PLE IT 461 - Implementing Internet Applications: Overview

Module Outline

6. Introduction to Blockchain

- **6.1.Blockchain Technology**
  - 6.1.1. What is Blockchain?
  - 6.1.2. Hashing
  - 6.1.3. Hash Chain of Blocks
  - 6.1.4. Public Key Cryptography
  - 6.1.5. Securing Hashchain With Public Key Cryptography
  - 6.1.6. Blockchain: Hashchain Inside Hashchain
  - 6.1.7. Consensus Mechanism
  - 6.1.8. Glossary
- **6.2.Blockchain Applications**
  - 6.2.1. A Brief History
  - 6.2.2. Distributed Consensus
  - 6.2.3. Smart Contracts
  - 6.2.4. Financial Applications
  - 6.2.5. Non-Financial Applications
  - 6.2.6. Future of Blockchain Applications

6. Introduction to Blockchain

6.A. Assignments

Assignments	Description	Deliverables	Due Date
1. Readings	Please complete the Required Readings in the Resources section of this module: *Blockchain: Simple Explanation.* Mazonka, Oleg. "Blockchain: Simple Explanation" (PDF). Journal of Reference. Volume 16, January 2017. http://jrxv.net/x/16/chain.pdf *Blockchain: How This Remarkable Technology Will Impact You, Your Organization and Society*. Mercer White Paper, January 2019. https://www.mmc.com/content/dam/mmc-web/insights/publications/2019/jan/gl-2019-blockchain-101-overview-mercer.pdf Optionally, please complete the optional reading in the Resources section of this module.	None	Jul. 25, 2020 - 11:59 pm
2. Complete the module content	Complete the following tasks: 1. View all module content. 2. Review the available resources and explore them as your interest and time permit. 3. Read the Summary page.	None	Jul. 25, 2020 - 11:59 pm
4. Participate in the module discussion forum	Please make at least two postings on the module discussion forum. One posting should include your reflection on this module (an initial posting) and the other should be a reply to another student's posting (peer posting). **Purpose** To reflect on your learning. **Tasks with Directions** Use Blockchain Forum to post a reflection about the knowledge/lessons learned. Then read the posts of the other students in the course and comment on at least one other student's post. **Submission Guidelines** Go to the Discussion Board page in Blackboard. Select Blockchain Forum and post. **Grading/Evaluation Criteria** Refer to the rubric that appears in the Syllabus under the Student Responsibilities section.	Two postings in the discussion board forum	Jul. 25, 2020 - 11:59 pm
5. Submit module feedback	Please complete the feedback form for this module. Your feedback is valuable and will be used for the current and future offerings of this course.	Feedback Form	

6.1.Blockchain Technology

6.1.1. What is Blockchain?

A blockchain is a decentralized, distributed, and oftentimes public, digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks.

Blockchain was invented by a person (or a group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The identity of Satoshi Nakamoto is unknown. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server.

A blockchain, originally block chain, is a growing list of records, packaged in blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

By design, a blockchain is resistant to modification of the data. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network that collectively adheres to a protocol for inter-node communication and for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority or through other consensus mechanisms. Although blockchain records are not unalterable, blockchains are considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance (able to continue operating even if some of the nodes fail or act maliciously).

A blockchain is essentially a hashchain in traditional computing terms. To understand blockchain, you need to know the following concepts:
• Hashing
• Hash chain
• A little bit of crypotography

Below is a video on how blockchain works, from Simply Explained on youtube:

Embedded Content - Available Online Only
Source: https://www.youtube.com/watch?v=SSo_EIwHSd4.

6.1.2. Hashing

A hash is a fingerprint of some input data. **A hash function is any function that can be used to map data of arbitrary size to data of a fixed size, called hash.** Hashing can be used to retrieve data, to verify that data hasn't changed, and to transport data without revealing the orginial. For example, passwords are often hashed.

One of the simplest hash functions is the modulo operation. Any digital string can be converted into a number (possibly very big); this number can be divided by a constant; and the remainder of that division is the result, hash. Obviously, the result is less than the constant, because its size is no greater than the size of the constant. This hash function is simple, but at the same time, it is not used too often, because people want to have another property: one-way computation. It should be easy to compute the hash, but finding any input to the hash function must be difficult, or better, virtually impossible.

Hash functions with the one-way computation property are sometimes called cryptographic hash functions. A cryptographic hash is like a signature or fingerprint for a data set. If you would like to compare two sets of raw data (source of the file, text or similar), it is better to hash it and to compare hashed values of a fixed size. Even if only one symbol is changed the algorithm will produce a different hash value. Some hashing algorithms are designed to produce unique hashes; in other words, diferent source data always (or with very small possibilty) result in different hash values.

The SHA (Secure Hash Algorithm) is one type of cryptographic hash functions. The one-way (or nearly ireversible) computation property and unique (or nearly-unique) hashing property make SHA suitable for checking integrity of your data, challenge hash authentication, anti-tamper, digital signatures, and blockchain.

For eample, SHA256 algorithm generates a fixed size 256-bit (32-byte) hash.

SHA256("abc") = ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad

SHA512 algorithm generates a fixed size 512-bit (64-byte) hash:

SHA512("abc") =
ddaf35a193617abacc417349ae20413112e6fa4e89a97ea20a9eeee64b55d39a2192992a274fc1a836ba3c23a3feebbd454d4423643ce80e2a9ac94fa54ca49f

Please try out the SHA256, SHA512 and several other cryptographic generators at https://www.freeformatter.com/

Below is a video on hash functions, from Simply Explained on youtube:

Embedded Content - Available Online Only

Source: https://www.youtube.com/watch?v=cczlpiiu42M.

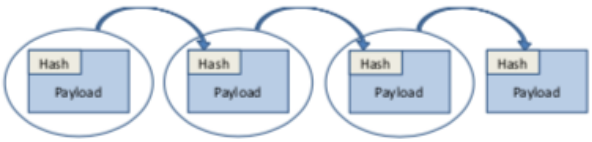
6.1.3. Hash Chain of Blocks

Hashchain is a sequence of homogeneous data chunks, or simply blocks, linked together by a hash function. Figure 1 schematically shows a simple hashchain.

Each data block consists of the payload and the hash of previous block. The payload in each block is arbitrary data. This hashchain has the important property: no data can be modified at any block without affecting the integrity of the subsequent blocks. For example, if the payload of the first block is changed, then the hash of the second block must be changed as well, and hence the hash of the third, and so on.

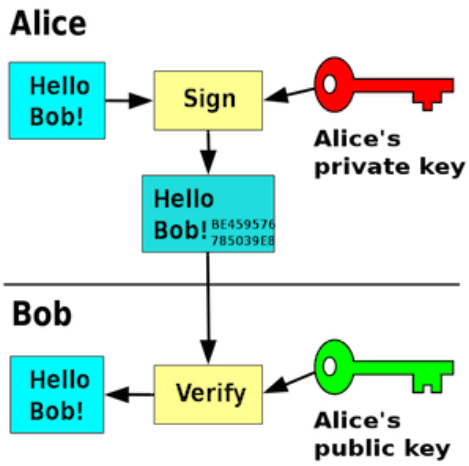
The next step is to make blockchain actions accountable, such as when creating a new block in the chain or updating data in a block. One way to do it is Public Key Cryptography (PKC), which is also an important concept in cybersecurity.

Figure 1



A simple hashchain

6.1.4. Public Key Cryptography



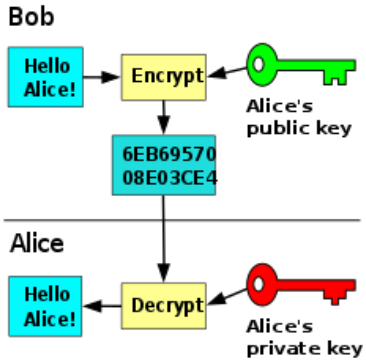
Digital signature with private key

The basic idea of Public Key Cryptography (PKC) is similar to secure hash functions – one way computation. Given some data m (m for message) anyone can compute encrypted value Encrypt(m). But, only the one who knows a special key related to this encryption can compute in the opposite way, i.e. find m from Encrypt(m). The latter process is called decryption.

To achieve PKC, one must first create a so-called pair of keys: public and private. The public key is used to encrypt data and can let be known to anyone. The private key is used to decrypt and must be kept in secret.

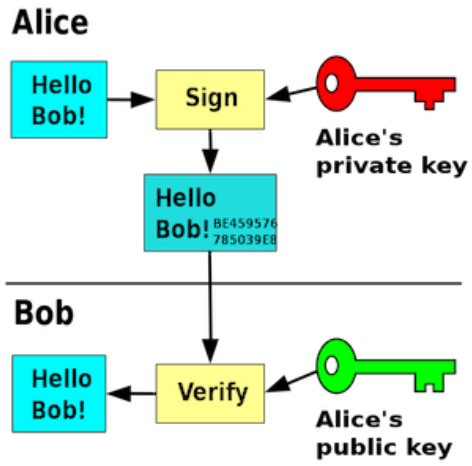
Two of the best-known uses of public key cryptography are:

Public key encryption, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key. This is used in an attempt to ensure confidentiality.



Public key encryption

Digital signatures, in which a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. This verification proves that the sender had access to the private key, and therefore is likely to be the person associated with the public key. This also ensures that the message has not been tampered with, as a signature is mathematically bound to the message it originally was made with, and verification will fail for practically any other message, no matter how similar to the original message.



Digital signature with private key

Below video explains Public Key Crypotography, which is one type of asymetric encryption, from Simply Explained on youtube:

Embedded Content - Available Online Only

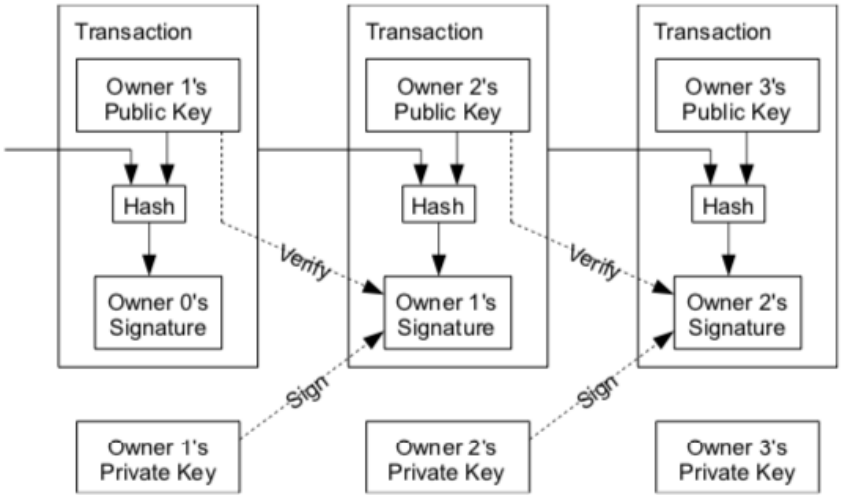
Source: https://www.youtube.com/watch?v=AQDCe585Lnc.

6.1.5. Securing Hashchain With Public Key Cryptography

Hashchain with PKC (public key cryptography) authorization can perform as a function for secure transfer of digital objects, often called tokens. Suppose that one hashchain represents a token. It may be something to which the real world assigns a value. The owner of the last block is the owner of this value because only he is able to pass it to somebody else.

If the last block contains the public key of the current owner and the digital signature of the previous block owner, then creation of the next block will require the signature of the current block, i.e. of the person who has the private key. When creating a new block, the current owner places another public key in the next block and signs that block. So the next block will be owned by whoever keeps the private key that corresponds to the newly published block. And the signature proves that only the previous owner could have done that.

Below is an illustration of the Bitcoin implementation, from the original Bitcoin paper, "Bitcoin: A Peer-to-Peer Electronic Cash System."

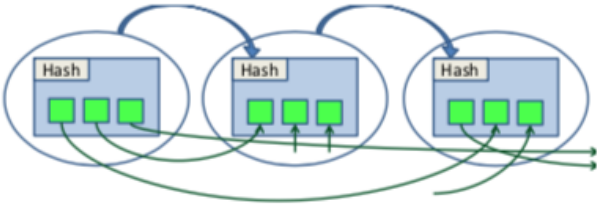


Bitcoin's Transaction Chain (from "Bitcoin: A Peer-to-Peer Electronic Cash System")

The meaning of "transactions" depends on the usage scenario of blockchain. Below is from Bitcoin: "We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership."

6.1.6. Blockchain: Hashchain Inside Hashchain

Imagine that there is a place where a continuous process constantly creates new blocks for a global hashchain. And imagine that you can place any data you like into the payload of the blocks of that global hashchain. If such a place and process would exist, then you can insert the blocks of a hashchain that represent values into the blocks of this global hashchain. In other words, that would be one hashchain inside another hashchain. Most blockchain systems utilize this hashchain-of-hashchain mechanism.



External and Internal Hashchains

The figure above shows an external hashchain where block data consists of blocks of internal hashchains. The blocks of the internal hashchains can chaotically appear in the external hashchain. The obvious condition is that older internal blocks cannot appear in newer external blocks. In blockchain solutions, the global hashchain is distributed among many computers. The external hashchain plays the role of the central repository, effectively replacing any authority entity. The external hashchain carries bits and pieces of internal hashchains, whose function includes uniquely and reliably binding the tokens (digital items of value) with their owners.

While the actual implementation of a blockchain may be different, recall the general definition of a blockchain: A blockchain is a decentralized, distributed, and oftentimes public, digital ledger that is used to record transactions across many computers, so that any involved record cannot be altered retroactively without the alteration of all subsequent blocks.

6.1.7. Consensus Mechanism

Different solutions exist for organizing the global hashchain and for making sure that the global hashchain is a trusted, agreed source of truth.

In a Bitcoin network, any participant can create a new block for the external hashchain as the carrier for blockchain transactions, and receive rewards for the new block creation. Since many parties try to create blocks, some different blocks are created independently. Since the propagation is not instant, new blocks may be created on top of those independently created blocks. That makes the global hashchain branch. But a rule ensures that there is only one current valid copy of the global hash chain distributed among many computers. In a Bitcoin network, the rule makes sure that only the longest branch is considered to be valid. This rule works fine because block creation in Bitcoin network requires significant computing work; hence, the probability of two or more branches surviving die out very quickly. In other words, the consensus (on the valid chain) in a Bitcoin network is achieved by proof-of-work.

Many newer blockchain systems adopt proof-of-stake as the consensus mechanism, which does not require expensive computing operations and which leads to energy and cost savings. With proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as a stake. The proof-of-stake consensus mechanism assumes that a majority of wealth is held by good actors; collusion in this distributed network is uncommon, and bad actors can be penalized with loss of stakes.

Below is a video on proof-of-stake vs. proof-of-work, from Simply Explained on youtube:

Embedded Content - Available Online Only
Source: https://www.youtube.com/watch?v=M3EFi_POhps.

6.1.8. Glossary

Blockchain technology is developed and shaped by many individuals and organizations. We should know the following commonly agreed technology definitions from the National Institute of Stantards and Technology (NIST.IR.8202):

Assets: Anything that can be transferred.

Asymmetric-key cryptography: A cryptographic system where users have a private key that is kept secret and used to generate a public key (which is freely provided to others). Users can digitally sign data with their private key and the resulting signature can be verified by anyone using the corresponding public key. Also known as Public-key cryptography.

Block: A data structure containing a block header and block data.

Blockchain: Distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

Consensus model: A process to achieve agreement within a distributed system on the valid state. Also known as a consensus algorithm, consensus mechanism, consensus method.

Cryptocurrency: A digital asset/credit/unit within the system, which is cryptographically sent from one blockchain network user to another. In the case of cryptocurrency
creation (such as the reward for mining), the publishing node includes a transaction sending the newly created cryptocurrency to one or more blockchain network users. These assets are transferred from one user to another by using digital signatures with asymmetric-key pairs.

Cryptographic hash function: A function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties:

1. (Preimage resistant) It is computationally infeasible to compute the correct input value given some output value (the hash function is ‘one way’).
2. (Second preimage resistant) One cannot find an input that hashes a specific output.
3. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output

Digital asset: Any asset that is purely digital, or is a digital representation of a physical asset

Digital signature: A cryptographic technique that utilizes asymmetric-keys to determine authenticity (i.e., users can verify that the message was signed with a private key corresponding to the specified public key), non-repudiation (a user cannot deny having sent a message) and integrity (that the message was not altered during transmission).

Hash chain: An append-only data structure where data is bundled into data blocks that include a hash of the previous data block’s data within the newest data block. This data structure provides evidence of tampering because any modification to a data block will change the hash digest recorded by the following data block.

Hash value: The output of a hash function (e.g., hash(data) = digest). Also known as a message digest, digest or hash digest.

Immutable: Data that can only be written, not modified or deleted.

Ledger: A record of transactions.

Permissioned: A system where every node, and every user must be granted permissions to utilize the system (generally assigned by an administrator or consortium).

Permissionless: A system where all users’ permissions are equal and not set by any administrator or consortium.

Proof of stake consensus model: A consensus model where the blockchain network is secured by users locking an amount of cryptocurrency into the blockchain network, a process called staking. Participants with more stake in the system are more likely to want it to succeed and to not be subverted, which

gives them more weight during consensus.

Proof of work consensus model: A consensus model where a publishing node wins the right to publish the next block by expending time, energy, and computational cycles to solve a hard-to-solve, but easy-to-verify problem (e.g., finding the nonce which, when combined with the data to be added to the block, will result in a specific output pattern).

Reward system: A means of providing blockchain network users an award for activities within the blockchain network (typically used as a system to reward successful publishing of blocks). Also known as incentive system.

Smart contract: A collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network. The smart contract is executed by nodes within the blockchain network; all nodes must derive the same results for the execution, and the results of execution are recorded on the blockchain.

Transaction: A recording of an event, such as the transfer of assets (digital currency, units of inventory, etc.) between parties, or the creation of new assets.

Transaction fee: An amount of cryptocurrency charged to process a blockchain transaction. Given to publishing nodes to include the transaction within a block.

Turing complete: A system (computer system, programming language, etc.) that can be used for any algorithm, regardless of complexity, to find a solution.

Wallet: Software used to store and manage asymmetric-keys and addresses used for transactions.

6.2.Blockchain Applications

6.2.1. A Brief History

When Satoshi Nakamoto, whose true identity is still unknown, released the whitepaper "Bitcoin: A Peer to Peer Electronic Cash System" in 2008 that described a “purely peer-to-peer version of electronic cash” known as Bitcoin, blockchain technology made its public debut.

Blockchain, the technology that runs Bitcoin, has developed over the last decade into one of today’s biggest ground-breaking technologies, with the potential to impact every industry -- from financial to manufacturing to educational institutions. Here’s a brief history of blockchain technology.

Bitcoin Beginnings: Shortly after Nakamoto’s whitepaper was released, Bitcoin was offered up to the open source community in 2009. Blockchain provided the answer to digital trust because it records important information in a public space and doesn’t allow anyone to remove it. It’s transparent, time-stamped, and decentralized. In a few years, similar cryptocurrencies flourished.

Blockchain Separates from Bitcoin and Cryptocurrencies: Around 2014, people started to invest in and explore how blockchain could alter many different kinds of operations. At its core, blockchain is an open, decentralized ledger that records transactions between two parties in a permanent way without needing third-party authentication. This creates an extremely efficient process and dramatically reduces the cost of transactions. When entrepreneurs understood the power of blockchain, there was a surge of investment and discovery to see how blockchain could impact supply chains, healthcare, insurance, transportation, voting, contract management and more.

Smart Contracts: Vitalik Buterin, an initial contributor to the Bitcoin codebase, became frustrated with Bitcoin's programming limitations and pushed for a malleable blockchain. Met with resistance from the Bitcoin community, Buterin and others set out to build the public blockchain called Ethereum. The largest difference between the two is that Ethereum can record other assets, such as loans or contracts -- not just currency. Ethereum launched in 2015 and can be used to build “smart contracts”—those that can automate a business process. This technology has attracted the attention of corporations that are intrigued by the potential of the smart contract functionality to save time and money.

Scaling blockchain technology: In a traditional blockchain network, every computer attempts to process every transaction, which can be very slow. As of early 2020, the average confirmation time for a Bitcoin transaction was over ten minutes (https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time/), and it took an average of 15 seconds for a transaction to be verified on the public Ethereum blockchain (https://ethgasstation.info/blog/ethereum-transaction-how-long/). Note that multiple confirmations are often required before a business transaction becomes “final”, and that the transaction time is often affected by network congestion and latency. In comparison, Visa can process 50,000 credit card transactions every second, and the banking industry uses systems that can do even more. On social media, tens of thousands of Facebook “Likes” happen every single second of the day. A scalable blockchain solution needs to allow transactions to occur at a much higher speed. Another issue is the transaction fee on blockchain networks. Average transaction fee is $4.82 on Bitcoin and $0.33 on Ethereum as of May 16, 2020 (ycharts.com). New blockchains have made various improvements to reduce the transaction costs and yet maintain the security. For example, a new blockchain protocol EOS.IO, powered by the native cryptocurrency EOS, claims to eliminate transaction fees and support millions of transactions per second (https://www.bitdegree.org/tutorials/eos-vs-ethereum/).

It has been an impressive decade of transformation for blockchain technology and it will be intriguing to see where the next decade takes us. (Forbes, Feb 16, 2018, "A Very Brief History Of Blockchain Technology Everyone Should Read")

Below is a video on how blockchain can be used in the real world:

Embedded Content - Available Online Only
Source: https://www.youtube.com/watch?v=aQWflNQuP_o.

6.2.2. Distributed Consensus

A blockchain is essentially a distributed database of records - a public ledger of all transactions or digital events that have occured and been shared among participating parties. Each transaction in the public ledger is verified by consensus of (a majority of) the participants in the system. And, once entered, information can never be erased. The blockchain thus contains a certain and verifiable record of every single transaction ever made. To use an analogy, it is easier to steal a cookie from a cookie jar kept in a secluded place than to steal the cookie from a cookie jar kept in a market place and being observed by thousands of people.

Bitcoin is the most popular example of blockchain technology. It is also the most controversial one, since it helps to enable a multibillion-dollar global market of anonymous transactions without any governmental control. It has triggered a number of regulatory concerns involving national governments and financial institutions. However, Blockchain technology itself is non-controversial, it has worked well over the years, and it is being successfully applied to both financial and non-financial world applications.

The current digital economy relies on certain trusted authorities. Most of our online transactions rely on trusting someone to tell us the truth—it can be an email service provider telling us that our email has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; it can be a social network such as Facebook telling us that our life events have been shared only with our friends; or it can be a bank telling us that our money has been delivered reliably to someone in a remote country. The fact is that we live our life precariously in the digital world by relying on a third entity for the security and privacy of our digital assets. The fact remains that these third party sources can be hacked, manipulated, or compromised.

This is where the blockchain technology comes handy. It has the potential to revolutionize the digital world by enabling distributed consensus, where each and every online transaction, past and present, can be verified at any time without any central authority or comprising the privacy of the parties involved. (BlockChain Technology: Beyond Bitcoin. Technical Report, October 2015, University of California at Berkeley. https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf)

6.2.3. Smart Contracts

A **smart contract** is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.

Many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing, or both. The aim of smart contracts is to provide security that is potentially superior to traditional contract law and to reduce contractual costs.

Smart contracts were first proposed in the early 1990s by computer scientist, lawyer, and cryptographer Nick Szabo, who coined the term. However, it did not find usage until the notion of crypto currencies or programmable payments came into existence. Now, blockchain and smart contract can work together to trigger payments when a pre-programmed condition of a contractual agreement is triggered. **Smart Contracts are the killer application of cryptocurrencies.** Blockchain technology makes it easier to register, verify, and execute Smart Contracts. Many cases where assets are transferred only upon meeting certain conditions require lawyers to create a contract and banks to provide Escrow service. Now, these lawyers and banks can be replaced by Smart Contracts.

The term "smart contract" is increasingly used to denote a computer program in the context of a blockchain or distributed ledger. In this interpretation, a smart contract is not necessarily related to the classical concept of a contract, but can be any kind of computer program. For example, Ethereum implements a Turing-complete language on its blockchain network and offers its programmable platform capabilities. Ethereum allows anyone to create their own cryptocurrency and to use that to execute and pay for smart contracts. Ethereum itself has its own cryptocurrency (ether) which is used to pay for the network services. Various blockchains are already powering a wide range of early applications in areas such as governance, autonomous banks, crowdfunding, financial trading, and settlement, using smart contracts.

Below is a video explaining smart contracts, from Simply Explained on youtube:

Embedded Content - Available Online Only
Source: https://www.youtube.com/watch?v=ZE2HxTmxfrI.

6.2.4. Financial Applications

Below are a few examples of financial applications using blockchain:

Crypocurrency: a digital asset designed to work as a medium of exchange wherein individual ownership records are stored in a digital ledger that uses strong cryptography. It typically does not exist in physical form, like paper money. Cryptocurrencies using blockchain technologies rely on decentralized control, as opposed to digital currency that relies on central banking systems. The blockchain serves as a public financial transaction database. Bitcoin, first released as open-source software in 2009, is the first decentralized cryptocurrency. Since the release of bitcoin, over 6,000 variants of bitcoin or other

cryptocurrencies have been created.

Private securities: It is expensive to take a company public. A syndicate of banks must work to underwrite the deal and attract investors. It is now theoretically possible for companies to directly issue the shares via a blockchain. These shares can then be purchased and sold in a secondary market that sits on top of the blockchain. Nasdaq first deployed blockchain technology on the secondary market it built, the Nasdaq Private Market, to enable secure issuance and transfer of shares of privately-held companies.

Cross-border payments: Blockchain can revolutionize international payments with simultaneous cross-border messaging, clearing, and settlement in seconds instead of days, creating a new global payment rail.

Asset leasing: Below is a video from IBM on how blockchain and smart contracts can used for car leasing:

Embedded Content - Available Online Only
Source: https://www.youtube.com/watch?v=IgNfoQQ5Reg.

6.2.5. Non-Financial Applications

Below are a few examples of non-financial applications using blockchain:

Certification and notarization: Verifying the authenticity of the document can be done using blockchain without the need for centralized authority. The document certification service includes Proof of Ownership (who authored it), Proof of Existence (at a certain time), and Proof of Integrity (not tampered) of the documents. Blockchain-based certification is counterfeit-proof, and it can be verified by independent third parties. Blockchain-based certification services secure the privacy of the document and those who seek certifications. By publishing cryptographic hashes of documents into a blockchain, the notary timestamping is taken to a new level. For example, Stampery (stampery.com) is a company which can stamp email or any files using blockchain. Many law firms use Stampery's technology for document certification.

Music industry: The music industry has gone through a big change in the last decade due to the growth of Internet and streaming services. The process by which music royalties are determined has always been a convoluted one, but the rise of the Internet has made it even more complex, giving rise to the demand of transparency in royalty payments. Blockchain can play a role by maintaining a comprehensive, accurate database of music rights ownership and music consumption in a public ledger. In addition to rights ownership, the royalty split for each piece of music as determined by "smart contracts" can be added to the database. The "smart contracts" would define relationships between different stakeholders, including artists, labels, publishers and streaming service providers, and automate their interactions. For example, Spotify acquired MediaChain, a peer-to-peer blockchain platform, to help solve royalty payment and rightsholder issues within the music industry.

Internet of Things (IoT): A vast majority of IOT platforms are based on a centralized model in which a broker or hub controls the interaction between devices, However, this centralized approach has become impractical for many scenarios in which devices need to exchange data between themselves autonomously. The blockchain technology facilitates the implementation of decentralized IoT platforms that support secured and trusted data exchange as well as record keeping. In such an architecture, the blockchain serves as the general ledger, keeping a trusted record of all the messages exchanged between smart devices in a decentralized IoT topology. IBM, in partnership with Samsung, has developed a platform ADEPT (Autonomous Decentralized Peer To Peer Telemetry), a decentralized Internet of Things (IOT). ADEPT uses three protocols-BitTorrent (file sharing), Ethereum (Smart Contracts) and TeleHash (Peer-To-Peer Messaging) in the platform.

Supply Chain: Blockchain has been widely used in supply chains. The video below demonstrates how IBM and Maersk are digitizing global trade to create trust and transparency in the supply chain using blockchain technology.

Embedded Content - Available Online Only
Source: https://www.youtube.com/watch?v=tdhpYQCWnCw.

6.2.6. Future of Blockchain Applications

The future of blockchain applications is literally unlimited. The video below, from Future Thinkers, on youtube shows a number of industries that blockchain will disrupt:

Embedded Content - Available Online Only
Source: https://www.youtube.com/watch?v=G3psxs3gyf8.

6.R. Resources

OPTIONAL READINGS

No.	Title	Type	Size
1	Bitcoin: A Peer-to-Peer Electronic Cash System. *The original bitcoin paper. https://bitcoin.org/bitcoin.pdf*		

REFERENCES

No.	Title	Type	Size
2	Top Blockchains of 2020. *https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/*		
3	A Very Brief History Of Blockchain Technology Everyone Should Read. *Forbes, Feb 16, 2018, "A Very Brief History Of Blockchain Technology Everyone Should Read" by Bernard Marr.*		
4	BlockChain Technology: Beyond Bitcoin. *BlockChain Technology: Beyond Bitcoin. Sutardja Center for Entrepreneurship & Technology Technical Report, October 2015, University of California at Berkeley. By Crosby, Michael; Nachiappan; Pattanayak, Pradhan; Verma, Sanjeev; Kalyanaraman, Vignesh*		
5	Simply Explained: a youtube channel.. *https://www.youtube.com/channel/UCnxrdFPXJMeHru_b4Q_vTPQ*		
6	IBM Blockchain: a youtube channel. *https://www.youtube.com/channel/UCpEJ53BOa9YWTTXerZtKNhg*		
7	Future Thinkers: a youtube channel. *https://www.youtube.com/user/wearefuturethinkers/videos*		
8	Average confirmation time of Bitcoin transactions from January 2018 to April 2020. *https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time/*		
9	How long does an Ethereum transaction really take? June 5, 2019. *https://ethgasstation.info/blog/ethereum-transaction-how-long/*		
10	EOS vs Ethereum – What's the Better Alternative? Updated Jan 17, 2020. *https://www.bitdegree.org/tutorials/eos-vs-ethereum/*		
11	Blockchain Technology Overview. *National Institute of Standards and Technology, Technology Report NIST.IR.8202, October 2018. doi.org/10.6028/NIST.IR.8202*		

REQUIRED READINGS

No.	Title	Type	Size
12	Blockchain: Simple Explanation. *Mazonka, Oleg. "Blockchain: Simple Explanation" (PDF). Journal of Reference. Volume 16, January 2017.*		
13	Blockchain, Mercer White Paper, January 2019. *https://www.mmc.com/content/dam/mmc-web/insights/publications/2019/jan/gl-2019-*		

blockchain-101-overview-mercer.pdf