Distributed Ledger and Blockchain Technology: Framework and Use Cases [*] [†]

Seoyoung Kim
Santa Clara University

Atulya Sarin
Santa Clara University

[Forthcoming in *Journal of Investment Management*]

April 2018

JEL Classification: G0; G2; N2, O0.
Keywords: distributed ledger; blockchain; decentralized autonomous organization; FinTech.

[*] We thank Sanjiv Das for helpful comments and discussion.

[†] The authors may be reached at: srkim@scu.edu; asarin@scu.edu.

Distributed Ledger and Blockchain Technology: Framework and Use Cases

April 2018

Abstract. Since its first widespread implementation in 2009, distributed ledgers in general, and blockchain technology in particular, have rapidly become a part of the FinTech vernacular. In this paper, we provide an overview of the history of trade settlement and discuss this nascent technology that may now transform traditional methods of verifying and settling transactions. In so doing, we discuss current and potential use cases of this technology and provide a business-oriented framework for proper as well as improper implementations and applications of blockchains and distributed ledgers.

JEL Classification: G0; G2; N2, O0.
Keywords: distributed ledger; blockchain; decentralized autonomous organization; FinTech.

1. Introduction

The idea of a distributed, permission-less ledger originated in the late 1990s,[1] with the first official use case, in the form of *Bitcoin*, emerging in 2009. Specifically, the original Bitcoin blockchain was designed to create "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact without the need for a trusted third party."[2]

A free-flowing exchange of goods requires confidence in the validity of the exchange. That is, smooth and fluid marketplace transactions are predicated on trust and well-established property rights, given that the exchange of goods is really defined by the exchange of the *rights* to those goods.[3] Modern markets have established centralized, trusted intermediaries for this purpose. More recently, FinTech disruptions have attempted to minimize the role of financial intermediaries by facilitating peer-to-peer transactions among strangers. Further, technological innovations increasingly enable automated implementation via smart contracts,[4] moving us away from manual verification and execution.

However, a trusted intermediary (e.g., Lending Club, Prosper) continues to broker these transactions. Thus, a natural question arises as to whether the intuitive evolution of transactions and exchanges of ownership can move toward a truly decentralized trustless economy. That is, can we achieve true peer-to-peer transactions without a trusted intermediary to validate the integrity of the exchange?

Our purpose is to provide an overview of the nascent technology that may now transform traditional methods of verifying and settling transactions. The rest of the paper is organized as

[1] See, for instance, proposals by Wei Dai, accessed on http://www.weidai.com/bmoney.txt>; and Nick Szabo, accessed on <https://unenumerated.blogspot.com/2005/12/bit-gold.html>

[2] Nakamoto, Satoshi. *Bitcoin: Peer-to-Peer Electronic Cash System,* accessed on <https://bitcoin.org/bitcoin.pdf>

[3] Demsetz, Harold (1967), "*Toward a Theory of Property Rights.*"

[4] Szabo, Nick (1997), *"Formalizing and Securing Relationships on Public Networks."*

follows. In Section 2, we explain the basic underpinnings of blockchain/distributed-ledger technology and how a decentralized autonomous organization works. In Section 3, we provide specific use cases within the blockchain ecosystem, and in Section 4, we provide a framework to determine when a blockchain approach is appropriate, and when it is not. Finally, in Section 5, we provide concluding remarks. A glossary of technical terms is provided in **Appendix A**.

2. Blockchain / Distributed Ledger Technology

We generally employ the terms "blockchain" and "distributed ledger" interchangeably, because the verification protocol on most open-source distributed ledgers is currently implemented on a public blockchain. However, there are other ways to design a distributed ledger protocol, and as we discuss further in Section 2.2 ("Other Considerations in Implementing a Distributed Ledger"), some of the latest innovations depart from the original blockchain approach.

For the avoidance of doubt, a blockchain verification protocol can be implemented on a single, centralized ledger rather than being maintained across many users or nodes. That is, a distributed ledger refers to a record of transactions replicated and maintained across multiple users or systems to mitigate the likelihood of accidental or malicious alterations. However, distributed ledgers can differ in how participants verify and add transactions to the ledger, and a blockchain-based protocol is one such method to do so. We now describe the basic design underlying a blockchain-based distributed ledger.

2.1. How Does a Basic Blockchain Implementation Work?

In a blockchain-based ledger, transactions are grouped together into blocks. Then, depending on the specific rules of the blockchain in question, the current block is closed and a new block is created once a certain number of transactions has been recorded or some other criteria have been fulfilled. This new block is cryptographically linked to the prior block, thereby forming a *blockchain*.

For instance, the Bitcoin blockchain is secured by a hashcash proof-of-work protocol, using double SHA-256 (also known as SHA256^2) to link each new block to the last. SHA-256 refers to a *secure hash algorithm* that generates a 256-bit (64-character) alpha-numeric hash code, also known as the checksum. Double SHA-256 repeats the hash process, thereby passing the hash code from the first iteration through the SHA-256 cryptographic hash algorithm once more.

To explain the Bitcoin blockchain, we first demonstrate a simplified blockchain-based distributed ledger, whereby the first element of each block is the hash code from passing all elements of the prior block through the SHA-256 hash function (see **Figure 1**). Suppose one participant in the distributed-ledger network attempts to alter the transaction records in Block N+1, so that Jane appears to have received 12 coins rather than the 10 coins she actually received. The resulting hash from this altered block will no longer match the hash code written into the first element of the subsequent block (see **Figure 1**), creating a domino effect that causes the original hash codes written into all subsequent blocks to also contradict the revised hash codes resulting from hashing the altered contents of each prior block.

Thus, as long as 51% of participants of the distributed ledger are honest, the network will reject this faulty block and reach consensus via the correct majority of peer blocks, resulting in what many refer to as an *immutable* ledger. However, the blockchain is not literally immutable, and from the example above, we can see that the most recent blocks are the most vulnerable. As a result, to prevent double spending, businesses and individuals typically require a transaction record to be several blocks deep before considering the transaction to be officially confirmed.

To explain the Bitcoin blockchain itself, we must discuss the role of miners on the Bitcoin network, where the current reward for “mining” a new block is 12.5 newly-created bitcoins (BTC).[5] Bitcoin miners look for an arbitrary number called a *nonce*, which, when combined with the current block’s transactions and then hashed, produces a double SHA-256 hash code with a certain number of leading zeroes. The required number of leading zeroes that determines the “winning” nonce is a simplified representation of the difficulty level of Bitcoin mining and prevents blocks from being formed too rapidly. The Bitcoin protocol is designed to form a new block approximately every ten minutes, and, accordingly, the current difficulty level is set to require a nonce that produces 18 leading zeroes in the double SHA-256 hash code when combining the elements of the block with this nonce.[6] Thus, this nonce is difficult to find, but easy to verify. The computational power required to solve for this nonce is what secures networks operating under a proof-of-work (PoW) consensus protocol.

Given the leaderless and permissionless nature of public blockchains and other open-source distributed ledgers, these systems are often referred to as *decentralized autonomous organizations* (i.e., DAOs). Before we discuss the governance mechanisms inherent in a DAO, we first discuss other issues to consider in implementing a distributed ledger.

2.2. Other Considerations in Implementing a Distributed Ledger

Given the increasing popularity of distributed ledgers such as the BTC and Ethereum (ETH) protocols, the ability of these systems to accommodate more users has been an increasing concern. This issue, referred to as horizontal scalability, has rapidly become a central consideration in updates to existing platforms as well as to the ex-ante design of newer platforms coming to market.

[5] bitcoinmining.com, *What is the Bitcoin Mining Block Reward,* accessed on <https://www.bitcoinmining.com/what-is-the-bitcoin-block-reward/>

[6] Medium, *Decoding the Enigma of Bitcoin Mining,* accessed on <https://medium.com/all-things-ledger/decoding-the-enigma-of-bitcoin-mining-f8b2697bc4e2>

Here, we discuss several prominent issues considered in achieving horizontal scalability, specifically pertaining to: (i) block size and block time, (ii) the consensus protocol (e.g., proof-of-work versus proof-of-stake), and (iii) the ledger design itself (e.g., blockchain versus directed acyclic graph).

Block Size/Time. One bottleneck to achieving horizontal scalability lies in the limit imposed on each block size. Because the Bitcoin blockchain difficulty level is designed to validate a new block formation approximately every ten minutes, the actual block sizes and formation times can vary. Naturally, with the dramatic increase in transaction volume, the average block sizes have increased over time,[7] and transaction times have recently seen much greater variability.[8] That is, the 1-MB limit currently imposed on each BTC block size is regularly exhausted in times of high volume, forcing transactions into subsequent blocks. In response, the Bitcoin Cash blockchain,[9] which hard-forked from block number 478,558 of the original BTC blockchain,[10] allows more transactions per block, with a maximum block size currently set to 8 MB per block.

However, larger blocks are more vulnerable to double-spend attacks, as explained earlier and demonstrated in **Figure** 1. That is, we have seen that the most recent blocks are the most vulnerable to malicious alteration, and larger blocks leave more transactions exposed. Other issues to consider are the additional network bandwidth required to relay larger blocks, and the additional computational power required to mine a new block under a proof-of-work consensus protocol. Although these additional costs are not prohibitive for increases in the order of several megabytes

[7] Blockchain. *Average Block Size,* accessed on <https://blockchain.info/charts/avg-block-size>

[8] According to CNBC, the average time to confirm a Bitcoin transaction in December 2017 was 78 minutes on certain days, but 1,188 minutes on others. See Ryan Brown, *Big transaction fees are a problem for bitcoin – but there could be a solution,* accessed <https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html>

[9] Bitcoin Cash, accessed on <https://www.bitcoincash.org/>

[10] A hard fork is the result of substantial changes to the consensus protocol that are not designed to be backward-compatible, thereby resulting in a separate blockchain. In contrast, soft forks are implemented regularly to update the blockchain protocol and are designed to be backward-compatible.

(as evidenced by Bitcoin Cash), the costs quickly compound if block sizes must continue to grow to accommodate an entire population rather than a small subset of technologically progressive adopters.

In comparison, the ETH blockchain has significantly smaller block sizes, and far shorter block times, with a new block typically being formed every 15 seconds.[11] However, rapid block formation has some disadvantages, such as a greater likelihood of accidental splits that must be resolved. That is, two miners may each find a conforming nonce within a short timeframe and begin to broadcast their respective new blocks to the rest of the network. The consensus protocol must ultimately invalidate one of these blocks to resolve the accidental split, leaving an orphan block (also known as the "uncle" block in the ETH network) behind.

Consensus Protocol. Another bottleneck lies in the chosen consensus protocol. As discussed, the original BTC blockchain is predicated on a *proof-of-work* (PoW) consensus protocol, whereby a computationally taxing problem must be solved to mine a new block. In contrast, many distributed ledger systems are moving to a *proof-of-stake* (PoS) consensus protocol, whereby a user or subgroup of users is designated to validate the next block. The selection process is often based on relative stake in the system, such as proportional ownership of native tokens, and can incorporate a stochastic element to avoid centralizing the validation process. Thus, under pure PoW, the integrity of the distributed ledger hinges on whether a single party controls 51% of computing power in the network, whereas under pure PoS, the integrity of the distributed ledger hinges on whether a single party controls 51% of the native tokens.

Although a PoS consensus protocol is far faster than a PoW protocol, the lower latency may introduce other vulnerabilities concerning the integrity of the validated blocks. Thus, the latest

[11] Etherscan, *Ethereum Average BlockSize Chart*, accessed on <https://etherscan.io/chart/blocksize>

iterations of PoS add punitive elements to the mechanism, and some propose to combine elements of PoS and PoW. Projects currently implementing a PoS protocol include Waves,[12] which is based on a delegated PoS approach, and NEO,[13] which is based on a variant referred to as a Delegated Byzantine Fault Tolerant (dBFT) protocol. Ethereum, which is currently based on a PoW consensus protocol, is expected to transition to a hybrid protocol involving elements of both PoW and PoS.[14] Other creative solutions have also been implemented, such as Ripple's XRP ledger consensus process,[15] which reaches consensus via multiple validation rounds across participants on the network.

Ledger Design. Finally, the latest innovations to improve horizontal scalability involve proposals to alter the ledger design itself and eliminate the use of blocks altogether. That is, some developers have proposed replacing the blockchain design with a *directed, acyclic graph* (DAG) to serve as the ledger for recording transactions. Under this design, each node that wishes to make a transaction must first validate a selected set of other transactions. The verification process is asynchronous, and different nodes will see different but overlapping subsets of transactions. Projects currently implementing this design include Byteball,[16] which launched in December 2016, and IOTA,[17] which is still under development.

2.2. How Does a Decentralized Autonomous Organization (DAO) Continue to Function?

Currently, the ongoing governance of a public blockchain or open-source distributed ledger is maintained implicitly through a native token or coin on the protocol known as a *cryptocurrency*,

[12] Waves, accessed on <https://wavesplatform.com/>

[13] NEO, *NEO White Paper,* accessed on <http://docs.neo.org/en-us/>

[14] Github, *ethereum / research,* accessed on <https://github.com/ethereum/research/wiki/Casper-Version-1-Implementation-Guide>

[15] Ripple, *The XRP Ledger Consensus Process,* accessed on <https://ripple.com/build/xrp-ledger-consensus-process/>

[16] Byteball, *Smart payments made simple,* accessed on <https://byteball.org/>

[17] IOTA, accessed on <https://iota.org/>

which serves as the required method of payment to transact on the protocol. Some DAOs, such as NEO,[18] have two tokens: one token for voting rights (i.e., the NEO token), and one token for use on the platform (i.e., the NeoGas (GAS) token). However, most DAOs have a single native token that is used to transact on the platform and also serves to compensate validators on the network. For instance, participants who wish to execute smart contracts on the Ethereum blockchain must use ETH (Ether tokens),[19] and participants who wish to engage in peer-to-peer currency transactions on the Ripple XRP blockchain must use XRP (Ripple tokens).[20] See Kim, Sarin, and Virdi (2018) for a more comprehensive overview of cryptocurrencies in general, and utility tokens in particular.

The value of the native tokens (i.e., coins) inherent in the distributed ledger protocol maintains the governance inherent in these leaderless, autonomously run organizations. That is, if the protocol does not remain up to date and other better platforms materialize, the native tokens used to transact on the original protocol become worthless. Thus, developers (who, themselves, own native tokens) are incentivized to maintain the protocol and design timely updates, without direction from a manager or centralized leadership. This type of implicit internal governance is similar to that of a neighborhood that autonomously keeps public areas safe and clean, because individual homeowners are motivated to maintain the value of their homes.

3. Current Use Cases

Since the advent of Bitcoin, the use of blockchain technology and distributed ledgers has rapidly multiplied. In this section, we discuss a variety of use cases within the nascent but burgeoning blockchain ecosystem, beginning with its original use case as a medium of exchange. In so doing,

[18] NEO, accessed on <https://neo.org/>
[19] Ethereum, accessed on <https://ethereum.org/>
[20] Ripple, *XRP The Digital Asset for Payments,* accessed on <https://ripple.com/xrp/>

our focus is on improvements to traditional methods of record-keeping and transaction-clearing, rather than on blockchain-based projects that do not highlight or truly leverage the benefits or enhancements derived from implementing a distributed ledger (e.g., tokenized securities and asset-backed tokens, which do not capitalize on the benefits of a trustless, decentralized system). In **Section 4**, we provide guidelines on when distributed ledgers are not only feasible but particularly beneficial.

3.1. Currency / Medium of Exchange

The first official, widespread implementation of a blockchain-based distributed ledger was based on the objective of providing a truly decentralized medium of exchange without the need for a trusted third-party intermediary. Since the advent of BTC in 2009, other similar projects have followed in its wake, including Litecoin,[21] which was deployed in 2011, and Bitcoin Cash, which hard-forked from the BTC blockchain in 2017.

Given the open-source nature of these public blockchains, privacy concerns have surfaced with regard to participating in these trustless, pseudonymous peer-to-peer exchanges. That is, all transaction records are memorialized on the blockchain, which can be viewed by anyone without permission. Thus, for any given public wallet address, we can view the current balance and entire history of transactions, with corresponding public wallet addresses of the counterparties to each transaction.[22] In response, some blockchain projects have developed privacy coins, which are also built on a public blockchain, but are designed to hinder traceability by repeatedly issuing multiple keys for each transaction. Projects that either feature or provide privacy options in peer-to-peer

[21] Litecoin, accessed on <https://litecoin.org/>

[22] For a comprehensive record of transactions on the Bitcoin blockchain, see, for instance, Block Explorer, accessed on <https://blockexplorer.com/>

exchanges include Monero[23] and Dash (formerly known as XCoin and Darkcoin),[24] both of which were deployed in 2014.

3.2. Other Transaction Settlements

The very nature of a blockchain-based distributed ledger lends itself naturally to other implementations designed to facilitate trustless yet secure settlements in a variety of settings. For instance, typical securities transactions currently settle within two business days, known in industry parlance as "T+2."[25] While part of the settlement time allows the parties to obtain the required cash or securities in transactions that involve short sales or margin trading, the T+2 convention still holds for transactions that simply transfer a long position from one party to another. Settling real-estate transactions requires even greater wait times, as well as a trusted third-party escrow service to broker the transaction and title insurance to protect the buyer in case the seller did not have the full rights to transfer the deed to the property in question.

Recently, blockchain-based projects have surfaced in an attempt to reduce the time required to verify and settle transactions and mitigate the risks inherent in false verifications. For instance, Ubitquity[26] has developed a blockchain-based platform for property records, and tZERO[27] is currently developing a distributed-ledger-based platform for equity trading.

[23] Monero, accessed on <https://getmonero.org/>

[24] Dash, accessed on <https://www.dash.org/>

[25] Lynch, Sarah N. 2017. *SEC shortens settlement cycle for securities trades.* Reuters. March 22. Accessed on <https://www.reuters.com/article/us-usa-sec-settlement/sec-shortens-settlement-cycle-for-securities-trades-idUSKBN16T1SW>

[26] Ubiquity, accessed on <https://www.ubitquity.io/web/index.html>

[27] tZERO, accessed on <https://www.tzero.com/>

3.3. Healthcare

Aside from cheaper, faster, and more reliable transactions, a distributed record-keeping process itself may prove to be the next step in healthcare.[28] Although medical records are available electronically in the form of electronic health records (EHRs), patients face substantial hurdles in distributing their medical history as they switch providers, see multiple specialists, or seek consultations. Difficulties compound in the emergency treatment of an unconscious patient, when aspects of the patient's medical history must be inferred, sometimes through invasive tests. MedRec,[29] which is currently under development, seeks to address these issues by creating a secure, properly anonymized method for storing patient records on a blockchain-based distributed ledger.

3.4. News and Social Media

Another area suited for disintermediation is the social-media space. For instance, Twitter and Facebook users operate with permission and are governed by a central authority who can remove posts or cancel accounts. The DAO aspects of a public blockchain provide the means to achieve a truly uncensored and decentralized social-media experience, although with the attendant negative externalities that accompany this lack of scrutiny. Current projects in this space include Eth-tweet,[30] which refers to itself as a "decentralized Twitter," and Presscoin,[31] which is currently under development and seeks to decentralize the news-reporting process.

[28] Halamka, John D., Andrew Lippment, and Ariel Ekblaw. 2017. "The Potential for Blockchain to Transofrm Electronic Health Records," *Harvard Business Review.* March 3. Accessed on <https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records>

[29] Medrec, accessed on <https://medrec.media.mit.edu/>

[30] Github, *yep / eth-tweet,* accessed on <https://github.com/yep/eth-tweet>

[31] Presscoin, accessed on <https://www.presscoin.com/>

3.5. Dark Pools

Finally, the implementation of a trustless, decentralized dark pool represents another natural DAO, given the mistrust in the order-routing process and potential disclosures along the way to execution.[32] A dark pool is a private trading venue where financial instruments can be exchanged anonymously. Thus, a truly trustless and anonymized dark pool that does not require faith in a central operator provides a natural path for this particular business model. Republic Protocol,[33] which is currently under development, seeks to provide a decentralized autonomous platform for handling hidden orders without the need to privately disclose those orders to a trusted third party.[34]

4. Framework for When (and When Not) to Implement a Distributed Ledger

Over the last two years, more than 50,000 blockchain-based projects have materialized on GitHub,[35] a popular online repository for file sharing and source-code management. However, in the rush to implement the next biggest DAOs, the implementations and use cases in most projects seem poorly considered, with an average life span of 1.22 years and a survival rate of just 8%.[36]

In this section, we provide a business-oriented framework to assess whether the implementation of a distributed ledger is not only feasible, but also appropriate and helpful for the particular problem at hand. That is, some projects are not fit to be implemented via a system of smart contracts, and some are definitively worse off when implemented via a distributed as opposed to centralized system. We therefore highlight the main considerations in determining

[32] Levine Matt. 2015. *ITG Hid a Secret Trading Desk in Its Dark Pool.* Bloomberg, August 12. Accessed on <https://www.bloomberg.com/view/articles/2015-08-12/itg-hid-a-secret-trading-desk-in-its-dark-pool>

[33] Republic Protocol, accessed on <https://republicprotocol.com/>

[34] Brady, Dale. 2018. *Into the Dark Pool: $30 Million ICO Could Pave Way for Huge Crypto Trades,* Coindesk, February 12. Accessed on <https://www.coindesk.com/dark-pool-30-million-ico-pave-way-huge-crypto-trades/>

[35] Leal Trujillo, Jesus, Steve Fromhart, and Val Srinivas. 2017. *Evolution of Blockchain Technology,* Figure 4, Deloitte, November 6. Accessed on <https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html>. Github can be accessed at < https://github.com/ >

[36] Ibid., Figure 3.

whether a distributed-ledger protocol is an appropriate solution. **Table 1** provides a summary of the decision-making process.

4.1. Can We (Employ Smart Contracts and Implement the Project on a Distributed Ledger)?

The first and most obvious question concerns whether the project requires some method of record-keeping that will need to be continually accessed, updated, and verified. Assuming it does, the next consideration is whether the transactions being recorded can be verified and implemented automatically and electronically via a system of pre-determined rules. For instance, the transfer of digital assets can easily be verified and implemented electronically, and even the transfer of rights to physical property can be verified and executed electronically (even if the property itself must change hands physically).

However, problems requiring more complex transactions, particularly those involving contracts that are inherently incomplete, are ill-suited for this modality. LegalFling,[37] a project attempting to record sexual consent on a blockchain-based ledger, is one such example. That is, consent in this arena is a nebulous, retractable, and often contentious concept, and the vast array of possibilities for what that consent entails is difficult to package in a simple set of automated rules.

4.2. Should We?

Once we have established that we *can* implement our project on a distributed ledger based on a system of smart contracts, the next set of issues to consider relates to whether we *should*. That is, a distributed system of record-keeping requires far more resources than maintaining a centralized ledger with a trusted intermediary. Thus, we must assess what, if anything, is to be gained from

[37] Legal Fling, accessed on <https://legalfling.io/#about-us>

decentralization, and whether the benefits outweigh the costs inherent in a distributed system. We highlight four key considerations along this regard.

1) Does the integrity of a new transaction record depend on prior transactions (e.g., is double-spending a concern)? That is, the last known state is an important record to check in verifying transactions involving exchanges of limited assets (e.g., BTC). However, if the last known state can neither confirm nor deny the integrity of the latest transaction (as in our prior example regarding consent), a ledger may not serve much purpose, let alone a distributed ledger replicated and maintained across multiple systems.

2) Does the project require read/write access by more than one system? If not, transaction records can be kept on a single centralized ledger.

3) Do we trust all writers, or can we use a trusted third party to maintain transaction records? Areas rife with distrust present the most promising projects for decentralization, given that a leaderless DAO does not have its own opportunistic or potentially nefarious agenda that a company might (e.g., a problem inherent in dark pools, which Republic Protocol[38] seeks to address). Conversely, the same inherent mistrust does not exist in the exchange of rights to photo licensing. Thus, a simple platform with a trusted intermediary is more efficient for this purpose than a decentralized platform with its own native token, as is the case with KODAKCoin,[39] which is currently under development.

4) Is privacy of transaction records a concern? Finally, once we have determined that a distributed ledger is both feasible and desirable, we must consider whether the privacy of the transaction records is a concern. As discussed, most public blockchains, such as BTC and ETH, show the entire transaction histories for all addresses beginning with the genesis block. Thus,

[38] See **Section 3.5**

[39] KODAKCoin, accessed on <https://www.kodak.com/US/en/kodakone/default.htm>

unless additional measures are taken to ensure the privacy of sensitive information (e.g., medical records), the use of a private, permissioned distributed ledger is preferable to one that is public and permissionless.

5. Concluding Remarks

Distributed ledgers, blockchain-based or otherwise, have quickly risen to prominence as they transform the way we verify and settle transactions without the need for a trusted third party. The rapid adoption of this technology has yielded highly innovative and useful solutions. However, it has also produced many ill-conceived projects where distributed ledgers are not only unnecessary but also detrimental.

Overall, the underpinnings and use cases of blockchains and distributed ledgers are fraught with confusion and misunderstanding. In this paper, we provide an overview of this nascent technology, we explain the basic mechanics behind distributed ledgers in general (and blockchain-based ledgers, in particular), we provide examples of recent use cases of this technology, and we provide a framework for assessing not only whether a distributed-ledger protocol is *feasible* but also whether it is an *appropriate* solution for the problem at hand.

References

BitcoinCash, Accessed on <https://www.bitcoincash.org/>

Bitcoinmining.com, *What is the Bitcoin Mining Block Reward?,* Accessed on <https://www.bitcoinmining.com/what-is-the-bitcoin-block-reward/>

Blockchain. *Average Block Size,* accessed on <https://blockchain.info/charts/avg-block-size>

Block Explorer, accessed on <https://blockexplorer.com/>

Byteball, *Smart payments made simple,* accessed on <https://byteball.org/>

Brown, Ryan. 2017. *Big Transaction Fees Are a Problem for Bitcoin – But There Could Be a Solution,* CNBC, December 19. Acessed on <https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html>

Dai, Wei. 1998. *b-money,* accessed on <http://www.weidai.com/bmoney.txt>

Dale, Brady. 2018. *Into the Dark Pool: $30 Million ICO Could Pave Way for Huge Crypto Trades.* Coindesk, February 12. Accessed on <https://www.coindesk.com/dark-pool-30-million-ico-pave-way-huge-crypto-trades/>

Dash, accessed on <https://www.dash.org/>

Demsetz, Harold. 1967. "Toward a Theory of Property Rights," *The American Economic Review* 57 (2), 347-359.

Etherscan, *Ethereum Average BlockSize Chart,* accessed on <https://etherscan.io/>

Ethereum, accessed on <https://ethereum.org/>

Github Inc., *yep / eth-tweet,* accessed on <https://github.com/yep/eth-tweet>

Github Inc., *ethereum / research,* accessed on <https://github.com/ethereum/research/wiki/Casper-Version-1-Implementation-Guide>

Halamka, John D., Andrew Lippment, and Ariel Ekblaw. 2017. "The Potential for Blockchain to Transform Electronic Health Records," *Harvard Business Review.* March 3. Accessed on <https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records>

IOTA, accessed on <https://iota.org/>

Kim, Seoyoung, Atulya Sarin, and Daljeet Virdi, 2018. "Crypto-Assets Unencrypted", Journal of Investment Management 16 (2), 1-31.

KODAKCoin, accessed on <https://www.kodak.com/US/en/kodakone/default.htm>

Leal Trujillo, Jesus, Steve Fromhart, and Val Srinivas. 2017. *Evolution of Blockchain Technology,* Figures 3 and 4, Deloitte, November 6. Accessed on <https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html>

Legal Fling, accessed on <https://legalfling.io/#about-us>

Levine Matt. 2015. *ITG Hid a Secret Trading Desk in Its Dark Pool.* Bloomberg, August 12. Accessed on <https://www.bloomberg.com/view/articles/2015-08-12/itg-hid-a-secret-trading-desk-in-its-dark-pool>

Litecoin, accessed on <https://litecoin.org/>

Lynch, Sarah N. 2017. *SEC shortens settlement cycle for securities trades.* Reuters. March 22. Accessed on <https://www.reuters.com/article/us-usa-sec-settlement/sec-shortens-settlement-cycle-for-securities-trades-idUSKBN16T1SW>

Medium, *Decoding the Enigma of Bitcoin Mining,* accessed on <https://medium.com/all-things-ledger/decoding-the-enigma-of-bitcoin-mining-f8b2697bc4e2>

MedRec, accessed on <https://medrec.media.mit.edu/>

Monero, accessed on <https://getmonero.org/>

Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System,* accessed on <https://bitcoin.org/bitcoin.pdf>

Neo, *Neo White Paper,* accessed on <http://docs.neo.org/en-us/>

NEO, accessed on <https://neo.org/>

Presscoin, accessed on <https://www.presscoin.com/>

Republic Protocol, accessed on <https://republicprotocol.com>

Ripple, *XRP The Digital Asset for Payments,* accessed on <https://ripple.com/xrp/>

Ripple, *The XRP Ledger Consensus Process,* accessed on <https://ripple.com/build/xrp-ledger-consensus-process/>

Szabo, Nick. 1997. "Formalizing and Securing Relationships on Public Networks," *First Monday* 2 (9).

Szabo, Nick. "Bit gold", Accessed on <https://unenumerated.blogspot.com/2005/12/bit-gold.html>

tZERO, accessed on <https://www.tzero.com/>

Ubitquity, accessed on <https://www.ubitquity.io/web/index.html>

Waves, accessed on <https://wavesplatform.com/>

Appendix A.
Glossary of Commonly Used Technical Terms with Corresponding Definitions

Blockchain
A continuously growing chain of transaction records, grouped into *blocks*, which provide the technical foundation on which most cryptocurrencies are currently developed and maintained. A *public* blockchain is a decentralized, permissionless system maintained by the collective masses. In contrast, a *private* blockchain is maintained by a centralized group of permissioned users.

Cryptocurrency
A digital asset predicated on a system of smart contracts that are designed to oversee coin supply and verify settlement and transfer of funds.

Decentralized Autonomous Organization (DAO)
A leaderless enterprise designed to operate autonomously based on a system of open-source smart contracts.

Distributed Ledger
A record-keeping system that is replicated and maintained across multiple users or nodes.

Double Spend
An accidental or malicious attempt to use the same token(s) in more than one transaction.

Hard Fork
A major change in the consensus protocol that is not backward-compatible and causes a split in the blockchain, resulting in in two separate cryptocurrencies.

Horizontal Scalability
The ability to maintain security and quality while increasing the capacity of users or nodes on the network.

Proof of Work
A system requiring a computationally difficult measure that is time consuming to find or produce, but easy to verify once found.

SHA-256
A cryptographic hash algorithm that, for any given input, generates a 256-bit (64-character) alpha-numeric hash code, also known as the checksum.

Soft Fork
A software update designed to be backward-compatible to maintain the original blockchain without a split.

Smart Contract
A program or protocol designed to verify and enforce a system of pre-determined rules.

Figure 1
Simple Blockchain Implementation

This figure graphically depicts the record-keeping process of a simple blockchain, whereby the contents of each block are passed through the SHA-256 function to form the hash code which constitutes the first element of the subsequent block. The bottom figure depicts an attempt to alter past transaction records in a closed block, which yields a new hash code that does not conform with the original hash code recorded on the subsequent block.

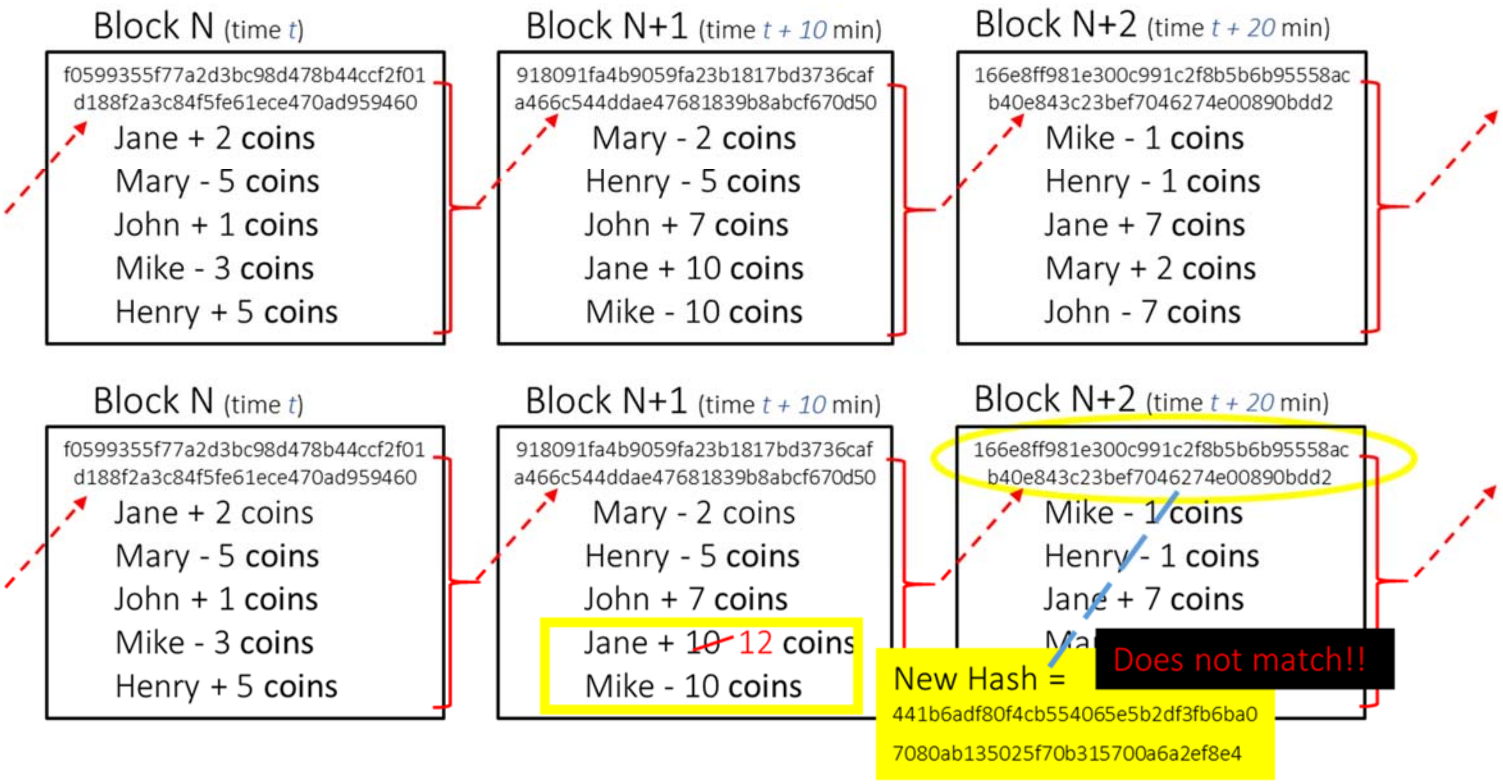
Block N (time t)
f0599355f77a2d3bc98d478b44ccf2f01
d188f2a3c84f5fe61ece470ad959460
Jane + 2 coins
Mary - 5 coins
John + 1 coins
Mike - 3 coins
Henry + 5 coins
Block N+1 (time t + 10 min)
918091fa4b9059fa23b1817bd3736caf
a466c544ddae47681839b8abcf670d50
Mary - 2 coins
Henry - 5 coins
John + 7 coins
Jane + 10 coins
Mike - 10 coins
Block N+2 (time t + 20 min)
166e8ff981e300c991c2f8b5b6b95558ac
b40e843c23bef7046274e00890bdd2
Mike - 1 coins
Henry - 1 coins
Jane + 7 coins
Mary + 2 coins
John - 7 coins
Block N (time t)
f0599355f77a2d3bc98d478b44ccf2f01
d188f2a3c84f5fe61ece470ad959460
Jane + 2 coins
Mary - 5 coins
John + 1 coins
Mike - 3 coins
Henry + 5 coins
Block N+1 (time t + 10 min)
918091fa4b9059fa23b1817bd3736caf
a466c544ddae47681839b8abcf670d50
Mary - 2 coins
Henry - 5 coins
John + 7 coins
Jane + ~~10~~ 12 coins
Mike - 10 coins
Block N+2 (time t + 20 min)
166e8ff981e300c991c2f8b5b6b95558ac
b40e843c23bef7046274e00890bdd2
Mike - 1 coins
Henry - 1 coins
Jane + 7 coins
Ma
New Hash =
441b6adf80f4cb554065e5b2df3fb6ba0
7080ab135025f70b315700a6a2ef8e4
Does not match!!

Table 1
When to Implement a Distributed Ledger

This figure graphically depicts the process in determining whether a distributed ledger is not only a feasible, but also an appropriate, record-keeping solution for the problem at hand.

		Implement Verification Protocol via Smart Contracts on a….		
	Smart Contract Infeasible or Unnecessary	Simple Centralized Ledger	Private Decentralized Ledger (with Permissioned Access)	Public (Permissionless) Distributed Ledger
Are transactions simple and definitive enough to be verified and settled electronically?	No	Yes	Yes	Yes
Does the integrity of a transaction depend on prior transactions? (e.g., is double-spending a concern?)	---	Yes	Yes	Yes
Do multiple systems require read/write access?	---	No	Yes	Yes
Do we trust all writers, or can we agree upon a trusted third party to record transactions?	---	---	No	No
Is privacy of transaction records a concern?	---	---	Yes	No[1]

[1] We note that privacy can still be maintained on public blockchains via newer methods currently employed by so-called *privacy coins*, such as DASH and Monero, as mentioned in **Section 3.1**.