Quest for Knowledge paper for presentation on April 17, 2019

Blockchain and Cryptocurrency: The Distributed Ledger

Robert C. Maher

1. Introduction

In 2006, the laptop of a U.S. Department of Veterans Affairs data analyst was stolen from his home. The laptop had unencrypted information concerning 26.5 million veterans and active-duty personnel, including name, social security number, and date of birth. The incident exposed poor training of VA staff, and called into question whether clients could trust the agency to protect personal data.

In 2007, an increase in delinquent home mortgages in the United States revealed a serious weakness in the subprime mortgage market. Both a cause and an effect of the worldwide Great Recession, the rippling effects of the ensuing banking crisis quickly toppled several major investment institutions, including Lehman Brothers, AIG, Freddie Mac, Fannie Mae, and Merrill Lynch. While some institutions were bailed out by the U.S. government, the rapid devaluation of many financial investments caused reverberating tremors in the financial system for years afterwards.

Late in 2008, Bernie Madoff, a deceitful investment advisor and Ponzi scheme perpetrator, was indicted for securities fraud, and eventually pleaded guilty to 11 federal felonies that bilked clients out of $65 billion, including fictionally reported gains.

These and other spectacular incidents caused widespread uncertainty about how much trust members of the public should place in what had long been accepted as the literal and figurative pillars of the financial system: namely, government agencies, banks, and major investment firms. There was a growing sense that these "trusted third parties" could no longer be trusted.

Out of the mess of the late 2000s and early 2010s, a new concept emerged that would allow person-to-person financial transactions without the need for a trusted third party institution. The underlying concept, soon forming the basis of an *electronic cash system* called *Bitcoin*, involved a distributed database rather than a trusted institution.

Bitcoin relies upon computer-based processing of a publicly distributed database ledger. The ledger is not owned by a trusted third-party, but instead is distributed to anyone who wants to download a copy. The ingenious way in which a public ledger can be used for transactions by parties who do not trust one another relies upon a set of mathematical encryption algorithms to create a secure data structure called a *blockchain*. Blockchain will be the general topic of the remainder of this paper.

There are many, many new and emerging applications of electronic cash systems besides Bitcoin. Along with Bitcoin, these systems are collectively referred to as *cryptocurrency systems* because the allocation and transfer of financial assets involves strong cryptographic techniques to secure and to verify the asset transfer. Blockchain networks are being proposed for a variety of *peer-to-peer* transaction systems that will theoretically no longer require a layer of trusted proprietary service providers or intermediary brokers.

This paper is organized as follows. First, I give a simplified overview of the conventional financial payment systems using physical cash, and the current electronic transaction systems using a trusted third party such as a bank or credit card company. Next, I describe the basic principles of the proposed decentralized public ledger system known as blockchain, and what is currently the most notable blockchain system, Bitcoin. Finally, I conclude this paper with several brief comments and observations.

2. The basics of conventional payment systems

In an old-fashioned non-electronic cash-based transaction, the tacit assumption is that the government mint produces currency that cannot be counterfeited easily. Under this assumption, the buyer and the seller accept the validity of the currency and agree upon the selling price for a product or service. The purchase is concluded when the buyer gives physical possession of the currency to the seller. Following the cash transaction, there is no concern that the buyer would try to "double-spend" the funds, because the loot has been physically given to the seller. Physical cash allows a so-called *peer-to-peer* transaction that does not involve an intermediary.

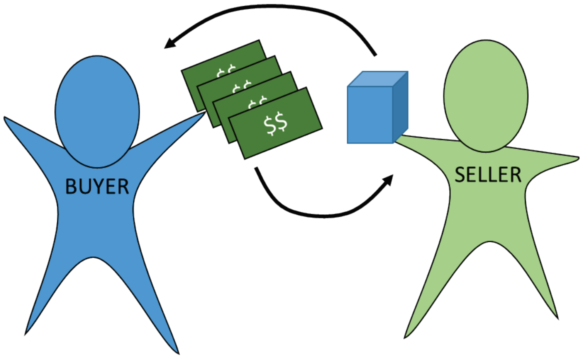

Figure 1: A peer-to-peer cash-based transaction (trusted currency).

At least theoretically, cash currency with unique individual serial numbers could be tracked as individually identified currency bills in a personal ledger. When used to buy something, the serial numbers of the cash would be removed from the buyer's currency log and entered into the seller's currency log. Because currency is essentially fungible, meaning that any dollar bill is equivalent to any other dollar bill regardless of serial number, it is conventional for accounting ledgers to contain just the amount of cash in or out, not the specific serial numbers affixed to each individual dollar bill transferred. But we could conceivably track the individually identified currency if we wanted to.

Storing and transferring physical dollar bills quickly becomes impractical for large purchases, and physical currency certainly does not work for electronic transactions. Thus, all of us have an agreement with a *trusted third party financial institution* that keeps our ledger and handles buyer/seller transactions in a standard manner. The financial institution generally co-mingles the physical dollars deposited by all of the account holders, and uses the ledger to keep track of each depositor's figures. At least that is what we *trust* the institution to do until there is a fraud or error of some kind.

While most of us are acquainted with making a payment using an old-fashioned check, behind the scenes we rely upon our trusted financial institutions to process that check and conclude the payment using funds that we have entrusted to our particular institution. In such a case, we no longer have a peer-to-peer transaction, because our financial institution is acting as an intermediary in concluding the transaction. Similarly, using the contemporary internet, an "online" purchase generally requires a trusted third party to enable the payment reconciliation, often by a large credit card firm, or an enterprise such as PayPal or Google Wallet.

Whether a paper check or an internet purchase, the third party "middleman" is so ubiquitous in these transactions that we might not even think much about the back-office operation that supports our common adventures in commerce. Consider the sequence of events that take place when making an online purchase with a credit or debit card. First, you and the seller have agreed upon a currency and a selling price. Second, you present your account number and some authentication information to the seller. Next, the seller presents the information to your financial institution, which then authorizes the desired amount. Your financial institution also makes note that funds from your account are no longer available to be spent (or in the case of a credit card, that your available amount of credit has been reduced). The seller then processes your order, and eventually receives the agreed upon payment from your financial institution. Typically, the financial institution collects a fee that it keeps in return for enabling the transaction.

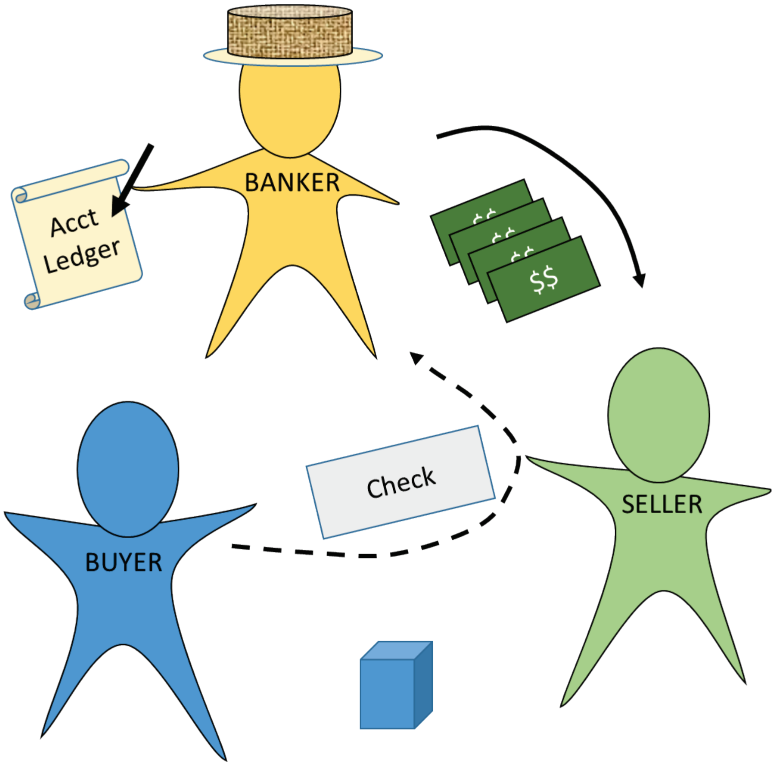

Figure 2: A transaction requiring a private ledger and "trusted intermediary" (the banker).

This relatively simple process can go wrong in a few different ways, especially in the area of the *trust* required among the buyer, seller, and the intermediary financial institution. Of particular concern is a breech involving the financial institution that fraudulently short-changes the buyer or swindles the seller. The most common fraud is a falsified amount presented to the financial institution by the "seller" (the thief) who then receives payment from the unknowing victim's account.

For individuals, the physical cash system allows peer-to-peer transactions without the necessity of a trusted third party. However, modern electronic transactions cannot be done practically via physical cash. Perhaps there is some way that individuals who distrust big financial institutions can cut out the third party intermediary and still engage in financial transactions on the internet?

That is what "Satoshi Nakamoto," the pseudonym of an anonymous computer expert (or group of experts), decided to invent in 2008. No one knows if Satoshi Nakamoto is a real person or a fictional character, but the original white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," appeared under his name in October, 2008.

3. Blockchain and Bitcoin

If one distrusts the "trusted" financial institutions, a peer-to-peer *electronic* transaction system would need to operate based on a shared, public digital ledger that all participants could see, not a hidden ledger at the bank. However, a public ledger that can be written into by anyone will obviously be susceptible to mistakes, fraudulent entries, and the likelihood of double-spending, e.g., first recording a payment transaction, then secretly erasing it and recording another payment using the same funds. How can these issues be eliminated without assigning a trusted authority to manage everything? The innovation involves several essential concepts, as described in the following sections.

3.1. Bitcoin as a "foreign" currency

Before continuing, a brief, preliminary explanation of "Bitcoin" may be helpful at this point. I find it useful to think of Bitcoin as one might think of a foreign currency, like Canadian dollars or the Euro. Just like a foreign currency, the "value" of a cryptocurrency like Bitcoin depends upon the money market exchange rate for that currency. The value is determined by the market price agreed upon by the buyer of the currency and the seller. Since the foreign currency's value in, say, U.S. dollars is determined by a market, the value of Bitcoin cryptocurrency also varies from hour to hour and day to day according to market forces. In fact, some of the initial interest (and hype) about Bitcoin was from speculative investors. Like any market, when buyers are eager to get in, but sellers are not eager to get out, the price goes up. The long-term viability of the Bitcoin cryptocurrency remains to be seen.

Thus, just like a store that accepts payment in U.S. dollars but not Canadian dollars, or a seller who can accept payment either in U.S. dollars or Euros, another seller might choose to offer a product or service priced in Bitcoin. If Bitcoin eventually attains sufficient participation and acceptance by merchants, it might become a new international financial tender for electronic peer-to-peer commerce between buyers and sellers anywhere in the world.

3.2. Blocks and Hashes

A peer-to-peer electronic commerce system is based upon a shared public ledger. In the model proposed by Satoshi Nakamoto, the digital public ledger consists of data *blocks* that contain a set of new transactions. A new block is appended onto the end of the existing ledger, thereby forming a *chain* with new links added onto the end—creating a so-called *blockchain*.

Once part of the blockchain, all preceding blocks cannot be altered or changed. This is because a valid new block added to the end of the chain contains special codes that depend intimately on every preceding block in the chain using a cryptographic *hash* function (see below). Even a tiny change anywhere in the blockchain would reveal a discrepancy in the added block, so the integrity of the blockchain ledger can be ensured with strong mathematical certainty. Anyone who downloads the blockchain database can verify the chain's integrity this way.

A *hash* function refers to a deterministic mathematical operation that computes a fixed-length string of characters and numbers from a longer block of data. For example, a very simple hash function might be: "count the number of binary '1' bits in the digital data block." The *hash value* in this example would be an integer that is the number of bits that are '1'. To illustrate using a very short block consisting of just eight bits, the block '00011011' would therefore have hash equal *4*, and a block '01001001' would have hash equal *3*. The range of possible hash values in this example is an integer from zero through eight. This sort of hash is often called a *checksum*.

This simple "count the 1's" hash function demonstrates two important points. First, knowing the hash value does not uniquely determine the contents of the original block. We can easily calculate the hash function for any block, but knowing the hash doesn't allow us to "invert" the process and figure out the block contents. Second, this particular example hash function is not very strong, because there are many block patterns that would give the same hash. For example, '00000001', '00000010', '10000000', etc., all have hash equal to 1. A hash function suitable for encryption would have additional mathematical complexity.

Nevertheless, a simple hash function like "count the 1's" can still be of practical use. If we kept track of the hash for a particular data block and then sent the block into a storage system, we could re-compute the hash when we later retrieved the block from storage and see if it was different from the original hash. This sort of simple hash could be used to detect a single *bit error* in the block: if the hash didn't match, then we would know that one of the original '1' bits must have changed to a '0', or vice versa. Of course, this simple hash function would not work if there were an even number of bit errors, since in that case the hash would still match the original.

For use in a *blockchain*, the blocks are longer than eight bits, and the cryptographic hash function is much more sophisticated than the "count the 1's" example. The hash function is designed to be very sensitive to even a small change in the block contents, and it is cryptographically strong in the sense that unlike the simple "count the 1's" strategy, it is infeasible to find two different block contents that have the same hash value. But like the simple hash function example, the blockchain cryptographic hash function is easy to compute, but essentially impossible to invert: knowing the hash value does not allow recreating the block contents.

3.3. The key system

Because the public ledger blockchain is available for all to see, privacy and security requires a set of user identity shields and passwords governing the transactions. Ownership of funds recorded in the blockchain are designated by unique codes known as *keys*. Like a physical lock and key, the blockchain keys have two complementary parts: a *public key* that is essentially an anonymous user identification code or digital signature, and a *private key* that is unique and known only by the owner who uses it, like a secret password. The public key and the private key have special mathematical properties that ensure that the keys are statistically impossible to guess from one another, but that work together in a manner analogous to a physical lock and key.

To prepare a message for inclusion in a blockchain, the user mathematically combines the message with the user's *private* key in such a way that the message is encoded but the private key is not revealed. Nonetheless, any other user who knowns the first user's *public* key can verify that the message was in fact encoded with the proper private key, and is therefore authentic.

For Bitcoin, the encoded message is a financial transaction involving the seller and buyer of the digital coins. The seller uses the private key to encode the transaction to show its authenticity. When the transaction is processed (see below), the transferred coins get a new public key and private key for the recipient, who can then keep or trade the acquired coins via the same mechanism.

3.4. Extending the blockchain: the "miners"

If any user could easily add or remove blocks from the chain, the system would quickly lose its integrity and synchronization. Instead, a blockchain system has a special category of users referred to as *miners*. The term *miner* comes from the concept of a gold miner: the way to create new assets when gold was the preferred standard for payment was to mine new gold. In a blockchain system, the miner is actually a computer process, and a blockchain network ideally has many of the so-called miners, each operating in competition with one another, anonymously and independently around the world. The role of the miners is to detect and aggregate transaction requests from users, validate the requests using the key signatures, and add them onto the end of the blockchain as a new and valid block.

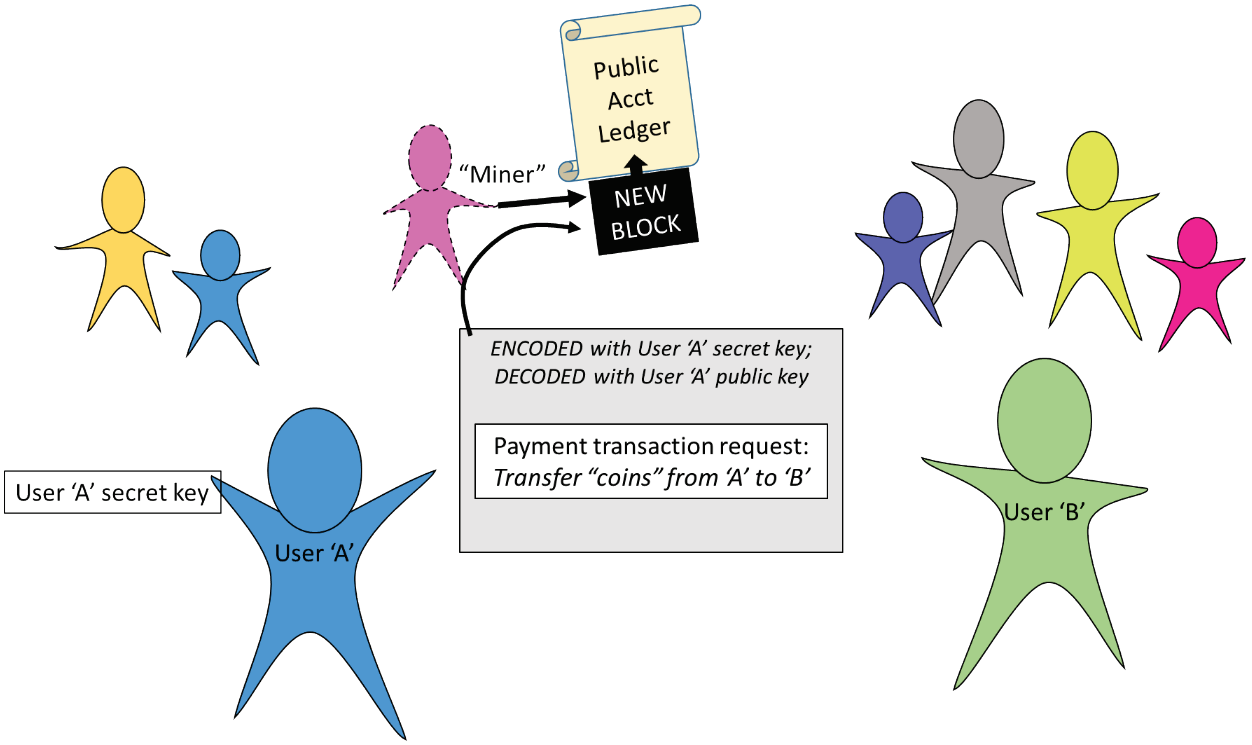
Public
Acct
Ledger
"Miner"
NEW
BLOCK
ENCODED with User 'A' secret key;
DECODED with User 'A' public key
Payment transaction request:
Transfer "coins" from 'A' to 'B'
User 'A' secret key
User 'A'
User 'B'

Figure 3: A "blockchain" transaction involves a public ledger and private encryption keys. All users can see and verify the ledger, even if the buyer and seller do not trust each other.

Part of the validation process is to look back through the block to verify that the seller in the transaction actually owns the specified asset and has not already transferred it, based on the public keys and block timestamps. But the primary job of the miner is to encode the new block cryptographically so that it is irreversible and tamperproof. This is accomplished using a scheme known as *proof-of-work*.

3.5. Proof of Work

In essence, the *proof of work* requirement makes it very computationally expensive to add a block to the chain, so the most capable computational resources on the network must be available to perform the mining task. As noted before, identical copies of the public blockchain are constantly distributed and available to all users. When it is time to accomplish new transactions and create a new block on the end of the chain, all the users will need to update their copies of the blockchain and verify that the new block is valid. If it was easy to add a new block or to re-calculate the entire blockchain, a nefarious user might decide to create bogus transactions, or to delete or edit prior transactions and create a different and fraudulent copy of the blockchain. That would defeat the whole purpose of having a public ledger.

To eliminate this problem, the creator of Bitcoin (the character named Satoshi Nakamoto) invented a way to make tampering infeasible. In order for a miner to add a new block on the end of the existing blockchain, the miner has to "guess" an encoding value (called a *nonce*) over and over from a vast number of random encoding keys until the hash function produces a hash value that is smaller in magnitude than a specified numerical value. In other words, the computed hash value has a certain number of leading zeroes. Since there is no way mathematically to predict in advance the nonce value that will work, the miner has to keep trying over and over until a match is found. The cryptographic basis of the hash function requires substantial computation for each nonce, so the miner must use substantial computer time (and therefore electrical power) to try to come up with a nonce that will produce a valid hash value. Bitcoin uses a standard hash function called SHA-256 (Secure Hashing Algorithm 256).

This guess-and-check process is analogous to having a lock that requires a key to close, and a huge container with keys that might or might not work in the lock. Looking at each key does not help: you have to try keys one by one until you find one that operates the lock. Only then can the miner add the new block to the blockchain and announce that a new public chain is available. When this happens, all the other users can test the new blockchain to verify that its "proof of work" meets the required cryptographic standard. If a user finds that the new blockchain is invalid, it is ignored. If it is found to be valid, the updated blockchain is used for future transactions and the process continues.

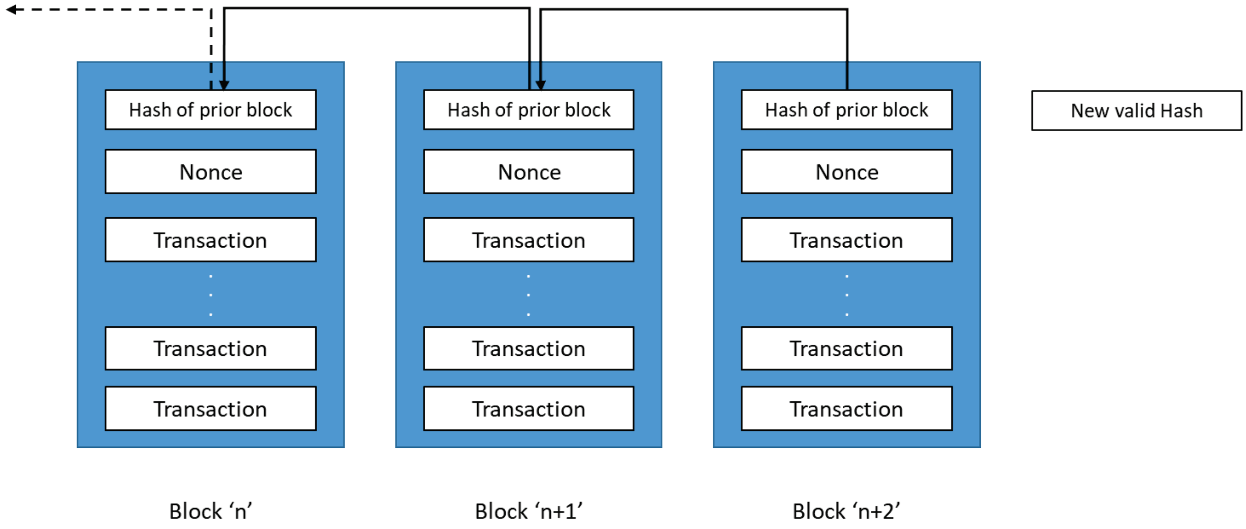

Figure 4: The "blockchain" uses mathematical cryptographic verification as proof of validity.

An important incentive feature that is used in the Bitcoin system is that there is a competition among the miners on the network to be the first one to compute a valid new block when processing the latest transaction requests. The miner receives a payment (in Bitcoin, of course) for accomplishing the new block generation. Thus, there is an incentive to have the most computing power to take on the cryptographic tasks in order to get credit for creating valid blocks on the chain.

The drawback to this approach, however, is that the amount of electrical power required to be a competitive miner in the Bitcoin system is currently so great that it is of environmental concern! It is my understanding that it currently requires about 10 minutes for a miner to produce a valid block using the fastest available computers, and over 200 kilowatt-hours of electrical energy. With retail electricity costing roughly 10 cents per kWh, that means $20,000 to compute one new block in the chain.

Because of the electrical power expense, future cryptocurrency systems may decide to use a different approach to "award" the opportunity to compute the next valid block in the blockchain. The system users could use some sort of lottery to select the next miner, or give selection preference to individuals with the greatest coin holdings, or use a bidding system. In any case, some solution to the electrical power consumption threat will need to be devised.

4. Will blockchain comprise the future of peer-to-peer commerce?

The origin of blockchain in general, and cryptocurrencies like Bitcoin in particular, was the distrust of financial middlemen and their potentially fraudulent behavior: a distrust of trusted authority. However, financial payment services are not the only types of transactions that currently involve a trusted intermediary. In a peer-to-peer world comprising blockchain systems, perhaps we can obtain recorded music directly from the musician and not pay a fee to an intermediary aggregator like Apple iTunes or a record label. Perhaps we can get a travel insurance contract or hire a rideshare service by engaging in a blockchain transaction, thereby avoiding a pushy sales agent or having to share personal information we would prefer to keep anonymous. Any transaction between peers who don't need or want to trust each other could be an application of blockchain techniques.

Some analysts are predicting that governments will start creating and using cryptocurrency in tandem with existing physical currency. This prospect may be difficult to imagine in a large and mature economy such as the United States or the European Union, but it could be feasible and even desirable for emerging economic systems in Africa, or perhaps in authoritarian countries like China. Even in the U.S., many people already conduct their business in a cashless manner. Questions will inevitably arise regarding the availability of the blockchain ledgers and the impact of electronic network outages or curtailment. It is already a serious issue for commerce if freely open communication is cut off due to an earthquake, hurricane, or terrorist act, and such worries would be amplified if the entire financial system operated with mandatory network connectivity.

In conclusion, it is clear that relatively new inventions like blockchain and cryptocurrencies like Bitcoin currently exist in an experimental phase. This means that there are likely to be new ideas and innovations emerging as more and more people become interested in the strengths and weaknesses of such systems. While the long-term viability of specific products like Bitcoin is not known, the consensus appears to be that the underlying blockchain principles of decentralized control, public access to the ledger and its algorithms, and security against fraud are now expected features of any new proposal for peer-to-peer transactions.

References:

Bitcoin.org, "How does Bitcoin work?" https://bitcoin.org/en/how-it-works, 2018
[accessed 24 March 2019].

Brito, Jerry, and Castillo, Andrea, "BITCOIN: A Primer for Policymakers," Mercatus Center, George Mason University, https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf, 2013
[accessed 24 March 2019].

Fortney, Luke, "Blockchain, Explained," Investopedia,
https://www.investopedia.com/terms/b/blockchain.asp, 10 February 2019. [accessed 24 March 2019]

Mitselmakher, Kate, "The Future of Blockchain Technology: Top Five Predictions for 2030," Blockchain Expo Event Series, https://www.blockchain-expo.com/2018/10/blockchain/future-of-blockchain-technology/, 11 October 2018 [accessed 24 March 2019].

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System." White Paper, 2008.
http://bitcoin.org/bitcoin.pdf, [accessed 24 March 2019].

Peck, Morgen E., "Blockchains: How They Work and Why They'll Change the World," IEEE Spectrum, https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world, 28 September 2017 [accessed 24 March 2019].