Communications of the Association for Information Systems

Volume 45 Article 25

12-2019

Tutorial: A Descriptive Introduction to the Blockchain

Meg Murray
Kennesaw State University, mcmurray@kennesaw.edu

Recommended Citation

Murray, M. (2019). Tutorial: A Descriptive Introduction to the Blockchain. Communications of the Association for Information Systems, 45, pp-pp. https://doi.org/10.17705/1CAIS.04525

Communications of the Association for Information Systems

Tutorial DOI: 10.17705/1CAIS.04525 ISSN: 1529-3181

Tutorial: A Descriptive Introduction to the Blockchain

Meg Coffin Murray
Kennesaw State University
mcmurray@kennesaw.edu

Abstract:

Blockchain technology, which supports the bitcoin cryptocurrency, has risen to prominence as the technology that will transform how business transactions occur and parties manage assets over the Internet. A decentralized system, the blockchain provides a way to digitally record and securely store verifiable and immutable transactions, which eliminates the need for trusted third-party intermediaries. While simplistically described as a decentralized ledger, the blockchain is a complex technology that integrates peer-to-peer networking, cryptography, and distributed consensus. In this paper, I explain blockchain's components, describe how a blockchain works, identify use case examples from various industries, explore potentials and limitations, and speculate on the progressive adoption of the blockchain as a transformative technology.

Keywords: Blockchain, Decentralized Ledger, Value Transfer, Bitcoin, Technology Adoption.

This manuscript underwent editorial review. It was received 12/16/2018 and was with the author for 2 months for 2 revisions. Eric Ngai served as Associate Editor.

1 Introduction

Blockchain technology, a decentralized ledger technology, provides a trusted and secure platform for digitally recording and securely storing verifiable and permanent transactions between multiple parties in the digitized networked world. Accordingly, the technology eliminates the need for costly middleman validation and verification processes. Blockchain technology first supported the Bitcoin cryptocurrency and remains the foundation from which other blockchains have emerged. While Bitcoin's future remains volatile, many have touted blockchain as the technology that will transform how business transactions occur and parties manage assets over the Internet. While blockchain remains in the early stages of the technology adoption lifecycle, its acceptance has begun to rapidly expand beyond innovators to early adopters (Rogers, 2003).

A complex technology, blockchain at its core refers to "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way" (Iansiti & Lakhani, 2017, p. 4). However, the term decentralized ledger better describes the technology; the blockchain relies on variations of distributed computing principles (Herlihy, 2019). Rather than being distributed, networked computers duplicate the entire blockchain in a peer-to-peer fashion. The blockchain is decentralized—not stored in a single location—which makes it more difficult to hack or exploit. The ledger holds details of all transactions that the blockchain has processed. Transactions are verified and validated through a process that employs cryptography and digital signatures and groups such transactions into blocks that all the computers that participate in a blockchain network regularly replicate and reconcile through consensus. In short, the blockchain integrates three concepts: peer-to-peer networks, public-key/private-key cryptography, and distributed consensus. One needs to understand the intricacies involved in orchestrating the blockchain's technologies to conceive its usefulness and benefits. In this paper, I explain blockchain's components, describe how a blockchain works, identify example use cases from various industries, explore its potential and limitations, and speculate on the progressive adoption of the blockchain as a transformative technology.

2 The Origin and the Legend

A white paper called *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008) first introduced the blockchain concept. Although the paper lists Satoshi Nakamoto as the author, the individual's true identity remains unknown. Today, ardent Bitcoin and blockchain followers commonly speculate on the author's identity. Interestingly, the word blockchain never appeared in the white paper; instead, the paper referred to a "chain of blocks". Instead, Hal Finney, the well-known computer scientist who also received the first Bitcoin from Nakamoto, coined the term (Satoshi Nakamoto Institute, 2008). In October 2008, three months following the registration of the domain Bitcoin.org, Nakamoto distributed the white paper to a cryptocurrency mailing list. In January, 2009, Nakamoto released the Bitcoin software as an open source project and mined the first Bitcoin. To memorialize the event, Nakamoto encoded the date and headline from the *London Times*, "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" into the coinbase (first) transaction of the genesis (first) block of the Bitcoin blockchain ("Genesis Block", 2017). In 2011, after communicating via email and on digital message board posts for two years, Nakamoto ceased communication. Today, however, his legend lives on—more than one million unspent Bitcoins attributed to Satoshi Nakamoto exist, and the Bitcoin community has adopted the term "satoshi" to reference fractions of a Bitcoin. Figure 1 outlines Satoshi Nakamoto's activity timeline.

The precepts put forth in the original paper referenced technology and ideology. As its underlying theme, the paper posited that one could create a democratized currency free from government control that permitted parties to directly and anonymously transfer funds between one another (Feuer, 2013). As such, some claim Bitcoin represented a rebirth of the "cypherpunk" dream, a vision that cryptographic technology could generate social and political change by weakening government power (Narayanan, 2013). Nakamoto architected Bitcoin without the need for a third-party intermediary to validate transactions or a centralized authority to issue currency, but many believe Nakamoto did not envision Bitcoin as a radical political movement. Instead, they believe Nakamoto designed it to deal with challenges associated with digital currency—most notably, the double-spend problem and the need for decentralized trust (Au & Power, 2018). Narayanan, Bonneau, Felten, Miller, and Goldfeder (2016) review prior attempts to establish digital cash systems and how these systems influenced the development of Bitcoin in detail. While many continue to debate the ideology behind the Bitcoin currency, the notion of the blockchain as a mechanism to track digital assets has quickly gained traction.

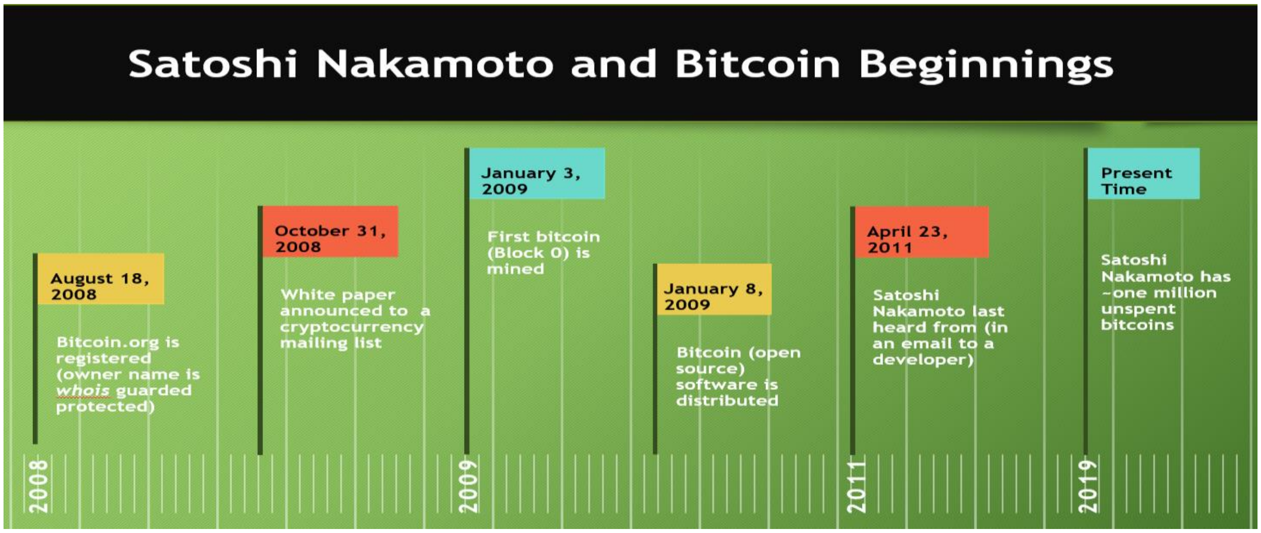

Satoshi Nakamoto and Bitcoin Beginnings
August 18, 2008
Bitcoin.org is registered (owner name is whois guarded protected)
October 31, 2008
White paper announced to a cryptocurrency mailing list
January 3, 2009
First bitcoin (Block 0) is mined
January 8, 2009
Bitcoin (open source) software is distributed
April 23, 2011
Satoshi Nakamoto last heard from (in an email to a developer)
Present Time
Satoshi Nakamoto has ~one million unspent bitcoins
2008
2009
2011
2019

Figure 1. Activities of Satoshi Nakamoto

Researchers have hailed blockchain technology as having the potential to revolutionize business, redefine companies, and reshape economies (Iansiti & Lakhani, 2017). They have attributed this disruptive potential largely to three factors: decentralization, the elimination of trusted intermediaries (Kaushal & Tyle, 2015), and a transaction system that supports irreversible transactions and an immutable ledger (Boaventura, 2018). They have frequently cited the benefits inherent in these features as motivations for organizations to adopt blockchain technology. Table 1 lists various blockchain traits mapped to commonly cited benefits. Blockchain remains in its infancy, so we have yet to try and test its benefits. However, genuine interest in and momentum around blockchain exists. The International Data Corporation (IDC) has forecasted an annual compound growth rate in blockchain spending of 81.2 percent until at least 2021 (Shirer & Goepfert, 2018), and Gartner has predicted this decade will end with blockchain business value growing to US$360 billion and surging to US$3.1 trillion by 2030 (Kandaswamy & Furlonger, 2018).

Table 1. Often-cited Blockchain Benefits

Blockchain trait	Benefit
User-controlled, open-source project	The blockchain is an open source project; no central authority owns or controls the software, which gives developers and users control over technology decisions.
Decentralized ledger	The blockchain is a decentralized system with no single point of failure.
Transparent yet private	Everyone can see all transactions in a blockchain, which provides traceability, but it retains no personally identifiable information.
One-way, non-reversible transactions	The blockchain avoids double-spend and chargebacks, which reduces the risk of fraudulent transactions.
Immutable	One cannot easily change data in a blockchain, which provides a permanent unalterable transaction history that facilitates an efficient and cost-effective audit process.
No third-party verification required	The blockchain reduces transaction costs.
Versatile	One can use the blockchain with any valuable asset that can be represented digitally.
Security	The blockchain incorporates cryptography, hashing, and consensus protocols to maintain transaction integrity.

3 The Blockchain Ledger

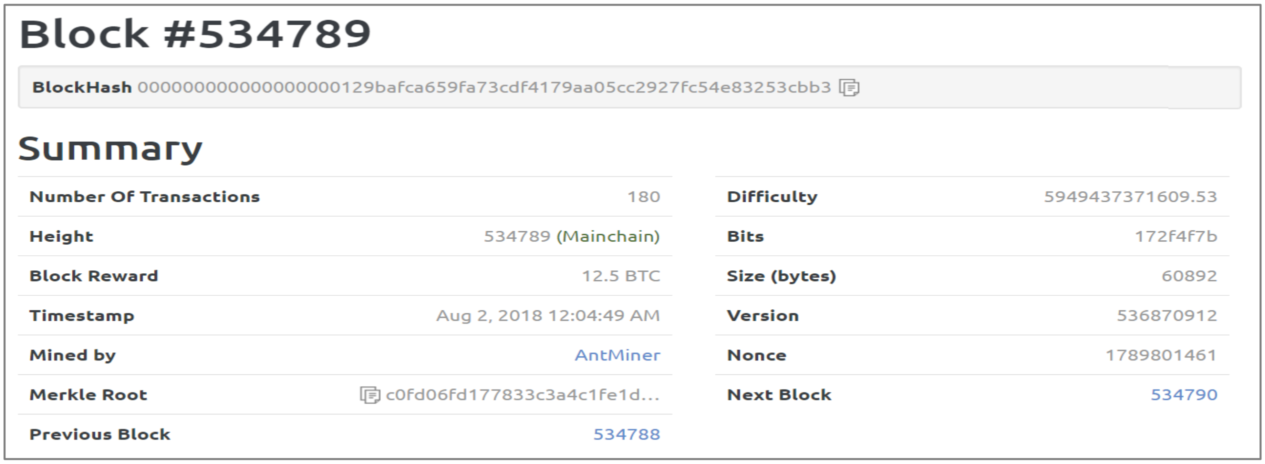
Blockchain verifies and records transactions. Specifically, a blockchain comprises a series of blocks contain transactions linked together in chronological order. An individual block comprises a listing of transactions and a block header. The metadata of the block header serves three purposes: it provides a unique summary of the block, a reference to the previous block, and parameters related to the consensus protocol used to validate newly formed blocks. Table 2 lists the type of data in a block header of blocks on the Bitcoin blockchain. The first two fields contain basic information such as software version and timestamp. Blockchain uses cryptographic hashing to uniquely identify each block, but it retains only the identifier of the previous block in the block header of the current block. Blockchain also uses cryptographic hashing via a Merkle tree root to create a unique summary identifier of all transactions included in the block. The remaining two fields, the difficulty target and the nonce, relate to the proof-of-work consensus protocol that Blockchain uses to create new blocks (i.e., mining in Bitcoin). I describe hashing and Merkle trees in detail in Section 4.2 and consensus mechanisms in Section 4.3.

Table 2. Metadata Fields in a Bitcoin Blockchain Block Header

Field	Description
Software version	Denotes validation rules used in this version of the blockchain software.
Timestamp	Creation time of the block (seconds from Unix epoch time)
Previous block identifier	Hash of the previous block's block header
Merkle root	Unique summary identifier derived from the hashes of all transactions included in the block
Difficulty target	The difficulty target level of the consensus mechanism mathematical challenge—in Bitcoin, this level relates to the number of leading zeros that the hash of the block header needs to include
Nonce	Numerical value that solves the mathematical challenge

One can find a detailed specification of the Bitcoin block header in the online Bitcoin developer reference at https://bitcoin.org/en/developer-reference#block-headers

Public blockchains are open ledgers, and one can use online block explorers to examine blockchain transactions. Figure 2 shows sample information that BlockExplorer (www.blockexplorer.com), an open source Bitcoin block explorer, reports. The block number, also referred to as the block height, appears at the top immediately followed by the block header hash that uniquely identifies the block. The block summary reports the number of transactions, the size of the block in bytes, and block header metadata. If available, the explorer also reports the type of hardware used to create or mine the block. In this instance, a node running the Antminer brand hardware "mined" this block. Finally, the explorer notes the block reward, the amount of new Bitcoin the miner received for mining the block (in this instance, 12.5 Bitcoin).



Block #534789

BlockHash 000000000000000000129bafca659fa73cdf4179aa05cc2927fc54e83253cbb3

Summary

Number Of Transactions	180	**Difficulty**	5949437371609.53
Height	534789 (Mainchain)	**Bits**	172f4f7b
Block Reward	12.5 BTC	**Size (bytes)**	60892
Timestamp	Aug 2, 2018 12:04:49 AM	**Version**	536870912
Mined by	AntMiner	**Nonce**	1789801461
Merkle Root	c0fd06fd177833c3a4c1fe1d...	**Next Block**	534790
Previous Block	534788		

Figure 2. Sample Block Information Provided by Blockexplorer.com

Blockchain rules state that every block must be uniquely identified. The unique identifier, known as the block header hash, is software generated by nodes on the network through a process of aggregating block header metadata and hashing it twice. The block itself does not retain the identifier. Instead, nodes on the network dynamically compute the block header hash for the previous block when network nodes validate block transactions or when a mining node forms a new block and uses it as the value of the previous block identifier in the new block's block header. The genesis block, the first block in a chain, needs to hard code the value of the previous block hash (usually zero). The linkage created makes it possible to work backwards and reach the genesis block from any given block in the chain as Figure 3 shows. This linkage also makes it difficult to change data contained in a block. A change in data in one block means that nodes on the blockchain must regenerate the block header hash of all subsequent blocks in the ledger they maintain in order to retain a valid blockchain.

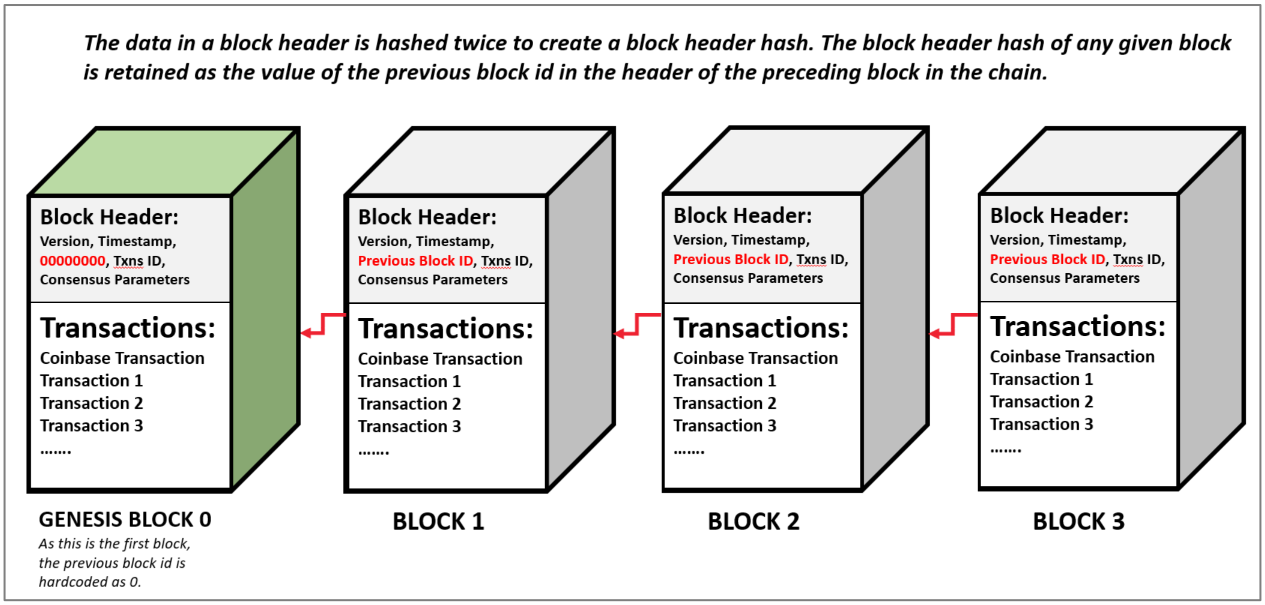
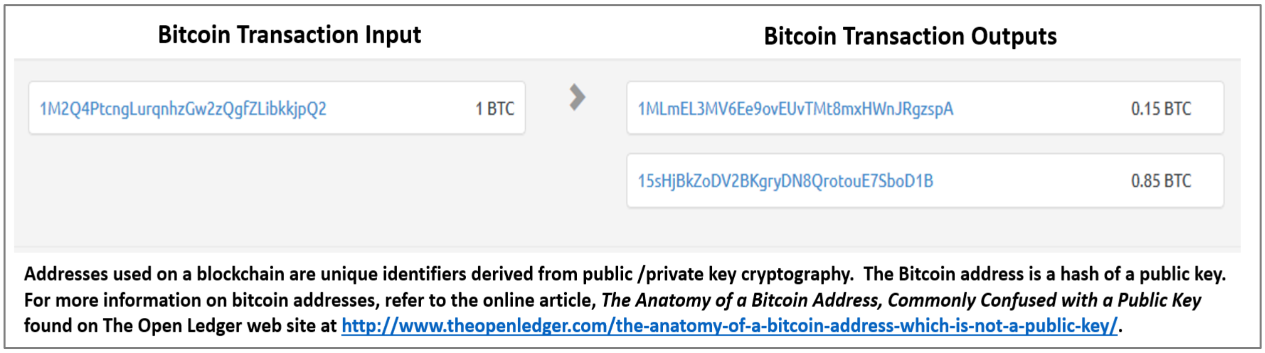

The data in a block header is hashed twice to create a block header hash. The block header hash of any given block is retained as the value of the previous block id in the header of the preceding block in the chain.

Figure 3. Example Blockchain Highlighting the Linkage between Blocks

Transactions represent value transfer between parties. On a blockchain, an address associated to an asset represents a party. Users of the blockchain compute addresses using public/private key cryptography. Transactions use public keys, or a derivative of a public key, as input and output addresses. I describe cryptography and hashing in detail in Section 4.2.

A typical transaction includes inputs that denote where assets come from and outputs that denote where assets go to (e.g., see Figure 4). This transaction has one input and two outputs. The input (see the left side in Figure 4) includes the sender's (or the Bitcoin's owner's) address and the amount the sender wants to send. The right side in Figure 4 shows the output addresses. Addresses are 256 bits, but block explorers typically show them in hexadecimal notation.


Bitcoin Transaction Input

1M2Q4PtcngLurqnhzGw2zQgfZLibkkjpQ2 1 BTC

Bitcoin Transaction Outputs

1MLmEL3MV6Ee9ovEUvTMt8mxHWnJRgzspA 0.15 BTC

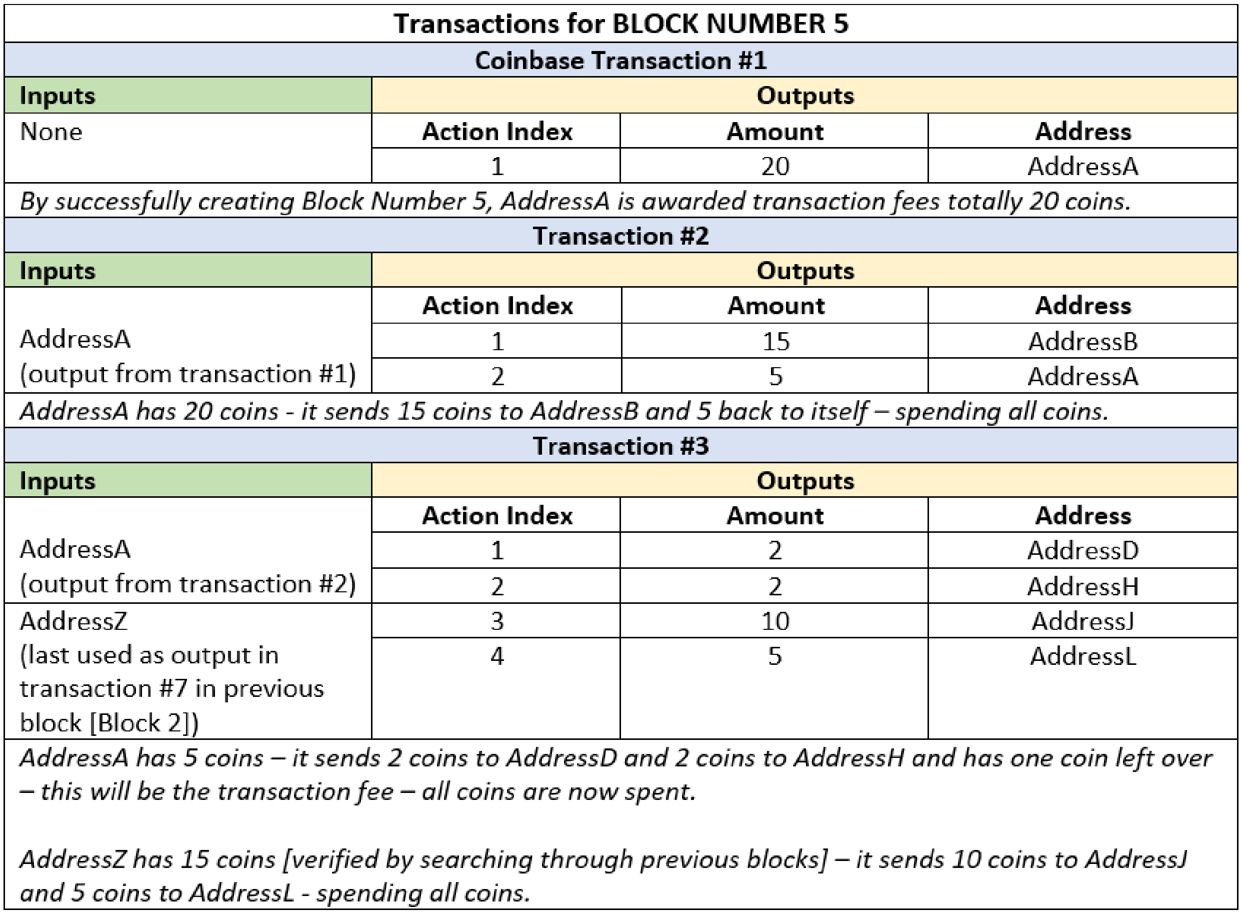
15sHjBkZoDV2BKgryDN8QrotouE7SboD1B 0.85 BTC

Addresses used on a blockchain are unique identifiers derived from public /private key cryptography. The Bitcoin address is a hash of a public key. For more information on bitcoin addresses, refer to the online article, *The Anatomy of a Bitcoin Address, Commonly Confused with a Public Key* found on The Open Ledger web site at http://www.theopenledger.com/the-anatomy-of-a-bitcoin-address-which-is-not-a-public-key/.

Figure 4. Example Inputs and Outputs in a Bitcoin Transaction

A block typically contains multiple transactions that average in the thousands. Further, every block must have at least one transaction, the coinbase transaction. The coinbase transaction has no inputs and its output pays the block's creator. The payment, which comprises transaction fees, rewards the work the creator did to validate transactions. In Bitcoin, the awarded fee comprises the aggregate value of the difference between the input and output values of every transaction in the block. Bitcoin has no fee attribute; the technology simply tallies fees when a new block is formed. In tokenized blockchains, such as cryptocurrencies, the reward may also include new coins (also the process by which new Bitcoins enter circulation).

Unlike other record-keeping systems, a blockchain does not retain account balances. The blockchain transaction process requires that all inputs be spent in their entirety. Further, the transaction process checks to insure inputs have not been previously spent. Figure 5 depicts the flow of inputs to outputs from three transactions using coins from a fictitious generic cryptocurrency. The coinbase transaction awards 20 coins to AddressA for creating the new block. AddressA wants to spend 15 of those coins. The second transaction depicts how AddressA might do so. AddressA sends 15 coins to a different address (i.e., AddressB) and then sends the leftover coins back to itself. In the third transaction, AddressA spends four of its five coins (i.e., sends two coins each to two different addresses). Bitcoin uses the remaining coin as a transaction fee. AddressA has now spent all five coins associated with it. The third transaction also demonstrates that inputs in a transaction may come from multiple addresses. AddressZ does not appear in this block. To determine the number of coins held by AddressZ, the transaction process searches previous blocks until it finds the last time AddressZ was used as an output address. In this case, this occurred in the seventh transaction in the second block (a previous block not shown in this diagram). AddressZ spends all 15 coins by sending coins to two different addresses.



Transactions for BLOCK NUMBER 5			
Coinbase Transaction #1			
Inputs	Outputs		
None	Action Index	Amount	Address
	1	20	AddressA
By successfully creating Block Number 5, AddressA is awarded transaction fees totally 20 coins.			
Transaction #2			
Inputs	Outputs		
	Action Index	Amount	Address
AddressA (output from transaction #1)	1	15	AddressB
	2	5	AddressA
AddressA has 20 coins - it sends 15 coins to AddressB and 5 back to itself – spending all coins.			
Transaction #3			
Inputs	Outputs		
	Action Index	Amount	Address
AddressA (output from transaction #2)	1	2	AddressD
	2	2	AddressH
AddressZ (last used as output in transaction #7 in previous block [Block 2])	3	10	AddressJ
	4	5	AddressL
AddressA has 5 coins – it sends 2 coins to AddressD and 2 coins to AddressH and has one coin left over – this will be the transaction fee – all coins are now spent. *AddressZ has 15 coins [verified by searching through previous blocks] – it sends 10 coins to AddressJ and 5 coins to AddressL - spending all coins.*			

Figure 5. Example Blockchain Transactions Spending All Coins

3.1 Scenario: Spending Bitcoin

Transactions vary in form and content depending on the particular blockchain technology. However, a scenario that uses a simplified version of Bitcoin as an example provides a way to conceptualize how parties spend Bitcoins in a blockchain transaction. In this scenario, Bob needs to pay Alice 100,000 satoshis (a Bitcoin contains 100,000,000 satoshis). Bob has 150,000 satoshis.

Before Bob can initiate a transaction, he needs to know his private/public key pair. He also needs to know Alice's Bitcoin address. Alice emails Bob her address as a QR code. Bob selects 5,000 satoshis as the amount he will offer as a fee to incentivize mining nodes to select and validate his transaction. Transactions are not final until they are validated, included in a block, and confirmed (see Section 4.3).

Bob can now create his transaction. If Bob's computer is a node on the network that runs the Bitcoin-core software, he can write the code needed to execute a raw-transaction (Baczuk, 2018). If Bob lacks programming skills, he will use a digital wallet. Various types of wallets exist, but most include the ability to create and store addresses (private/public key values), create and broadcast transactions, and report balances. Bitcoin (2019a) describes wallets in detail. Bob uses a wallet to create and store his private/public key pairs and to generate transactions. The input address that this transaction uses will be an address that Bob's wallet has already stored. The wallet software will generate and use a new private/public key pair and corresponding Bitcoin address as the output address to receive Bob's change. Alice's address will receive 100,000 satoshis and Bob's new address will receive 45,000 satoshis. To maintain his privacy, Bob did not return the 45,000 satoshis to the input address that this transaction used. Nakamoto (2008) recommended creating a new key pair for every transaction to make it difficult to link addresses to a common owner (p. 6). The block creator will collect the remaining 5,000 satoshis, the difference between the input (150,000 satoshis) and output (145,000 satoshis). This amount will be the output amount contained in the coinbase transaction generated when a new block is formed. Bob will spend his transaction in its entirety when the new block containing his transaction joins the chain.

4 How the Blockchain Works

Nakamoto originally devised the blockchain by integrating three technologies: peer-to-peer networks, cryptography, and distributed consensus. The blockchain as a system constitutes a network of computers, called nodes, that each retain a complete copy of the blockchain ledger (i.e., all the data in all blocks). Nodes participate in the blockchain in different ways. Full nodes retain copies of the blockchain, relay transaction information, and participate in transaction validation and confirmation. Mining nodes, also referred to as full function or forger nodes, additionally participate in creating nodes. Figure 6 provides an abstracted view about how the blockchain works. Once a node creates a transaction, it broadcasts it to the network. Other nodes on the network verify the transaction and combine it with other transactions to form a block. The node that is first to form a new block that meets the rules established by an agreed-on consensus protocol broadcasts it to the network. Peer nodes validate the block and, if it adheres to the rules, append it to the existing blockchain.

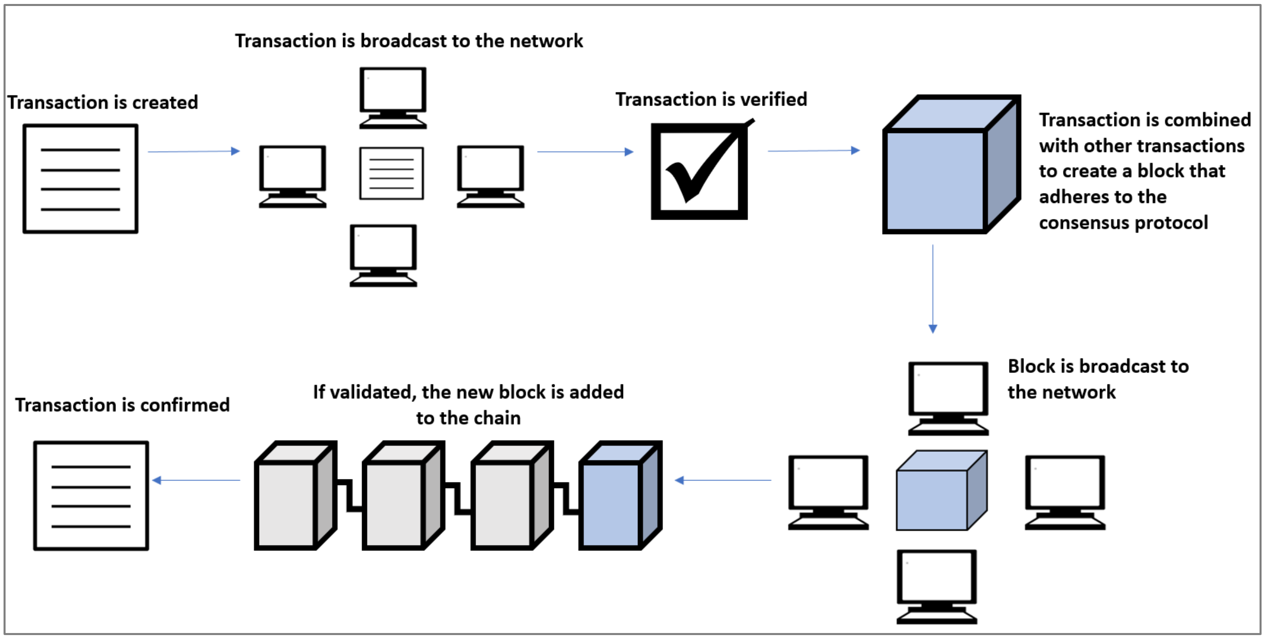

Transaction is broadcast to the network
Transaction is created
Transaction is verified
Transaction is combined with other transactions to create a block that adheres to the consensus protocol
Block is broadcast to the network
If validated, the new block is added to the chain
Transaction is confirmed

Figure 6. Overview of How a Blockchain Works

4.1 Peer-to-Peer Networking

A public blockchain operates in an unstructured peer-to-peer network in which nodes can participate voluntarily; nodes connect or disconnect at will. For example, anyone, provided they have adequate computing resources, can become a node on the Bitcoin blockchain by simply downloading and running the open source Bitcoin-core software (https://bitcoin.org/en/download). P2P networks have no central authority and no hierarchy; all nodes have equal status and can freely communicate with one another. In the blockchain, this network typography provides two protection points: 1) no single node can take control of the network and 2) no single point of failure exists. Multiple nodes store exact copies of the full blockchain.

4.2 Cryptography

Blockchain heavily uses cryptography, which includes public key cryptography, digital signatures, and cryptographic hash functions. Public key or asymmetric cryptography uses an encryption scheme that creates two mathematically related keys, a public key and a private key. Most blockchains use the Elliptic Curve Digital Signature Algorithm (ECDSA), a U.S. Government standard (National Institute of Standards and Technology, 2013). Johnson, Menezes, and Vanstone (2001) describe ECDSA in detail. A private key generates a public key, but the reverse lacks computational feasibility. As I note in Section 3, a blockchain transaction uses public keys or a derivation of them as input and output addresses. The Bitcoin blockchain uses a Bitcoin address derived from a hash of the public key.

Public keys and private keys take on special meaning in cryptocurrencies. Bitcoin provides a good example. We can think of Bitcoins as digital money with no physical counterpart. Owning a Bitcoin is exclusively affiliated with a private key; whoever knows the private key can spend the Bitcoin. Bitcoin owners need to protect their keys. If owners forget or lose their private key, they lose their Bitcoin forever. Indeed, in a well-known example, a Bitcoin owner accidentally threw away a hard drive that contained the private keys to more than 7,500 Bitcoins (Young, 2018). Bitcoin users also have responsibility over sharing their correct public Bitcoin addresses. Users lose Bitcoins that they send to a non-existent address forever, and they cannot reverse Bitcoins that they send to the wrong address. With Bitcoin, users cannot find the recipient of misdirected Bitcoin as addresses on the blockchain do not include any personally identifiable information. Consequently, Bitcoin users have come up with creative ways to manage their addresses, although most use some form of a digital wallet.

Blockchains also use digital signatures. Digital signatures use a private key to sign and verify a transaction using an associated public key. In Bitcoin, for example, a node that generates a transaction broadcasts a digital signature along with transaction data and a public key to the network. Nodes in the network use the public key to verify the signature and validate that the holder of the private key owns the Bitcoin. Nodes also use the public key to trace back through transactions to ensure that no one has previously spent the Bitcoin. Figure 7 identifies the steps in the blockchain that employ public-key cryptography. Nodes use public-key cryptography to create key pairs and sign and verify transactions to insure that only verified transactions are added to a block.

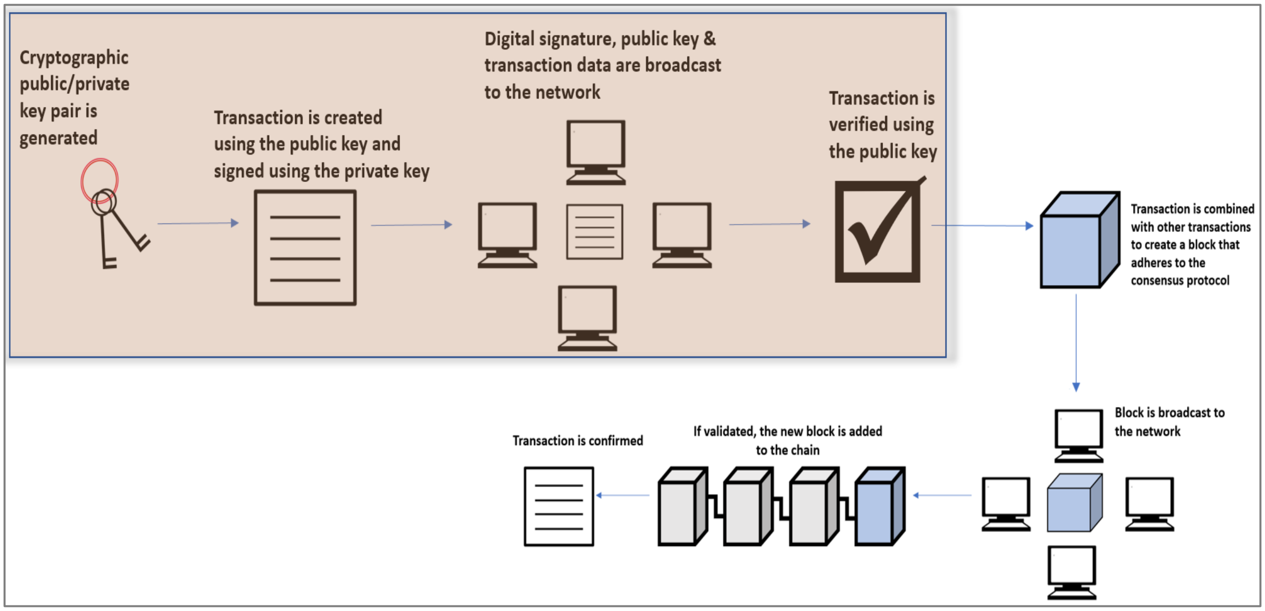
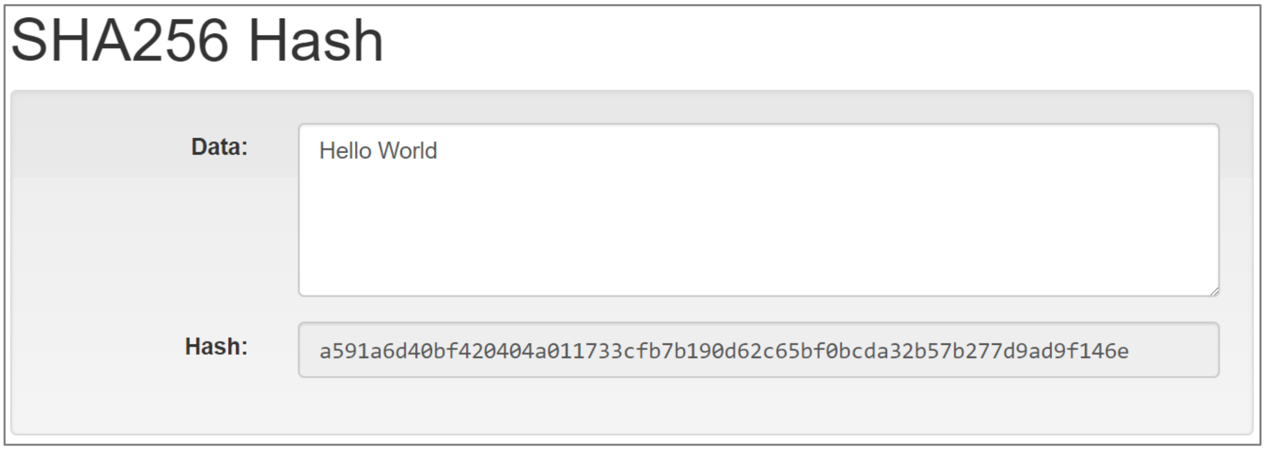

Cryptographic public/private key pair is generated
Transaction is created using the public key and signed using the private key
Digital signature, public key & transaction data are broadcast to the network
Transaction is verified using the public key
Transaction is combined with other transactions to create a block that adheres to the consensus protocol
Block is broadcast to the network
If validated, the new block is added to the chain
Transaction is confirmed

Figure 7. Public-key Cryptography in a Blockchain

Blockchain frequently uses hashing. A hash refers to a one-way function that reduces data to a fixed alphanumeric string. The same input always hashes to the same value. The National Institute of Standards and Technology (2015) has published the most commonly used hash function (i.e., SHA-256). Anders Brownworth, while teaching at MIT, created an interactive website to demonstrate how hashing works and how blockchain technology applies it (https://anders.com/blockchain/hash.html). Figure 8 demonstrates the hash of the string “Hello World”.



SHA256 Hash

Data: Hello World

Hash: a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

Figure 8. Example Hash of a String of Text

Following how Merkle trees apply hashing (Merkle, 1987), blockchains use it to generate unique identifiers for transactions. The node that forms a new block constructs a Merkle tree root by hashing paired data until a single hash remains. In the blockchain, the process includes hashing, pairing, and rehashing every transaction (see Figure 9). The Merkle root is the hash of all hashes of all transactions in a block. As I note in Section 3, the block header retains the Merkle root.

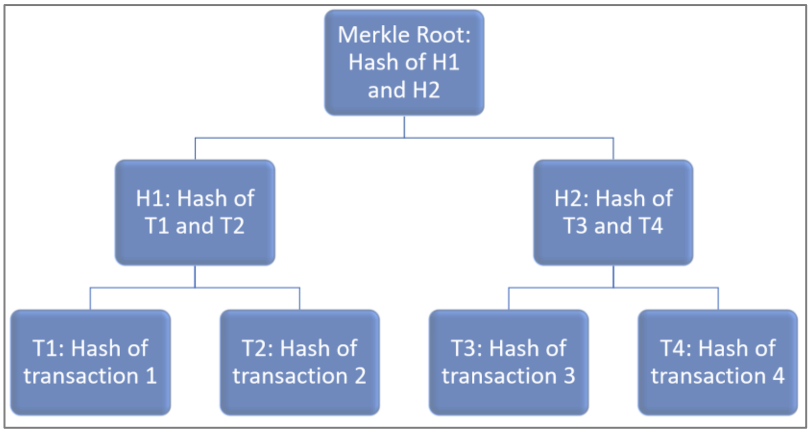

Merkle Root: Hash of H1 and H2
H1: Hash of T1 and T2
H2: Hash of T3 and T4
T1: Hash of transaction 1
T2: Hash of transaction 2
T3: Hash of transaction 3
T4: Hash of transaction 4

Figure 9. Merkle Tree Root

Blockchains use hashing in this way due to their immutability. As Figure 10 graphically depicts, one cannot easily cheat a blockchain because one cannot easily change any data in a block. Specifically, a change in data in one transaction changes the hash value of that transaction, which leads to cascading changes in the Merkle root and the value of the block header hash. This eliminates the link with the next block and breaks the chain. To reestablish the link, one would have to rehash the current block header’s value and recalculate the attribute for the previous block identifier’s value for each consecutive block in the chain. The user who creates the modified block headers must have enough control over the network to ensure nodes on the network accept the modified blocks before a mining node adds additional blocks to the chain. Consequently, users would have little chance to achieve success; other nodes in the blockchain will almost certainly reject such changes.

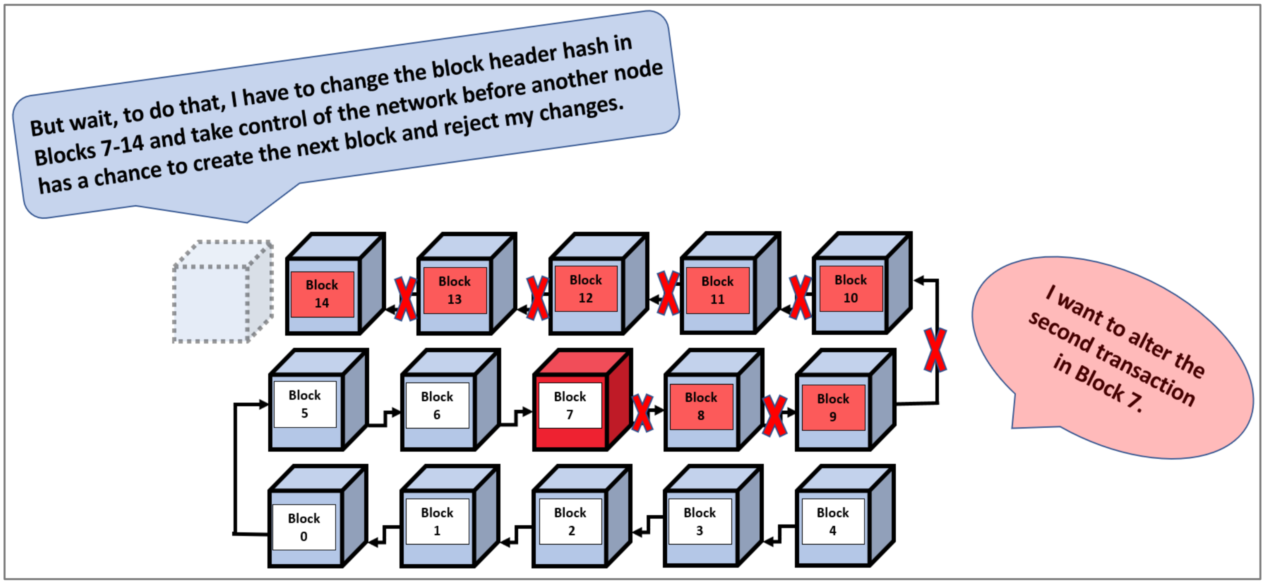

But wait, to do that, I have to change the block header hash in Blocks 7-14 and take control of the network before another node has a chance to create the next block and reject my changes.
I want to alter the second transaction in Block 7.
Block 14
Block 13
Block 12
Block 11
Block 10
Block 5
Block 6
Block 7
Block 8
Block 9
Block 0
Block 1
Block 2
Block 3
Block 4

Figure 10. Why it is Difficult to Change Data in a Blockchain

4.3 Distributed Consensus

One fundamental challenge in a distributed computing environment involves finding a way to reach agreement among remote processes that must operate together to achieve a common outcome (Fischer, Lynch, & Paterson, 1985). To describe this challenge, researchers have often used the Byzantine General’s Problem as an analogy (Lamport, Shostak & Pease, 1982). In this scenario, a general who commands several divisions must effectively communicate a plan of attack to various lieutenants. If more than one-third of the lieutenants are dishonest, the general will fail. On the other hand, if loyal lieutenants come to consensus, they will be able to thwart the efforts of a small number of traitors and the general will succeed. The challenge in a blockchain involves ensuring that all nodes act on the same data and that a bad node cannot transmit and post false transaction data. The nodes need a way to reach consensus to ensure that the addition of newly created blocks results in continuing a single ledger. In the blockchain, consensus refers to a set of computer science algorithms that define the processes that nodes in a distributed system use to achieve agreement on a single data value (Fischer, 1983). The most common include proof of work (PoW) and proof of stake (PoS).

4.3.1 Proof-of-work Consensus

In his white paper, Nakamoto (2008) proposed the proof-of-work (PoW) consensus mechanism. PoW has since become synonymous with the term mining. Describing PoW in the Bitcoin blockchain represents a good way to demonstrate consensus and connect it to the mining process. In Bitcoin, PoW addresses many issues, some particularly relevant to cryptocurrencies. Consensus had to provide a way to resolve the Byzantine General’s problem, incentivize nodes to participate in verifying transactions, and provide a way to distribute Bitcoins into circulation (Nakamoto, 2008). Nakamoto proposed that one could achieve integrity in the consensus process by instituting a system where the expense to defraud (the cost of computing hardware and electricity) would exceed the cost to earn a reward (the award of Bitcoin). One achieves PoW by finding the solution to a mathematical puzzle that only brute force can solve. In the Bitcoin blockchain, the solution involves finding a nonce, a number that results in a hash of a block header that contains a specified number of leading zeros. The Bitcoin protocol sets the number of leading zeros as the target difficulty. The more leading zeros, the more computing power one needs to find the nonce. Bitcoin protocol rules specify that mining nodes adjust the target difficulty every 2016 blocks (about every two weeks) by increasing or decreasing the required number of leading zeros to meet an average time of 10 minutes for someone to mine a successful block. Mining activity simply iterates different values for a nonce until the node finds a valid hash. The node that first finds the nonce claims the block reward of transaction fees and “newly minted” Bitcoins. (The Anders Brownworth website (https://anders.com/blockchain/block.html) provides an interactive activity that allows users to experiment with creating a nonce.) Once a mining node finds a nonce, the node adds it the block header and broadcasts the block to the network. Other nodes in the network verify block transactions and validate the nonce's legitimacy. Consensus arises when those nodes append the new block to the chain and when mining nodes use the newly accepted block's block header hash as the value of the identifier of the previous block hash in the header of the block they are now working to create. At this point, the network also confirms a transaction. A transaction is reconfirmed each time a mining node adds a subsequent block to the blockchain. Figure 11 displays the image of how a blockchain works with annotation specific to the Bitcoin mining process that Nakamoto (2008) outlined.

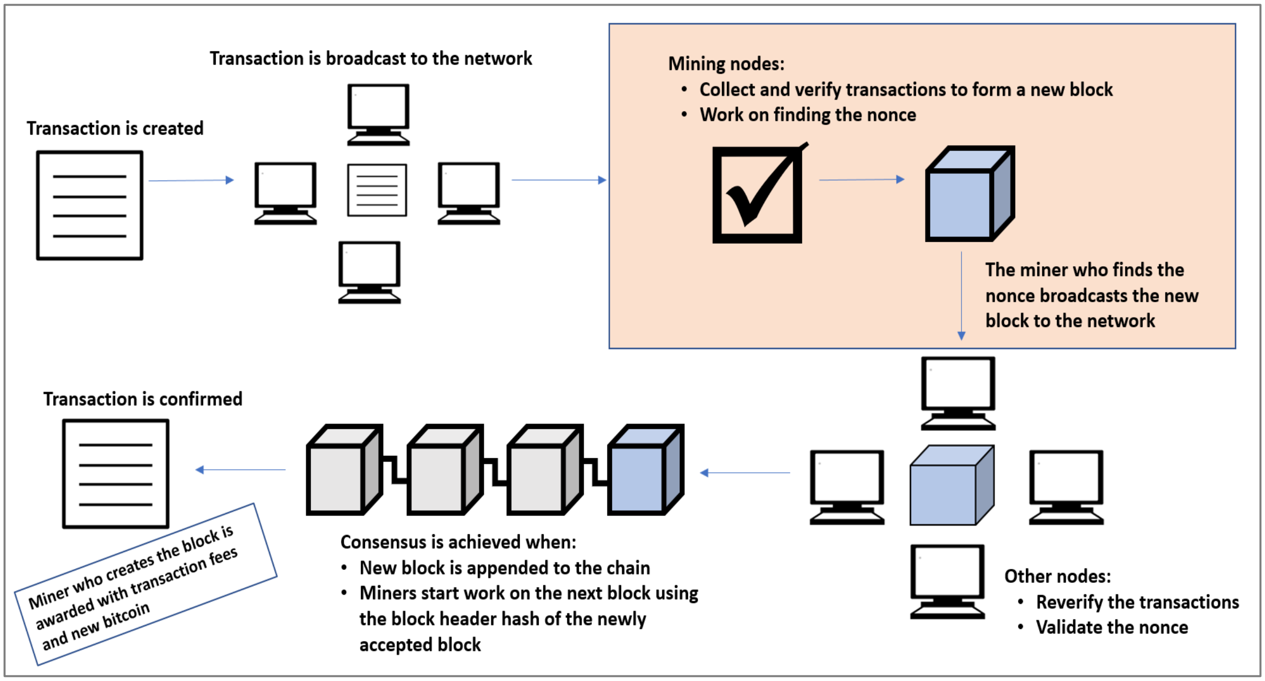

Transaction is broadcast to the network
Transaction is created
Mining nodes:
• Collect and verify transactions to form a new block
• Work on finding the nonce
The miner who finds the nonce broadcasts the new block to the network
Transaction is confirmed
Miner who creates the block is awarded with transaction fees and new bitcoin
Consensus is achieved when:
• New block is appended to the chain
• Miners start work on the next block using the block header hash of the newly accepted block
Other nodes:
• Reverify the transactions
• Validate the nonce

Figure 11. Bitcoin Blockchain Mining Process

As an aside, the Bitcoin currency has interesting blockchain rules. As I mention in Section 4.3.1, through PoW, Bitcoins enter circulation when they are awarded to the mining node that creates a new validated block. At genesis, Nakamoto set this award to 50 Bitcoins for each new block. Bitcoin, however, has a fixed supply. Nakamoto intentionally stipulated as much since a fixed monetary supply does not experience inflation. Consequently, the number of Bitcoins awarded is reduced over time; the number halves every 210,000 blocks (about every four years). The award of new Bitcoins ceases when the number of Bitcoin reaches 21 million, which will occur in approximately 2140. From this time forward, the reward for mining will revert to only transaction fees**.**

Scenario: Bitcoin blockchain workflow: this scenario describes the Bitcoin workflow from transaction creation to transaction finality based on block confirmation. Bob needs to pay Alice 100,000 satoshis; Bob has 150,000 satoshis and chooses a transaction fee of 5,000 satoshis.

Bob uses his digital wallet to generate a transaction to transfer 100,000 satoshis to Alice and broadcast it to the network. Nodes on the network retrieve the transaction and add it to a "mempool", a queue of pending transactions. Miners set parameters—such as preferred transaction size and fee amount—for prioritizing transactions. When selected from the mempool, mining nodes validate or reject Bob's transaction. The validation process assures the transaction meets blockchain protocol rules, which includes verifying the digital signature, that the total input value exceeds than the total output value, and that no one has previously spent the input addresses. Bitcoin nodes maintain an address database with unspent transaction outputs (UTXO) that they update as they confirm transactions. Only addresses in the UTXO are considered unspent.

A mining node validates Bob's transaction and adds it to the forming block. The mining node works to win the block by finding the nonce. The first node to find the nonce adds the coinbase transaction and block header metadata to the new block and broadcasts the new block to the network. Other nodes on the network retrieve the block, verify the transactions, and validate the nonce. If a node accepts the block, it appends it to the blockchain and publishes it to the network. At this point, the network has confirmed the block containing Bob's transaction. However, users should wait for at least six confirmations (Comben, 2018) to make certain nodes on the network have not reversed a transaction (“Irreversible Transactions”, 2018). Thus, Bob and Alice should wait until other nodes add five more blocks to the chain (i.e., six confirmations) before they consider their transaction final. Multiple confirmations ensure that network nodes did not append the block to an unintended fork in the chain and also avert double-spend, the risk that users spend a Bitcoin more than once. Each block added to the chain reconfirms the validity of the transactions contained in previous blocks.

4.3.2 Other Forms of Consensus: Proof of Stake

PoW consensus has several drawbacks, such as its vulnerability to the 51 percent attack whereby a single entity gains control over the majority of the mining power. This entity can now take control of the blockchain ledger, which allows the entity to alter past transactions and reject future transactions. PoW mining also consumes many resources (mostly in terms of power consumption). One study projected the annual energy consumption rate for mining Bitcoins when one Bitcoin costs US$8000 to be 67 TwH (terawatt hours), equivalent to approximately 20 percent of Britain's total energy use (DeVires, 2018). The excessive costs associated with mining have been attributed to a reduction in the number of Bitcoin miners and represent one reason other consensus mechanisms have started to gain in popularity.

Many have touted proof-of-stake (PoS) consensus mechanisms as a possible alternative to PoW consensus mechanisms. In PoS consensus, protocol rules are used to select block creators based on predetermined criteria (Rosic, 2017). Blockchain developers have proposed different forms of PoS, but they all basically require some type of investment in a pay-to-play scheme that sets the rules for how blockchain nodes choose the creator of the next block. For example, in an ownership-based PoS, ownership percent determines the chance a blockchain node will be selected to create the next block. Other schemes use criteria such as ownership age, available hard drive space, or willingness to use coins that will be “burned” or taken out of circulation. The Intel Corporation developed Proof of Elasped Time (POET) that uses a random lottery scheme to establish wait time before a node can participate in block creation, and others have proposed implementing directed acyclic graph (DAG) data structures into consensus mechanisms. Ripple, a global payment system and the second largest cryptocurrency, developed its own version of a proof-of-consensus mechanism based on the Byzantine agreement protocol (Chase & MacBrough, 2018). As blockchain technology has evolved, new forms of consensus have also emerged; various parties have proposed at least 30 consensus mechanisms (Vasa, 2018). While consensus makes up a core component of a blockchain, each blockchain implements its own version of a consensus mechanism.

4.3.3 Blockchain Fork

Every node in a blockchain network works independently, which makes it is possible for any node on the network to create and simultaneously broadcast multiple blocks to the network. If different nodes accept and append different blocks, a fork in the chain occurs and more than one version of a blockchain exists (as Figure 12 depicts). Consensus ensures that the majority of nodes on the network reject forks. Unintended or accidental forks occur when mining nodes create and broadcast valid blocks to the network at the same time, which results in two versions of the chain. Bitcoin always accepts/recognizes the longest chain, which ensures that the majority of nodes on the network will eventually reject and eliminate unintended forked chains. Unintended forked chains occur more commonly in open participation blockchains that employ PoW consensus, less commonly in blockchains that limit participation in block validation, and not at all in PoS systems that select a single block creator.

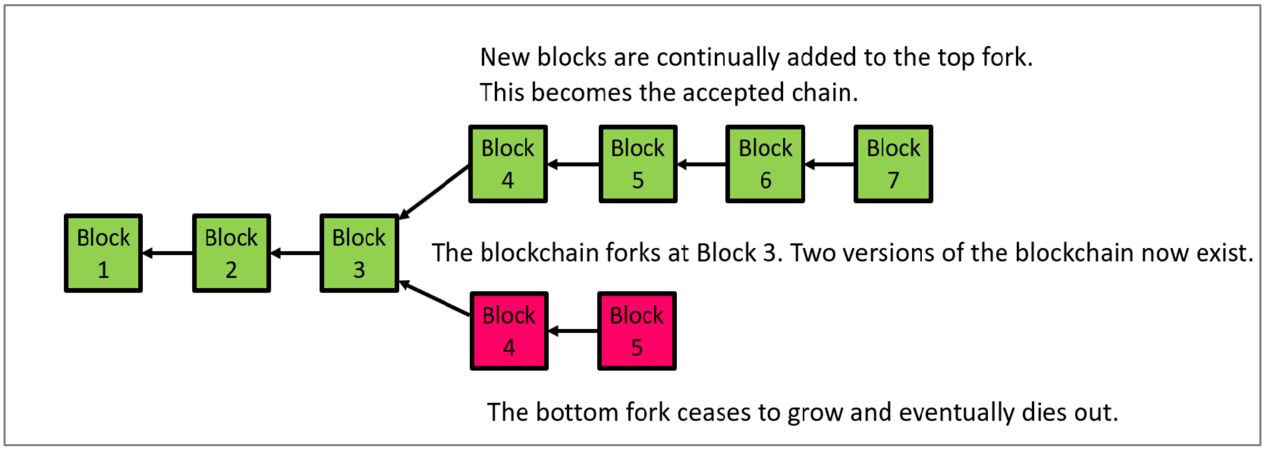

New blocks are continually added to the top fork.
This becomes the accepted chain.
Block 4
Block 5
Block 6
Block 7
Block 1
Block 2
Block 3
The blockchain forks at Block 3. Two versions of the blockchain now exist.
Block 4
Block 5
The bottom fork ceases to grow and eventually dies out.

Figure 12. Forks in a Blockchain

Forks occur for other reasons as well (Asolo, 2018). A soft fork happens when developers make agreed-on software updates to the blockchain core software. In the lag time before all nodes implement the new rules, two sets of blocks might emerge: blocks that adhere to the old rules and blocks that adhere to the new. This temporary situation resolves when all nodes complete the software upgrade. Hard forks, on the other hand, arise intentionally. Hard forks occur when disagreement among software developers results in two separate versions of the blockchain core software and various nodes on the network opt to implement the different versions. At this point, the chain splits in two with one fork following the old rules and the other following the new rules. Each fork continues as its own independent chain, but both retain a common history up to the split. The cryptocurrencies Bitcoin Cash and Bitcoin Gold exemplify hard forks to the Bitcoin blockchain.

5 Types of Blockchains: Public versus Private

Nakamoto (2008) defined the original blockchain to be open, public, and permissionless. The Bitcoin blockchain allows anyone to establish a node on the network, participate in consensus and mining, and view transactions in the blockchain ledger. However, as parties have proposed various blockchain applications, so too have they proposed restrictions to blockchain participation. Juxtaposed to the open blockchain lies the closed, private, permissioned blockchain that people can participate in by invitation only. While more efficient, they are also more vulnerable to manipulation. Other blockchains adopt a hybrid model that allows anyone to establish a node on the network or view transactions but restrict further participation, such as block creation or block validation. Many Hyperledger projects fall into this category. Federated or consortium blockchains support a specific group or function. In these private blockchains, a select group of nodes control consensus (e.g., blockchains that banks form to support financial transactions between them).

Figure 13 depicts the different types of blockchains on a continuum. The classification system is not discrete; other combinations can exist. For example, one could implement a permissioned blockchain in either a public or private network. Some argue that movement along the continuum further from the public blockchain simply describes a centrally controlled system that existing database technologies typically support (Narayanan, 2015). Others argue that a blockchain's openness does not define its applicability or usefulness (Thompson, 2017). Rationales for implementing a permissioned blockchain include the need to manage transaction' digital identity (e.g., retaining patient privacy when sharing healthcare data) or to speed up transaction throughput. However, all blockchains, public and private, rely on similar principles with the sole distinction between them relating to "who is allowed to participate in the network, execute the consensus protocol, and maintain the shared ledger" (Jayachandran, 2017).

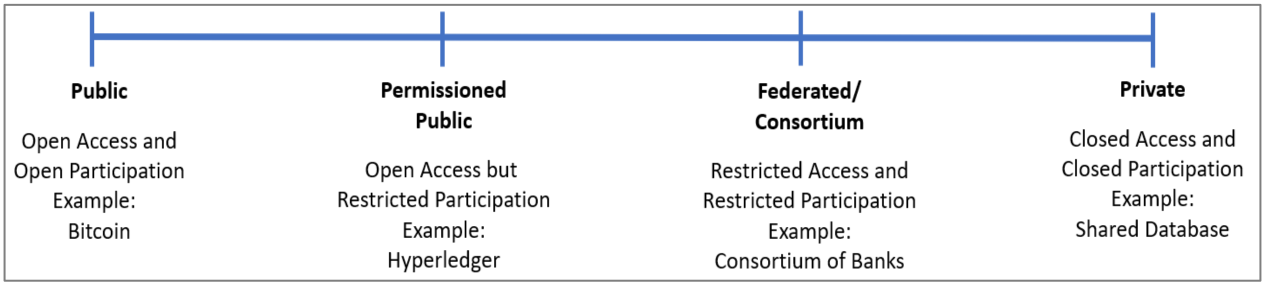


Figure 13. Continuum of Blockchain Implementations

5.1 Distributed Ledger Technology

Distributed ledger technology (DLT) refers to “a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time” (TechTarget, 2017). Distributed database technology has been around for decades, but interest in distributed ledgers did not proliferate until blockchain technology appeared. In 2015, under The Linux Foundation’s guardianship, various companies formed the Hyperledger project. Hyperledger membership comprises more than 230 companies from various industries with major contributors including IBM and Intel. The project represents an open source collaborative effort to advance blockchain technology through developing modular blockchain solutions (The Linux Foundation, 2018).

Blockchain researchers often use the terms DLT and blockchain interchangeably, but, while all blockchains are distributed ledgers, not all distributed ledgers are blockchains (Au & Power, 2018, p. 45). For example, some distributed ledger systems do not use a blockchain as their data structure, and private distributed ledger systems do not need a complex consensus mechanism. The challenge going forward does not involve clarifying the terminology but rather interjecting them where they can best address the problem at hand.

6 Blockchain Challenges

We have learned much about blockchain possibilities and challenges since Nakamoto operationalized the Bitcoin blockchain in 2009, lessons that bound and inform how the technology will evolve. Table 3 lists themes related to the Bitcoin blockchain that have frequently appeared in the trade press and news media and strategies to address them. While this analysis focuses on Bitcoin, issues examined apply to other blockchains as well. Ultimately, we need to address these issues to more deeply diffuse blockchain technologies.

Table 3. Lessons Learned from the Bitcoin Blockchain

Theme	Issue
Usability	Blockchain technology is complex and requires deep technical knowledge to understand. On the other hand, we can and must simplify how one interacts with it as a prerequisite to widespread adoption. The ability to interact with a blockchain (i.e., buy, sell, and spend Bitcoin) needs to be accessible to all types of users regardless of their technical prowess. **Resolution strategies:** a blockchain ecosystem must include applications that simplify the user experience similar to how graphical browsers abstract HTTP’s complexities for Web users. For example, digital wallets provide a user interface for cryptocurrency blockchains, and many have begun work to improve wallet design’s user interface and user experience.
Scalability: Size of the blockchain	The Bitcoin blockchain has grown to more than 205GB in size (Blockchain, 2019). As the size of a blockchain increases, it becomes more expensive for nodes to participate in the network. Decentralization and, subsequently, the blockchain’s integrity depends on volunteer nodes to validate transactions and create blocks. **Resolution strategies***:* one approach to addressing blockchain size includes creating partial or light weight nodes; another approach proposes splitting the chain into multiple subchains or peer-level side-chains.

Table 3. Lessons Learned from the Bitcoin Blockchain

Scalability: Block size, transaction throughput and block confirmation time	Bitcoin blockchain protocols restrict block size to one megabyte and set the average time to mine a block to 10 minutes, which limits transaction throughput to an average of 4.6 transactions per second and transaction confirmation to 10 minutes (one hour to attain the recommended six confirmations). Visa, the well-known global payment company, reports transaction throughput as 1700 transactions per second and transaction confirmation in seconds (Li, 2019). The blockchain transaction bottleneck prevents Bitcoin from becoming competitive as an alternative online-payment method. **Resolution strategies**: solutions to this complex issue, such as increasing the block size or decreasing block creation time, have yielded limited success. Other proposals include off-chain channels, sharding techniques, and adding a transaction processing layer to the blockchain (Kasireddy, 2017).
Mining	To encourage participation in the blockchain, Bitcoin instituted an award incentive (i.e., new Bitcoins and transaction fees) to nodes who first “mine” a block. Nakamoto designed mining to consume many resources so that the cost to defraud the system would exceed the cost to earn the reward. As Bitcoin's price increases, interest in mining soars. Increased mining activity has consequences: an unsustainable growth in energy consumption (Digiconomist, 2019), which results in increasing costs and ultimately reduces interest in mining. **Resolution strategies**: a notable solution has included alternative consensus mechanisms, such as proof of stake, that replace “mining” with selecting block creators based on predetermined criteria.
Transaction Fees	Miners find transactions with higher fees more attractive. At the height of the Bitcoin frenzy when users made many transactions, fees rose quickly. Stories abound of transaction fees that exceeded transaction value. The volatility in transaction fees impacts whether people adopt Bitcoin as a viable digital payment option. **Resolution strategies:** fees directly relate to transaction throughput; increasing throughput decreases fees. Two approaches have had promising results. The Segregated Witness (SegWit) protocol increases block size primarily by removing signature data from a transaction (Lombrozo, Lau, & Wuille, 2015). The Lightning Network (LN), an off-chain payment channel, allows two parties to transact with each other multiple times in between two blockchain transactions, an initial funding transaction and a final closing transaction. LN is especially useful for micro or small payments that do not justify high transaction fees (Poon & Dryja, 2016).
Security	The blockchain supports a secure and immutable ledger. However, if a miner assumed majority control of the mining computing power or flooded the network with fraudulent data, the miner would compromise the ledger’s integrity (Orcutt, 2018b). The greatest threat to security, however, resides with third-party applications and currency exchange websites where hackers have gained access to private keys and absconded with large amounts of Bitcoin. **Resolution strategies**: people find vulnerabilities and flaws in any technology no matter how secure (Orcutt, 2018b). Suggestions to reduce vulnerability in the blockchain include implementing controls by switching to PoS consensus mechanisms or permissioned blockchains.
Governance	Bitcoin is an open source software project (Bitcoin, 2019b). The user community recommends software revisions, a group of volunteer software developers manage software developments, and implementation occurs through acceptance from stakeholders (Light, 2016). Disagreement that results in different versions of the software split the chain (i.e., hard fork) into separate chains that operate independently. For Bitcoin, such splits create competing cryptocurrencies. **Resolution strategies**: to achieve stability in the software-development process, recommendations call for stakeholders to establish metrics to assess software changes’ necessity and thresholds to determine when changes should be made (Trump, Well, Trump, & Linkov, 2018).

Table 3. Lessons Learned from the Bitcoin Blockchain

Sustainable Interest	Blockchain technologies support cryptocurrencies, yet many use the terms interchangeably. As such, many people project volatility in a cryptocurrency's currency to volatility in the technology. However, acceptance of cryptocurrencies as stable and viable alternatives to fiat currencies represents the primary issue with cryptocurrencies, not the technology (Adkisson, 2018). That is, interest in blockchain technology may rise and fall with the hype surrounding individual cryptocurrencies. **Resolution strategies***:* investment in blockchain projects has not subsided, and organizations across many industries continue to propose, test, and implement blockchain applications and related Hyperledger technology.

7 Blockchain Use Cases and Applications

Nakamoto (2008) originally developed blockchain technology to support digital currency. Currency, however, represents just one type of asset. One can easily extend blockchain platforms to any asset that one can digitize, represent with a digital identity, or tokenize. Tokenization refers to a process in which a percentage of rights is associated to an asset. Blockchain technology as a record system has many benefits and applications.

Smart contracts, such as the ones that Ethereum supports (https://www.ethereum.org/), represent another well-known way to use a blockchain. Smart contracts, however, differ from legal contracts; rather, they comprise if-then statements that run in self-executing software code (Orcutt, 2018a). Nodes on a blockchain implement a smart contract as a software program, which allows blockchain users to associate additional information with a transaction. Contract authors write the code that stipulates the contract's rules and trigger the code to automatically execute according to specified conditions. As smart contract code resides on the blockchain, one cannot alter it, which increases the reliability that a contract's parties will carry out its terms as set forth and, ultimately, eliminates the need for third-party dispute resolution or intermediation. Some even speculate smart contracts will replace the need for lawyers in business transactions (Sonderegger, 2018).

Blockchain enthusiasts have projected blockchain technology to impact all industries. Reports of use case scenarios and example pilot projects abound. For example, Business Insider has highlighted potential applications for finance, business, government, and technology (Meola, 2017), and Forbes has identified more than 30 initiatives already underway that span industries such as entertainment, retail, healthcare, and logistics (Marr, 2018). Blockchain enthusiasts believe that blockchain has limitless uses and endless possibilities (Smith, 2017). Table 4 includes some proposed blockchain applications from various industries.

Table 4. Blockchain Use Case Examples from Various Industries

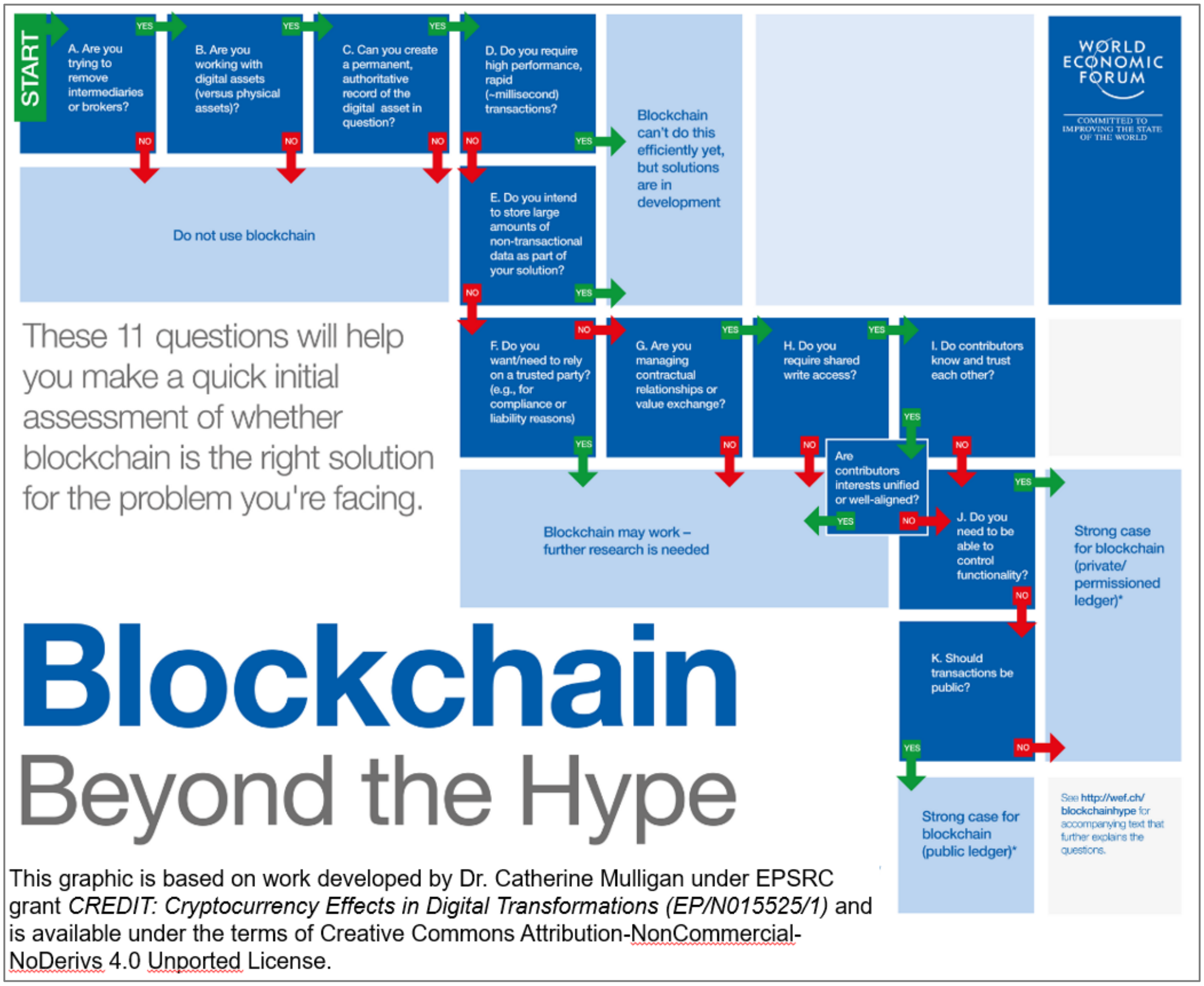
Industry	Sample use case
Energy	System that tracks the buying and selling of energy decentralizing the energy market by helping small suppliers sell energy, which includes individuals who want to sell energy from their solar panels
Entertainment	System that tracks ticket sales to thwart ticket fraud
Exotic cars	System that supports fractional ownership of collector cars
Finance	System that supports global payments
Finance	System that supports peer-to-peer transactions (which includes money transfers)
Government	Land-registry system that records property transactions and makes ownership verifiability open to the public
Healthcare	System that allows healthcare professionals to store and retrieve electronic patient records for telemedicine consultations
Identify management	System that verifies someone's identity via biometric information stored on a blockchain
Insurance	System that supports proof-of-insurance verification in real time

Table 4. Blockchain Use Case Examples from Various Industries

Internet of things	Service that provides a secure way for devices to register and validate themselves on a network in order to maintain integrity in device-to-device communication
Money	Platform that supports cryptocurrency
Non-profit	System that allows donors to see how recipients spend their contributions
Real estate	System that connects buyers and sellers with real estate agents who accept lower commissions
Retail	System that tokenizes loyalty reward programs, which makes it easy for consumers to swap earned points
Social engagement	Matchmaking service that rewards “matchmakers” for connecting people in various venues
Supply chain	System that tracks food from the farm to the table, which allows consumers to see exactly where their food comes from
Voting	System that allows voters to verify their votes were recorded

As with any technology, one should not use blockchain technology in every situation due to its complexity and need for resources. Blockchain researchers have proposed several models that prescribe ways to assess whether blockchain technology would help suit a particular situation. The FITS model evaluates suitability on four factors: propensity for fraudulent transactions, intermediary use, throughput requirements, and data stability (McCullagh, 2017). The blockchain better fits business environments with a high fraud risk and where third-party intermediaries provide low value. Throughput constitutes another major consideration since blockchain technology cannot easily attain a high throughput rate. Finally, blockchain best suits stable data or data that stays the same over time, such as property ownership. The FITS model represents a first step in determining blockchain viability.

The World Economic Forum has produced perhaps the most comprehensive blockchain-adoption assessment framework (Mulligan, Scott, Warren, & Rangaswami, 2018). Specifically, the framework asks 11 questions as a decision tree (see Figure 14). Like the FITS model, the framework evaluates areas such as trust, intermediaries, throughput, and data stability. The assessment purports that a blockchain best suits assets that one can represent in a digital format and whose form does not change. For example, a blockchain works well for tracking wheat’s movement between buyers and sellers but not for tracking wheat’s transition to flour or flour’s transition to bread (Mulligan et al., 2018). The World Economic Forum ascribes a blockchain’s business value to its creating a trusted solution for managing contractual relationships and value transfers. In summation, blockchain offers a viable solution in situations where trust poses an issue, intermediaries participate in the process, and parties need a permanent record.


START
A. Are you trying to remove intermediaries or brokers?
B. Are you working with digital assets (versus physical assets)?
C. Can you create a permanent, authoritative record of the digital asset in question?
D. Do you require high performance, rapid (~millisecond) transactions?
YES
NO
Do not use blockchain
Blockchain can't do this efficiently yet, but solutions are in development
E. Do you intend to store large amounts of non-transactional data as part of your solution?
F. Do you want/need to rely on a trusted party? (e.g., for compliance or liability reasons)
G. Are you managing contractual relationships or value exchange?
H. Do you require shared write access?
I. Do contributors know and trust each other?
Are contributors interests unified or well-aligned?
J. Do you need to be able to control functionality?
K. Should transactions be public?
Blockchain may work – further research is needed
Strong case for blockchain (private/ permissioned ledger)*
Strong case for blockchain (public ledger)*
See http://wef.ch/ blockchainhype for accompanying text that further explains the questions.
WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD
These 11 questions will help you make a quick initial assessment of whether blockchain is the right solution for the problem you're facing.
Blockchain
Beyond the Hype

This graphic is based on work developed by Dr. Catherine Mulligan under EPSRC grant *CREDIT: Cryptocurrency Effects in Digital Transformations (EP/N015525/1)* and is available under the terms of Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Unported License.

Figure 14. World Economic Forum's Blockchain Assessment Flowchart (Mulligan et al., 2018)

8 Blockchain Adoption

Researchers have studied innovation diffusion for decades. In particular, to describe technology adoption, they have widely used the theoretical framework that Rogers (2003) developed. Rogers proposed that the diffusion process occurs over time and follows an S-curve pattern. The adoption rate begins with a period of slow gradual growth followed by a period of dramatic rapid growth that eventually stabilizes and finally declines. Rogers classified adopters into four groups: innovators, early adopters, early majority, late majority, and laggards. Innovators, the first to experiment with a technology, take risks and willingly accept uncertainty about the future. Innovators tend to possess a high technical skill. Early adopters recognize a technology's potential and assume a leadership role in advocating for its acceptance. The early majority, risk-averse individuals who opt for adoption as an innovation attracts more followers, want to be among the first rather than the last group of adopters. The late majority also refers to risk-averse individuals, but, while they remain skeptical, they feel pressure to adopt. Laggards want evidence that an innovation works before deciding to adopt. Using this scale, according to Stratopoulos and Wang (2018), blockchain diffusion appears to reside with early adopters, which the high number of news articles, firm disclosures, book titles, and business publications reporting blockchain initiatives and pilot projects evidences. Gartner has concurred in noting that much activity has occurred because CEOs want to garner recognition as innovation leaders (Kandaswamy & Furlonger, 2018). Figure 15 depicts the innovation diffusion S-curve and blockchain adoption's potential current state.

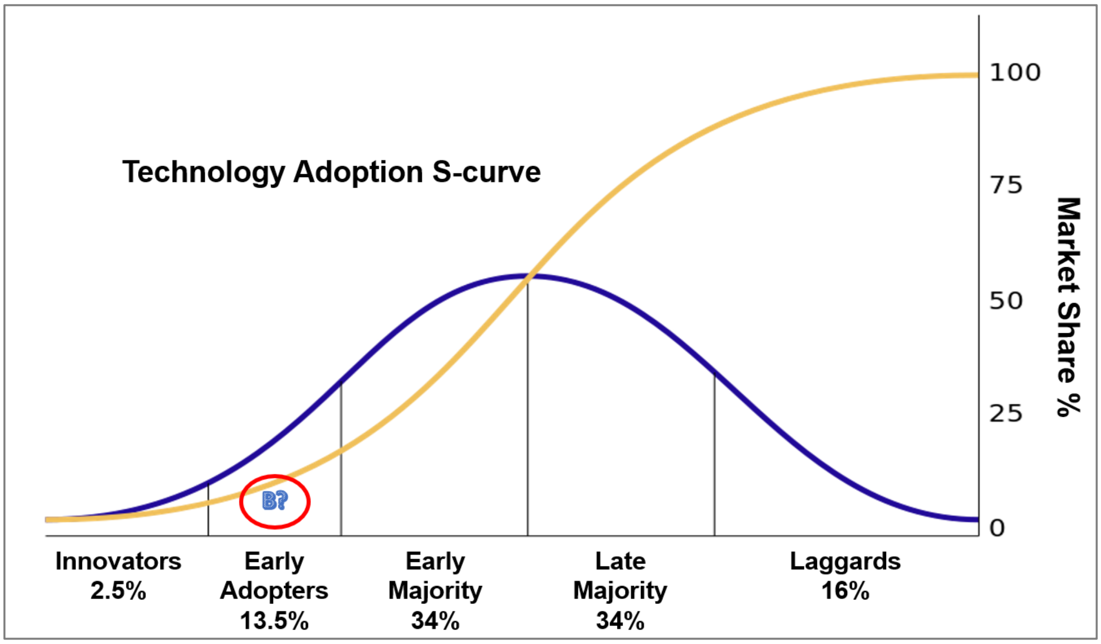


Figure 15. Diffusion of Innovation S-Curve Estimating Blockchain Adoption (Adapted from Rogers, 2003)

Widespread blockchain adoption will take years, though experimentation has begun in earnest and developers have created thousands of blockchain projects. Deloitte has reported on a study in which the company found that the open source GitHub repository received 86,000 project submissions between 2009 and mid-2017 (Trujillo, Fronthart, & Srinivas, 2017). However, the company also noted that, by the end of the study, only eight percent of the projects remained active—not an unusual pattern. Gartner has described the current period as one of irrational exuberance where enthusiasm drives interest, but adoption remains light (Kandaswamy & Furlonger, 2018). We saw a similar situation with TCP/IP and the Internet. TCP/IP revolutionized data transmission and made the Internet possible. However, we realized the Internet's transformative power only after 30 years of trial applications to novel use cases (Iansiti & Lakhani, 2017). Gartner has predicted a similar trajectory for blockchain technology (Trujillo et al., 2017).

Iansiti and Lakhani (2017) have proposed a framework for tracking blockchain adoption that relies on how novelty and complexity affect how a foundational technology and its associated use cases evolve. The more novel a technology, the more effort one needs to understand its application and usefulness. Consequently, new technologies typically focus on a single-purposed application. As others begin to see value in the technology, they envision new uses, and the technology's impact grows. However, at the same time, the complexity required to coordinate the growing diversity of players in the technology ecosystem increases. The need to resolve that complexity gives rise to novel transformative applications that can change "the very nature of economic, social, and political systems" (Iansiti & Lakhani, 2017, p. 10). The blockchain no longer exclusively supports Bitcoin; rather, a highly diverse and complex blockchain ecosystem has emerged. Sustainable transformative applications may be far away (p. 10), but blockchain will impact most businesses. The only question that remains concerns when the impact will manifest (Iansiti & Lakhani, 2017, p. 11).

9 Conclusion

Conceived as a transparent, self-governing, democratized digital currency to support electronic transaction processing (Nakamoto, 2008), the blockchain represents disruptive technological innovation. The Bitcoin blockchain addresses problems that electronic money schemes encounter via a decentralized trust system that adopts peer-to-peer networking, cryptography, and distributed consensus. Blockchain retains an immutable and traceable distributed and identical transaction record, which enables new forms of value transfer that do not require an intermediary or central authority (Kandaswamy & Furlonger, 2018). Subsequent efforts that generalized blockchain technology to support value transfer for all types of assets sparked many people's imagination, and some have proclaimed it a technological breakthrough that promises to revolutionize business and redefine economies (Iansiti & Lakhani, 2017).

The hype is real, but blockchain is not a panacea. Blockchain entered the technology realm as a cryptocurrency platform, which propelled it into the mainstream. However, some have expressed concern that overpromotion of this untested, underdeveloped platform could undermine its long-term potential (Mulligan et al., 2018). Addressing myriad issues that plague asset transfers over the Internet, blockchain has its challenges, most notably scalability, latency, and integration. Sustainability will depend on how we resolve these challenges, yet it will take time, effort, resources, commitment, and perseverance before we successful deploy blockchain technology.

Any conclusion made about blockchain would be incomplete without reference to Bitcoin. The Bitcoin craze increased the public's awareness of the technology, which led to an expanded Bitcoin ecosystem, other blockchains, and additional forms of decentralized ledgers. The Bitcoin cryptocurrency has had a wild run, and its future remains uncertain. Blockchain, however, has catalyzed a quest to discover and realize its potential as a transformative technology.

References

Adkisson, J. (2018). Why bitcoin is so volatile. *Forbes*. Retrieved from https://www.forbes.com/sites/jayadkisson/2018/02/09/why-bitcoin-is-so-volatile/#698be53a39fb

Asolo, B. (2018). Blockchain soft fork & hard fork explained. *Mycryptopedia*. Retrieved from https://www.mycryptopedia.com/hard-fork-soft-fork-explained/

Au, S., & Power, T. (2018). *Tokenomics: The crypto shift of blockchains, ICOs, and tokens*. Birmingham, UK: Packt Publishing.

Baczuk, J. (2018). How to create a raw bitcoin transaction—step by step. *Medium*. Retrieved from https://medium.com/coinmonks/how-to-create-a-raw-bitcoin-transaction-step-by-step-239b888e87f2

Bitcoin. (2019a). *Bitcoin developer guide: Wallets.* Retrieved from https://bitcoin.org/en/developer-guide#wallets

Bitcoin. (2019b). *More free software projects*. Retrieved from https://bitcoin.org/en/development#more

Blockchain. (2019). *Blockchain size.* Retrieved from https://www.blockchain.com/charts/blocks-size?timespan=all

Boaventura, A. (2018). Where and how can blockchain be a better option than the traditional centralized systems? A straightforward answer for a very common question. *Medium*. Retrieved from https://medium.com/oracledevs/where-and-how-blockchain-can-be-a-better-option-than-the-traditional-centralized-system-model-edb0e3e1c9ee

Chase, B., & MacBrough, E. (2018). *Analysis of the XRP ledger consensus protocol.* Retrieved from https://arxiv.org/pdf/1802.07242.pdf

Comben, C. (2018). What are blockchain confirmations and why do they matter? *Coin Central*. Retrieved from https://coincentral.com/blockchain-confirmations/

DeVires, A. (2018). Bitcoin’s growing energy problem. *Joule*, *2*(5), 801-805.

Digiconomist. (2019). Bitcoin energy consumption index. Retrieved from https://digiconomist.net/bitcoin-energy-consumption

Feuer, A. (2013). The bitcoin ideology. *The New York Times*. Retrieved from https://www.nytimes.com/2013/12/15/sunday-review/the-bitcoin-ideology.html

Fischer M. J. (1983). The consensus problem in unreliable distributed systems (a brief survey). In M. Karpinski (Ed), *Foundations of computation theory* (LNCS vol. 158, pp. 127-140). Berlin, Germany: Springer-Verlag.

Fischer, M. J., Lynch, N. A., & Paterson, M. S. (1985). Impossibility of distributed consensus with one faulty process. *Journal of the Association for Computing Machinery, 32(*2), 374-382.

Genesis block. (2017). In *Bitcoin.com wiki.* Retrieved from https://wiki.bitcoin.com/w/Genesis_block

Herlihy, M. (2019). Blockchains from a distributed computing perspective. *Communications of the ACM*, *62*(2), 78-85.

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118-127.

Irreversible transactions. (2018). In *Bitcoin wiki*. Retrieved from https://en.bitcoin.it/wiki/Irreversible_Transactions#Attack_vectors

Jayachandran, P. (2017). The difference between public and private blockchain. *IBM.* Retrieved from https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, *1*(1), 36-63.

Kandaswamy, R., & Furlonger, D. (2018). Blockchain-based transformation: A Gartner trend insight report. *Gartner.* Retrieved from https://www.gartner.com/doc/3869696?refval=&pcp=mpe#a-1126710717

Kasireddy, P. (2017). Blockchains don't scale. Not today, least. But there's hope. Retrieved from https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

Kaushal, M., & Tyle, S. (2015). The blockchain: What it is and why it matters. *Brookings*. Retrieved from https://www.brookings.edu/blog/techtank/2015/01/13/the-blockchain-what-it-is-and-why-it-matters/

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems, 4*(3), 382-401.

Li, K. (2019). The blockchain scalability problem & the race for visa-like transaction speed. *Hackernoon*. Retrieved from https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44

Light, J. (2016). The key-decision makers in bitcoin. *Lightcoin*. Retrieved from https://lightco.in/2016/05/10/bitcoin-decision-makers/

Lombrozo, E., Lau, J., & Wuille, P. (2015). Segregated witness (consensus layer). *Github*. Retrieved from https://github.com/CodeShark/bips/blob/segwit/bip-codeshark-jl2012-segwit.mediawiki

Marr, B. (2018). 30+ real example of blockchain technology in practice. *Forbes*. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/05/14/30-real-examples-of-blockchain-technology-in-practice/#ee4dd78740de

McCullagh, A. (2017). Blockchain technology is not a commercial panacea to every problem. *LinkedIn*. Retrieved from https://www.linkedin.com/pulse/blockchain-technology-commercial-panacea-every-dr-phd-dr-adrian/

Meola, A. (2017). The growing list of applications and use cases of blockchain technology in business & life. *Business Insider*. Retrieved from https://www.businessinsider.com/blockchain-technology-applications-use-cases-2017-9

Merkle, R. C. (1987). A digital signature based on a conventional encryption function. In *Proceedings of the Conference on the Theory and Application of Cryptographic Techniques* (pp. 369-378).

Mulligan, C., Scott, J. Z. Warren, S., & Rangaswami, J. P. (2018). *Blockchain beyond the hype: A practical framework for business leaders*. *World Economic Forum*. Retrieved from https://www.weforum.org/whitepapers/blockchain-beyond-the-hype

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://nakamotoinstitute.org/static/docs/bitcoin.pdf

Narayanan, A. (2013). What happened to the crypto dream? Part 1. *IEEE Security & Privacy, 11*(2), 75-76.

Narayanan, A. (2015). "Private blockchain" is just a confusing name for a shared database. *Freedom to Tinker*. Retrieved from https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton, NJ: Princeton University Press.

National Institute of Standards and Technology (2015). *Secure hash standard (SHS) (FIPS-PUB 180-4).* Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

National Institute of Standards and Technology. (2013). *Digital signature standard (FIBS-PUB 186-4).* Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Orcutt, M. (2018a). States that are passing laws to govern "smart contracts" have no idea what they're doing. *MIT Review*. Retrieved from https://www.technologyreview.com/s/610718/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/

Orcutt, M. (2018b). How secure is the blockchain really? *MIT Review*. Retrieved from https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/

Poon, J., & Dryja, T. (2016). The Bitcoin lightning network: Scalable off-chain instant payments. Retrieved from https://lightning.network/lightning-network-summary.pdf

Rogers, E. M. (2003). *Diffusion of innovations*. New York, NY: Free Press.

Rosic, A. (2017). Proof of work vs proof of stake: Basic mining guide. *Blockgeeks*. Retrieved from https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Satoshi Nakamoto Institute. (2008). *Emails*. Retrieved from https://satoshi.nakamotoinstitute.org/emails/)

Shirer, M., & Goepfert, J. (2018). New IDC spending guide sees worldwide blockchain spending growing to $9.7 billion in 2021. *International Data Corporation*. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS43526618

Smith, A. (2017). Your business linking to the blockchain. *Huffington Post*. Retrieved from https://www.huffingtonpost.com/entry/your-business-linking-to-the-blockchain_us_5a33e0c3e4b02bd1c8c60609

Sonderegger, D. (2018). Blockchain: Can smart contracts replace lawyers? Retrieved from https://abovethelaw.com/2018/02/blockchain-can-smart-contracts-replace-lawyers/

Stratopoulos, T. C. & Wang, V. (2018). *Blockchain technology adoption*. *SSRN*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3188470

TechTarget. (2017). *Distributed ledger technology: Definition.* Retrieved from https://searchcio.techtarget.com/definition/distributed-ledger

The Linux Foundation. (2018). *About Hyperledger*. Retrieved from https://www.hyperledger.org/about

Thompson, C. (2017). Private blockchain or database? How to determine the difference. *The Blockchain Review*. Retrieved from https://medium.com/blockchain-review/private-blockchain-or-database-whats-the-difference-523e7d42edc

Trujillo, J., Fronthart, S., & Srinivas, V. (2017). Evolution of blockchain technology: Insights from the GitHub platform. *Deloitte*. Retrieved from https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html

Trump, B. D., Wells, E., Trump, J., & Linkov, I. (2018). Cryptocurrency: Governance for what was meant to be ungovernable. *Environment Systems and Decisions*, *38*(3), 426-430.

Vasa. (2018). ConsensusPedia: An encyclopedia of 30 consensus algorithms. *Hackernoon*. Retrieved from https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f

Young, J. (2018). How a cryptocurrency investor lost $60 million in bitcoin and never got it back. *CCN*. Retrieved from https://www.ccn.com/how-a-cryptocurrency-investor-lost-60-million-in-bitcoin-and-never-got-it-back/

About the Authors

Meg Coffin Murray is a Professor of Information Systems in the Coles College of Business at Kennesaw State University. She holds a PhD in Information Systems, an MBA in Finance, and a MS in Computer Science and has over forty years of experience in academe and industry. She specializes in developing and implementing emerging technologies to meet educational, business, and societal needs. Her work involves devising strategies to assess, remediate, and amplify skills needed to leverage IT in innovation, a primary driver of economic growth. Her current focus is on the emerging role of blockchain technology, machine learning, and artificial intelligence. She is a contributing member of industry blockchain working groups, holds a certificate in the study of cryptocurrencies, and frequent presents on bitcoin and the blockchain.