attack Resistance: Since the blockchain doesn't have a central point of control and can better survive malicious attacks, decentralized systems are more "expensive" to attack and destroy or manipulate.
Free from Scams: it is much more difficult for users to cause harm to other users by scamming.
Removing Third-Party Risks: enables users to make an exchange without a third party as an intermediary which eliminates risks.
Higher Transaction Rate: transactions can reduce times to minutes and can be processed anytime compared to how transactions are done through banks now.
Lower Transaction Costs: done through eliminating 3rd party intermediaries and overhead costs for exchanging assets.
Transparency: changes to public blockchains are viewable by all parties and all transactions are immutable which means they cannot be altered or deleted.
Authenticity: the blockchain is complete, consistent, timely, accurate, and widely available.

II. Consensus

for a transaction to be valid, all participants must agree on the validity of the Transaction [5]

III. Provenance

participants know where the asset came from and how its ownership changed over time [5]

IV. Immutability

no participant can tamper with a transaction once it has been recorded to the blockchain. If a transaction was made by mistake and a change needs to be made, a new transaction must be used to reverse the error. Both transactions remain on the blockchain [5]

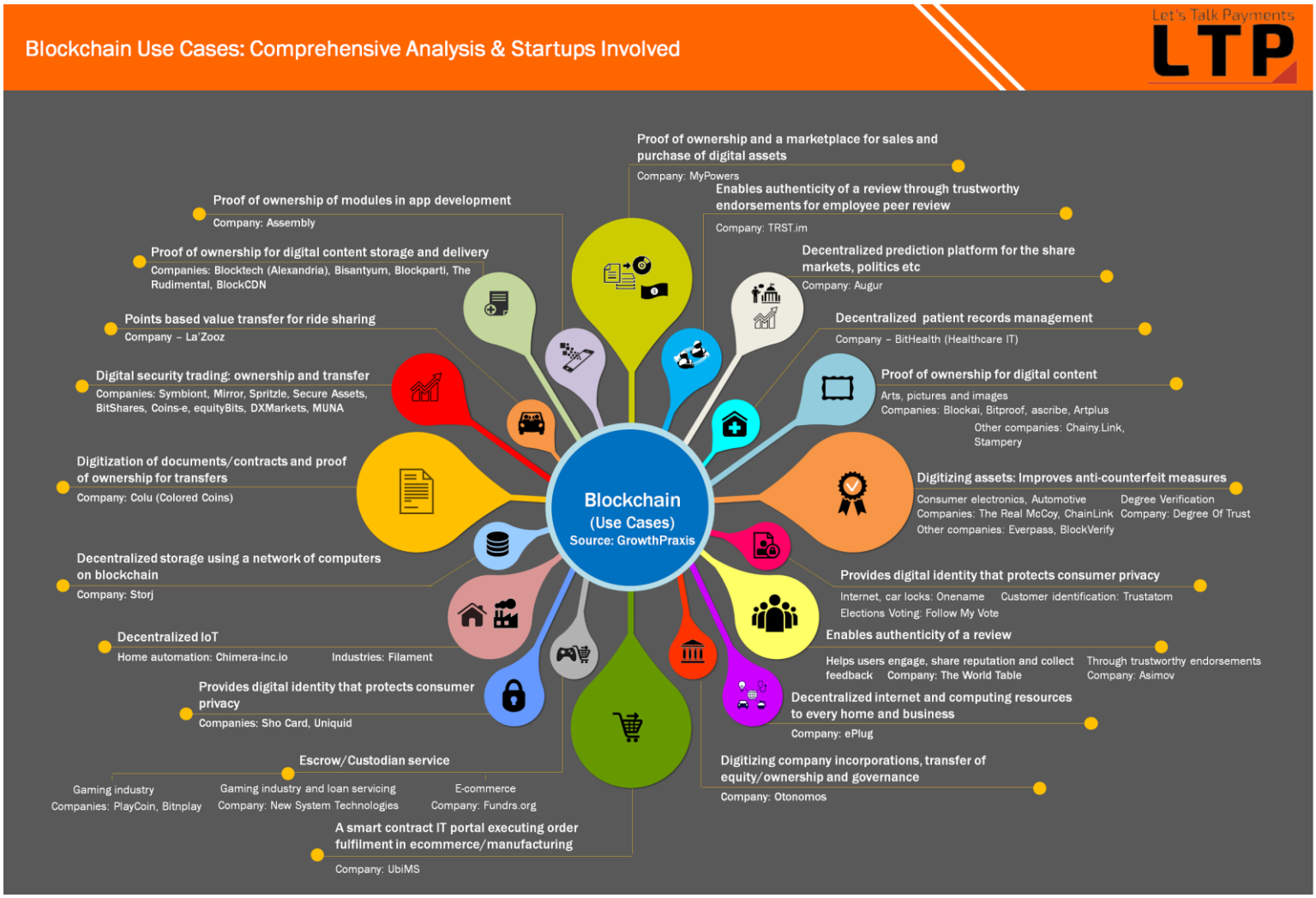
V. Finality

a single, shared ledger provides one place to go to determine who owns the asset or if a transaction has been completed [5]

Chapter 3: Blockchain Applications

The concepts of parallel blockchains and sidechains allow for tradeoffs and improved scalability using independent blockchains which allow for further innovation [3]. Various benefits of blockchains include decentralization, recording and validating every transaction which provides security and reliability, authorization of transactions by miners which make the transactions immutable and prevent hacking threats, and they discard the need for third-party or central authority for P2P transactions [3]. Various companies and institutions are studying blockchains to apply them to various areas such as money transfers, risk management, smart bonds, and cryptocurrencies.

Smart Contracts
Sharing Economy
Crowdfunding
Governance
Supply Chain Auditing
File Storage
Prediction Markets
Protection of Intellectual Property
Internet of Things
Neighborhood Microgrids
Identity Management
AML and KYC
Data Management
Land Title Registration
Stock Trading



// insert all use cases for applications here

Chapter 4: Blockchains and Security

Blockchains eliminate the risk with data being held in a central location since they store data across its network [1]. Computer hackers will no longer be able to exploit central points of vulnerability when networks implement the blockchain for data [1]. Blockchain uses encryption for security with public and private keys as a basis. A public key is a long and randomly-generated string of numbers and is used as the user's' address on the blockchain [1]. Any actions done by the user on that network get recorded as belonging to that specific public key [1]. The private key is used as a "password" that gives its owner access to assets on the network [1].

Chapter 5: Blockchains and Web 3.0

Chapter 6: Blockchain and the CIA Triad

There are two main types of blockchains: public and private. Public Blockchains are permissionless, meaning that data is publically available to anyone who wishes to participate on the network [2]. Private Blockchains are permission based platforms established by groups or individual firms, or divisions within an organization. Data can only be accessed by those users who are part of the group and are properly authenticated [2]. Blockchains can help with digital identities and maintaining data integrity. They have the ability to improve cyber defense since they can secure and prevent fraudulent activities and detect data tampering based on their underlying characteristics of immutability, transparency, auditability, data encryption, and operational resilience [2].

Confidentiality

The CIA triad represents confidentiality, integrity, and availability. Confidentiality is defined as the property that sensitive information is not disclosed to unauthorized individuals, entities, or processes [2]. The main concern of confidentiality is ensuring only interested and authorized parties can access the correct and appropriate data to them [2]. If an attacker can gain access to the blockchain network, then they are more likely to gain access to the data. Therefore, authentication and authorization controls need to be implemented [2]. Various blockchain implementations are starting to address data confidentiality and access control challenges by providing full block data encryption and AAA capabilities. [2]. Full encryption of blockchain data ensures that it won't be accessed by unauthorized parties while this data is in transit.

With public blockchains, there's no requirement to control network access since the chain protocols allow anyone to access and participate in the network [2]. Private blockchains require that appropriate security controls are in place to protect network access. Blockchains can provide advanced security controls: leveraging the public key infrastructure (PKI) to authenticate and authorize parties, and encrypt their communications [2].

Today, if an attacker gains access to the blockchain network and its data, this doesn't always mean that the attacker can read or retrieve the information stored on the blockchain. Full encryption of data blocks can be applied to guarantee its confidentiality. End-to-End Encryption ensures that only those who have authorization to access the encrypted data i.e.

through their private key can decrypt and see the data [2]. Using encryption keys along with PKI on a blockchain can provide higher levels of security. Implementing secure communication protocols on a blockchain guarantees that even when an attacker tries to do a man-in-the-middle attack, the attacker won't be able to either forge the interlocutor's identity or disclose any data while in transit [2]. Accessing the blockchain from multiple devices using the same key can put the organization at a higher risk of losing control of their private keys.

Integrity

Integrity is defined as guarding against improper information modification or destruction. It includes ensuring information nonrepudiation and authenticity [2]. This may consist of data encryption, hash comparison, or digital signatures. Blockchains have built in immutability and traceability that provide means for data integrity.

Blockchains are secure from the perspective that they enable users to trust that the transactions stored on them are valid [2]. Blockchains use sequential hashing and cryptography. They also have a decentralized structure. These 3 characteristics make it very challenging for any party to tamper with it compared to a standard database [2]. 51% of users need to agree a transaction is valid before it is added to the blockchain (consensus model protocol).

Blockchains guarantee that nothing will be erased. The solution to the "right to be forgotten" problem of integrity is to encrypt the personal information written in the system to ensure that forgetting the keys will ensure that the information is no longer accessible. Therefore, we should focus on blockchain's value to provide unaltered evidence of facts by writing the hash of transactions to it, while the transactions themselves are stored outside of the system. This ensures integrity of transactions and enables the ability to erase transactions, leaving only small traces of forgotten information on the chain. Every transaction added to a blockchain (private or public) is digitally signed and timestamped. The organization can trace back to a specific time period for each transaction and identify the party (through their public address) on the blockchain [2]. Nonrepudiation is the assurance that someone can't duplicate the authenticity of their signature on a file or the authorship on transaction that they originated [2]. It increases the reliability of the system (detection of tamper events or fraudulent transactions) since every transaction is cryptographically associated to a user. Any new transaction added to the blockchain will result in a change of the global state of the ledger. The implication is that with every new iteration of the system, the previous state of the system

will be stored which results in a fully traceable history log [2]. This provides entities with an extra level of reassurance that data is authentic and hasn't been tampered with.

Availability

Availability means ensuring timely and reliable access to and use of information. The Distributed Denial of Service (DDoS) is the most common attack and can cause the most disruption to internet services as websites are disrupted and apps become unresponsive [2]. DDoS attacks on blockchain networks are costly since they attempt to overpower the network with large volumes of small transactions. The decentralization and peer-to-peer characteristics of the blockchain make it harder to disrupt than client-server architectures. Blockchains are also subject to DDoS attacks but they are able to withstand them a lot better than regular network architectures. Since Blockchains have no single point of failure, this decreases the chances of an IP-based DDoS attack disrupting normal operation. If a node is taken down, data is still accessible via other nodes on the network since they all have a full copy of the blockchain at all times [2]. Bitcoin has withstood cyber-attacks for more than 7 years. Organizations can still face risks from external events outside of their control despite using blockchains (i.e. global internet outage) [2]. Blockchains have operational resistance due to their combination of peer-to-peer nature and number of nodes on the network, operating in a distributed and 24/7 manner. Organizations can make a node under attack redundant while the rest operate as usual. Even if a major part of the blockchain is under attack, it'll operate as normal due to the distributed nature of the technology. Obviously, blockchains aren't "bullet-proof."

Chapter 7: Centralization vs. Decentralization

Chapter 8: Security Properties of the Blockchain

Chapter 9: Smart Contracts vs. Blockchain

Chapter 10: Blockchain Performance and Maintenance

Chapter 11: Blockchain Capabilities and Limitations

Chapter 12: Blockchain Tutorial

Creating a Private Ethereum Blockchain

Step 1: Install Geth and Mist
GETH: https://geth.ethereum.org/downloads/ - install appropriate version
MIST: https://github.com/ethereum/mist/releases --install appropriate version

Unzip Geth and Mist to a safe location. Geth is the executable that syncs the blockchain to your computer. Mist is used to track the sync progress and is also the platform to use for connecting to the public Ethereum blockchain or a testnet.

Step 2: Run Ethereum-Wallet.exe within the Mist/Ethereum Wallet folder. This will visually show the progress of the Ethereum Sync

Step 3: Run Geth.exe within the Geth folder previously downloaded. This will initialize the syncing of the blockchain.

Installing Nodejs Using Windows Terminal

Windows CMD Command List: https://commandwindows.com/command3.htm

cd | chdir: displays name of curr directory or changes curr directory
cls: clears the screen
dir: displays list of folders and subfolders (ls)
mkdir: make a folder in current directory

pushd/popd: change current directory

Step 1: Install nodejs : https://nodejs.org/en/ 8.9.0 (node -v in CMD to check nodejs version)

Step 2: Install npm using npm install --global

Installing git and web3js Using CYGWIG Terminal

Step 1: Install git - https://git-for-windows.github.io/

Follow install instructions and keep default selections. Once you finish, restart your CMD. Type git version in cmd and you should see the version

Step 2:

Step 2:

References [IEEE]

[1]"What is Blockchain Technology? A Step-by-Step Guide For Beginners", Blockgeeks, 2017.

[2] E. Piscini, D. Dalton and L. Kehoe, "Blockchains and Cyber Security", Deloitte, 2017.

[3] "Know more about Blockchain: Overview, Technology, Application Areas and Use Cases - Lets Talk Payments", Lets Talk Payments, 2017.

[4]"4 Key Features of Blockchain", Techracers, 2017.

[5]M. Gupta, Blockchain for Dummies. for Dummies: A Wiley Brand, 2017.