Beyond the Buzzword: Demystifying Blockchains

Sophia Buehrer, Nathaniel Lovin, Mahdi Mohamed, Benjamin Stone, and Kiran Tomlinson
Department of Computer Science
Carleton College, Northfield, MN 55057
{buehrers, lovinn, mohamedm2, stoneb, tomlinsonk}@carleton.edu

***Abstract*—In recent years, blockchains have received significant interest in public, academic, and business circles. However, few sources provide clear and accurate information on either the technical details or practical uses of this data structure. In this paper, we outline the core goals of blockchains, analyze their flaws, and examine some of their most influential and promising applications. To begin with, we discuss the issues inherent to any blockchain-based system, including security, privacy, and environmental considerations. We conclude that the extensive history of attacks on blockchains casts doubt on any guarantees of their security. Furthermore, the most popular proof system for supporting blockchains, proof-of-work, is energy-intensive and wasteful. While alternatives to proof-of-work exist, only time will tell if these can be successfully adopted without further detriment to blockchain security. In the context of these overarching difficulties, we weigh the potential of three important blockchain applications: cryptocurrencies, smart contracts, and supply chain tracking. Regarding cryptocurrencies, we conclude that the benefits of eliminating trusted third parties must be balanced against economic volatility and the possibility of inherent flaws in the blockchain protocols. Turning to smart contracts, we argue that their current uses are relatively inconsequential and that expanding smart contracts to a larger scale seems infeasible. On the other hand, we consider supply chain management to be an area in which blockchains directly solve existing problems and have potential to completely rework current tracking infrastructure. Overall, the widespread fervor for blockchains should be tempered by cautious exploration, as there are only a few areas that demonstrate concrete improvement over existing data structures.**

***Index Terms*—Blockchain, cryptocurrency, smart contract.**

I. Introduction

Blockchains are unique among data structures in their power to attract adamant supporters, spark heated debates, and drive investment by their mere presence. Even in technical circles, the strengths and weaknesses of blockchains remain poorly understood. In this paper, we aim to give the reader an understanding of the reality underlying the blockchain craze. Synthesizing a wide variety of academic and technical sources, we describe how blockchains fail and where they may succeed.

Before beginning our analyses of the potentials and pitfalls of blockchains, we first need to define their purpose and goals to provide a metric under which we can evaluate them. Blockchains, sometimes called distributed ledgers, are designed to store data about the interactions between mutually distrusting parties that each have something to gain by modifying the data. Additionally, blockchains are founded on the premise that third parties like banks and governments should not be trusted with this data. In order to accomplish these goals simultaneously, we want the data structure to be decentralized, immutable, transparent, and incentive-compatible.

First of all, when we say that a data structure is *decentralized*, we mean that no single entity has complete control over its contents. Instead, the responsibility of maintaining the data is distributed over a large network of equal peers. Secondly, in this context, a data structure is *immutable* if information added to it can never again be changed. This is a desirable property of a ledger, which should contain an unmodifiable account of historical data. Next, blockchains are *transparent* in that everyone in the distributed network can view the data contained within. Moreover, every participant is aware of any attempt to add new data to the ledger. Finally, we want this data structure to be *incentive-compatible*: it should be in everyone's best interest to be an honest and productive member of the network. In a similar vein, network members should be disincentivized from breaking the rules and corrupting data.

These are the four core tenets of blockchains. Beyond these, there are some additional attributes often ascribed to the data structure, namely privacy, anonymity, and security. In this paper, we will discuss the extent to which blockchains achieve these goals, both in the context of specific applications and more generally. Before doing so, we will provide a brief overview of blockchains to remind our reader of their origins, structure, and public perception, each of which is vital to a full understanding of the data structure. In addition, we will describe our methods for collecting and interpreting the materials that informed this paper.

A. Blockchain Overview

Blockchains were first proposed in a 2008 paper posted online by an unknown person (or persons) under the pseudonym Satoshi Nakamoto [1]. This paper outlined a new digital currency, Bitcoin, that was claimed to have all of the properties described above: decentralization, immutability, transparency, and incentive-compatibility. Bitcoin was based on a new data structure consisting of a sequence of discrete chunks of data linked by cryptographic hashes—a chain of blocks.

We assume that our readers have a general understanding of blockchains. However, it is worth providing a reminder of important terms that will come up throughout this paper. A blockchain is composed of blocks that store data. The type of data depends on the application, but represents the most important part of a block. Every block also contains the hash of the previous block, which is what links blocks together and prevents them from being easily modified. The operation and maintenance of a blockchain requires a network of connected peers, often called nodes. These nodes propagate incoming data to the rest of the network and include that data in the next block they are mining. Nodes mine new blocks by completing a proof that they have invested resources in the creation of the block (typically through proof-of-work). Once a block has been mined, it is added to the blockchain and shared throughout the network.

A surprising amount of public attention has been paid to this rather abstruse computer science concept. Blockchains have even been touted as the solution to many of the world's problems in popular books with titles such as "Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World" [2] and "The Truth Machine: The Blockchain and the Future of Everything" [3]. The excitement around blockchains is perhaps most visible in its ability to motivate investment. In late 2017, the company formerly known as Long Island Iced Tea changed its name to Long Blockchain Corp. and its share prices skyrocketed by almost 300%, despite the fact that they still only made iced tea and lemonade [4]. (Long Blockchain Corp. is now under investigation by the Securities and Exchange Commission [5].) Other examples of the blockchain craze abound, from blockchain-powered dating apps [6] to multi-billion dollar Ponzi schemes [7]. On the other hand, many smart and technically-minded people are convinced that blockchains are the next big thing. The central goal of this paper is to disentangle fact from fiction and provide a clear, unbiased overview of blockchains and their potential.

B. Methods and Sources

There is an extensive amount of literature on blockchains, both popular and academic, ranging from proposed applications to discussions of existing vulnerabilities. We decided to focus on academic papers published in journals and conferences, technical reports, and white papers (which are often used to describe new blockchain implementations). In choosing papers to read, we emphasized peer-reviewed articles that had been well cited, with allowances for recent publications. We also sought to determine possible author biases, as many individuals engaged in blockchain research have conflicting financial interests.

The authors of this paper are senior Computer Science majors at Carleton College who compiled this information as part of a comprehensive project that is an integral part of the major. Our opinions have been formed as a result of six months of research and discussion. None of the authors are affiliated with or invested in any blockchain companies. We have sought to approach the subject both fairly and critically, without falling prey to either pro- or anti-blockchain fanaticism—both of which are rampant in online sources and popular books.

In the rest of the paper, we will first address blockchain security, privacy, and energy use, which are relevant to all blockchain applications. Then, we will analyze three of the most popular and promising blockchain applications: cryptocurrencies, smart contracts, and supply chain tracking. For each, we will examine how well blockchains achieve their core goals in that context and evaluate the viability of the application.

II. Security

In any discussion of the long-term viability of blockchains, security must play a central role. Any widespread adoption of blockchains would be contingent on settling the debates over the existence of inherent vulnerabilities in the blockchain protocols. Although blockchain proponents argue that the incentive structure prevents or minimizes the damage hostile actors can do, others make the case that current protocols remain fundamentally insecure. We will bring up examples of attacks both against the blockchain protocol itself and against the mechanisms used to interact with blockchains. Although blockchains seem to be resilient to some of these attacks, others, such as selfish mining, appear to successfully manipulate the incentive structure to an attacker's advantage. Beyond those flaws, users need a variety of tools to make use of blockchains. These tools bring with them the potential for conventional software security flaws. This means that even if blockchains are demonstrated to be completely secure in a theoretical sense, end-users may not be able to take full advantage of that security.

A. Immutability of Blocks

The key aspect that allows nodes in a blockchain network to trust the contents of a block without having to trust each other is that those blocks are immutable once they are added to the blockchain. Once a user gains the ability to change the contents of a block on the blockchain, the validity of the contents of every subsequent block is comprised, rendering the entire blockchain useless.

Blockchains use methods like proof-of-work to make blocks difficult to modify. The two key features that allow these algorithms to achieve this is that users must commit significant resources in order to add a block, and each new block must contain the hash of the previous block. The cost of adding a new block discourages malicious actors because it randomizes who gets to add a new block each time, effectively giving all users an equally low probability of being able to add a new block. If a user changes the contents of a block, this results in a new hash. Because the old hash is linked to in the next block, that block's hash will also change, meaning the attacker will have to update every subsequent block in order for that change to be accepted. Considering that the rest of the network is working on the unmodified version of the blockchain, this malicious actor will likely never catch up.

B. 51% Attack

The only way to successfully change the contents of a block is if an attacker can coordinate at least 51% of the hash power of the network to work on building their modified version of the blockchain. Every single blockchain is susceptible to a 51% attack. Smaller blockchains tend to be the most vulnerable. For example, Monacoin, Bitcoin Gold, Zencash, Verge, and Litecoin Cash were victims of 51% attacks in 2018 alone [8]. This shows that when new (and perhaps even improved) proof-of-work blockchains are released, we should be wary of trusting them if they have not been widely adopted.

In theory, once a network gets a sufficiently large number of users, such coordination should become too hard for this attack to be a serious threat. This might lead us to conclude that larger and more mature blockchains are more secure. However, this ignores the formation of mining pools. As the number of miners increases, the probability that any one of them is able to add a block diminishes. This then incentivizes miners to join mining pools in order to decrease the variance in their rewards. These large pools, however, make blockchains both more centralized and less secure. For example, Bitcoin's top five mining pools control 55.5% of network's hashing power in March 2019 [9]. So even the largest blockchain network is susceptible if a few mining pools go rogue. Considering how large these pools are, and that most of their miners are honest, the probability that any of these mining pools would actually attack is very low. The only entity capable of conducting a 51% attack on a large network like Bitcoin would be a nation-state, so until that happens, sufficiently large blockchain networks are likely secure against these attacks.

C. Selfish Mining Attack

The main way blockchains incentivize nodes to mine blocks is by paying these nodes for their work with a fixed amount of a cryptocurrency for every block they mine and add to the blockchain. This incentivizes nodes to share a block as soon as they mine it, so their block gets accepted before any other block. In a selfish mining attack [10], certain miners try to game the system and increase their proportion of the rewards by keeping a block private after mining it. They then get a head start on mining the next block. If another miner mines a block, they broadcast the block they already mined to compete with it. The rest of the network chooses which block to add the blockchain, and if the attacker's block get adopted by the majority of nodes on the network, they get the reward. Meanwhile, the attacker stays ahead of the rest of the network by continuing to keep private all the subsequent blocks they mined, while the rest of the network wastes their resources mining already mined blocks. This process allows the selfish miners to waste the resources of other miners and get proportionally more rewards if they control at least 25% of the network's hash power. Other nodes are then incentivized to join the selfish mining faction, causing it to grow until it has a 51% majority, at which point the system is fully compromised. Furthermore, in blockchains that use transaction fees instead of block rewards, a more sophisticated selfish mining strategy guarantees disproportionate rewards with any amount of mining power [11].

However, selfish mining is easily detectable, so it has not been especially prevalent. Only Monacoin appears to have suffered a selfish mining attack, in May 2018, which resulted in about $90,000 in losses [12]. Nonetheless, the selfish mining attack reveals that there may be subtle flaws in the blockchain protocol itself that are not intuitively apparent. The simple existence of an attack like this means that claims of blockchain incentive-compatibility are dubious at best.

D. Attacks on Wallets and Exchanges

Furthermore, even the largest and most secure blockchain protocol requires users to interact with it through third-party tools. The main blockchain-related attacks exploit failures of these tools, especially wallets and cryptocurrency exchanges. The most popular third-party blockchain applications are hot wallets, which are online applications used to store private cryptographic keys, and cryptocurrency exchanges, which are used to trade a cryptocurrency for a another cryptocurrency or a fiat currency. The biggest hacks have been against hot wallets owned by online cryptocurrency exchanges. This was the case for the exchange Coincheck, which in January of 2018, had $500 million worth of the NEM cryptocurrency stolen [13]. In 2018 alone, there were six exchange hacks totaling in a loss of $865 million [14]. The amount stolen from all exchange hacks ever adds up to $1.5 billion [14].

Prior to the Coincheck hack, the largest exchange hack happened to Mt. Gox. By 2013, Mt. Gox processed about 70% of Bitcoin transactions [15]. The company was not transparent about its poor security procedures and had between 2010 and 2014 routinely shipped bug-riddled code [16]. Hackers were able to steal 850,000 Bitcoin, worth more than $460 million [16]. The main takeaway is that these online wallets are not secure. They should not be used for long term storage of private keys; hardware cold wallets from reputable manufacturers are considerably more secure.

III. Privacy

Beyond the basic security of blockchains, one of the central goals of many blockchain applications has been to ensure privacy and anonymity for their users. On one hand, this allows criminal enterprises to make use of these anonymized platforms for illicit financial activities. However, a desire for privacy and anonymity is a perfectly reasonable one, especially given recent revelations surrounding the amount of data large corporations collect and share about their users. In this section, we briefly discuss how blockchains can protect anonymity and then analyze ways in which this can fail.

A. Anonymity

Blockchain protocols attempt to anonymize users through the use of public key cryptography for authentication. This allows users to conduct transactions without having to reveal information about their identity. Cryptocurrencies like Bitcoin and Monero are notorious as the payment method of choice for those conducting illicit activities on the dark web, further cementing the public perception that blockchains are anonymous. Decentralized public blockchains, however, prove to be only pseudonymous at best. Blockchains keep a distributed public record of every single transaction every made, and every key pair involved in a transaction is linked to a fixed wallet address. The are multiple blockchain explorer applications like blockchain.com [17] that allow anyone to view every transaction in every block, what wallets were involved, and all other transactions in which that wallet has participated. Once a person's pseudonym (key or address) is connected to their real-life identity, the blockchain then becomes a public record of that person's entire transaction history.

B. Deanonymization Efforts

Considering that people tend to jeopardize their anonymity for convenience, deanonymizing tends to be quite easy. For example, deanonymizing happens anytime the person on the other end of a transaction is aware of your real life identity. If your friend Bob pays you in Bitcoin, you can then track Bob's subsequent transactions. Also for convenience sake, a lot of people use online third-party applications like Coinbase.com [18] to store their wallets and exchange between cryptocurrencies and fiat currencies. Exchanges like Coinbase.com require users to provide their credit card and bank account information, so if you use these services, you are entrusting your anonymity in their hands.

Governments also have plans to use this abundant and permanent source of information to track anyone. Currently, Russia and China have task forces in place monitoring foreign and domestic exchanges in order to build profiles of accounts that are suspected of belonging to individuals who they consider criminals [19]. The United States has taken it a step forward by going around exchanges completely. Documents acquired by Edward Snowden indicate that the NSA has developed a program called OAKSTAR that can "extract raw internet data from fiber-optic cables in order to identify the IP addresses and IDs of those sending and receiving Bitcoin" [19]. The program is disguised as a VPN that has been downloaded by approximately 16,000 users in countries spanning the globe. [19]. Also in 2016, the IRS subpeonaed Coinbase.com, forcing them to provide the identities of individuals who use their services [19]. This further indicates the US government's ability to both track activities on blockchains and connect users to their real life identity. In addition, research has shown that it is possible to deanonymize Bitcoin users by exploiting the network protocol directly, taking advantage of how transactions are broadcast [20].

C. Protecting Anonymity

There are several ways to make tracking harder, but each comes with its own set of drawbacks. One option is to generate a different public and private key pair for every transaction and keep them in several wallets. The downside to this is that you need to keep track of more key pairs. Moreover, whenever you conduct a multi-input transaction, the outgoing transaction will include multiple addresses as inputs, proving that their wallets belong to the same entity. Another option is to use a mixing service, which randomly trades your coins with other coins, making it impossible to determine the original history of the coin you get back. The downside this system is that it requires users to trust a third party to both give return coins, and not keep a record transactions that flow through them.

A promising solution to staying anonymous is using secure coins. The most popular secure coin is Monero, which does not store public address on the blockchain. Instead it hides the amount transferred in a transaction and obfuscates which user a transaction is coming from [21]. Yet several vulnerabilities exist in Monero's approach, which involves "mixing the coin someone spends with a sampling of other coins used as decoys known as 'mixins'" [22].

Initially, Monero allowed users to conduct transactions without using mixins [22]. This meant that later on when these previously identified coins were used as mixins, they could easily be identified and used to identify the rest of the coins. Then, if any of those coins were used as mixins, they then could be used to identify those other coins, continuing the cycle of deanonymization.

As of February of 2017, Monero is now requiring that every user includes at least four mixins in each transaction, but transactions prior to this date are still vulnerable [22]. In fact, many early adopters of Monero, believing in the coin's privacy features proceeded to conduct transactions for illicit goods. For example, the dark-website AlphaBay began using Monero in July 2016, so any transactions conducted on the site between July 2016 and February 2017 could be deanonymized [22]. This goes to show that any privacy feature is always at risk of a new deanonymizing method being discovered and then being retroactively used.

Another vulnerability that still plagues Monero privacy claims is that even when a coin is mixed, the real coin tends to be the most recent coin in that transaction. This timing analysis allowed researchers to correctly pick out the real coin from the fake coins 90% of the time [22]. Monero has since changed how it manages mixins, but timing analysis can still distinguish the real coin from fake ones about 45% of the time [22]. Monero's spokesperson response to these challenges was "privacy isn't a thing you achieve, it is a constant cat-and-mouse battle," [22] which nicely sums up the state of privacy on the blockchain. Despite Monero's claims, this demonstrates that their privacy guarantees cannot be taken at face value. The safest approach is to assume all activity can be and will be tracked, so conduct business on the blockchain accordingly.

IV. Energy and Environment

Moving past the privacy and security aspects of blockchains, we will discuss the proof-of-work protocol, its environmental costs, and possible substitutes. As proof-of-work remains widely used in the largest blockchains, an analysis of its shortcomings gives additional perspective on applications that depend on it.

A. Proof-of-work

Proof-of-work is the proof system first proposed for use with blockchains [1], but is it really the best proof system moving forward? While proof-of-work is the most commonly used proof system in blockchain applications, there is continuing debate on whether or not it is environmentally sound. Proof-of-work was originally designed in order to prevent large amounts of spam emails being sent at once [23]. The system would not affect normal usage of email, but would make it difficult for anyone to send out millions of emails at once [23]. However, when translated to applications such as Bitcoin, or other large scale projects, problems start to appear. Dziembowski et al [23] argue that Bitcoin's use of proof-of-work constitutes an environmental hazard and note that with the right hardware, it is possible to complete the proofs with much less time and energy than intended [23]. This argument is also made in papers not advocating for their own alternative to proof-of-work, such as [24] and [25].

If proof-of-work were to be adopted on an even larger scale than it currently is, this could pose very real environmental problems, given the amount of energy it consumes. Though the actual energy figures are unclear, people have attempted to calculate emissions and environmental impact of proof-of-work. Carbon dioxide emissions related to proof-of-work have been estimated at $6.10 \cdot 10^{11}$kg per year [26]. To put this in context, in 2009, the total carbon dioxide emissions from fuel consumption were about $2.90 \cdot 10^{13}$ [26], making emissions from proof-of-work about 2.1% of the total. It has been further estimated that Bitcoin mining alone takes up 0.14% of the world's energy consumption [25]. The main cost of bitcoin mining is in fact the associated energy cost [24] of proof-of-work. Energy estimates for Bitcoin are widely variable, ranging from about 10MW (the equivalent of a power plant's output) to 3-6GW (the total consumption of Denmark) [24]. The calculation put forward in [24] puts 45MW as a minimum, with 100-500MW being the most realistic total output. Per year, this comes out to be 3-16PJ [24]. Vranken states that this is less than the current energy use of the banking and gold industries [24]. However, since banking and gold are industries that are far more useful and active, this is not a fair comparison. The energy used by proof-of-work blockchains is significant, especially given the relatively short period that they have existed and the relatively small-scale adoption of Bitcoin. While some may be of the opinion that energy is not a concern at this moment, it would certainly become one if the use of proof-of-work blockchains expands.

B. *Alternatives*

Since proof-of-work is wasteful, people have begun to look into other ways of completing the proof stage of the blockchain protocol. The most common alternatives are proof-of-stake and proof-of-space. While they might be able to replace proof-of-work, it is not entirely clear whether their low energy consumption makes up for their other drawbacks.

The concept behind proof-of-work is that energy—often quantified by CPU output—must be spent in order to publish a block. It is possible to use other resources in this step, such as disk space, as in proof-of-space [23]. This method requires storage space to be set aside during set-up, which is later verified in order to confirm that mining has taken place properly. The argument for proof-of-space is that everyone has extra unused disk space, thus removing the need for the specialized hardware that has emerged in response to the processing power requirements of proof-of-work. However, there are issues associated with the protocol—a malicious actor could potentially delete the data file after receiving it from the verifying party. This can be mitigated, but is an issue to consider [23]. Proof-of-space also presents environmental issues of its own. If hard drive space is used as a resource in the process, then the demand for drives would result in a waste of physical resources and the energy used in their manufacture.

Proof-of-stake is another possible alternative to proof-of-work. Proof-of-stake assumes that because each person in the network is invested in the venture, that they have a vested interest in keeping the mining process going. Thus under proof-of-stake, the more someone invests in a network, the more likely they are to get to mine the next block in the chain. This is accomplished by randomly choosing a node to be the next miner with probability proportional to each node's wealth [27]. Proposed benefits of proof-of-stake schemes include that it may be a lot more difficult for a potential attacker to get enough currency to take control of the network. The incentive for continuing to use a proof-of-stake blockchain is that by participating, each node invests in the continued health of the system. Another possible benefit is that there is no need to take up any real resource—there is no need for specific hardware with proof-of-stake [28]. However, there are of course some potential drawbacks to proof-of-stake as well. These include the rich-get-richer effect, making sure that initial distribution of currency is fair, discouraging forks (the nothing-at-stake problem), finding ways of dealing with malicious nodes [27], and creating rewards encourage participation in the system [29]. Like proof-of-space, proof-of-stake proposes a way around the energy consumption issue, but it does not seem any more secure than proof-of-work, especially since it relies on miners having some degree of collaborative spirit. While the investment model may keep most miners working in a non-malicious way, there is no way to guarantee this.

Though many protocols for replacing proof-of-work exist, it is hard to say whether they would be any better when used on a large scale. Proof-of-stake is vulnerable and its security and stability are questionable [27]. Proof-of-space also has security issues [23] and have its own potential environmental concerns. So while proof-of-work is environmentally wasteful, the alternatives are far from convincing.

V. Cryptocurrency

Satoshi Nakamoto's original Bitcoin white paper begins by setting out the need for an electronic payment system that does not depend on a trusted third party. According to cryptocurrency proponents, removing trusted third parties leads to decreased fraud and easier transactions as merchants would not need as much information from buyers [1]. The entire cryptocurrency ecosystem is based around these hopes and promises. Do they pan out?

A. Proponents' Case

There are many reasons why people might support a decentralized currency, such as privacy concerns and changing the power structure. But why does this need to be a separate currency instead of just a system for sending cash via the internet? At least part of it is a worry about the replacement of hard money (for example, the gold and silver standard) with fiat money (money created at the will of the government). With fiat money, according to this story, comes hyperinflation and the debasement of the currency due to government malfeasance or poor management [30], [1]. While these issues have not hit the United States and post-War Europe yet, according to this view it is inevitable that they will after events like the Great Recession and Quantitative Easing. This can be seen with Nakamoto's coinbase for the genesis block "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks," suggesting a looming collapse of the pound [31].

Bitcoin, and most cryptocurrencies based on its implimentation, are thus planned to be inherently deflationary—a fixed amount of coins are available at any time, growing at a fixed rate or not at all, and if more transactions are to be conducted, the value of the coin goes up. Since the money supply is controlled by code and not central bankers, it cannot have hyperinflation or be debased.

This causes an issue though, since if money is predicted to be worth more tomorrow than today, what incentive is there to spend it today?

B. Bitcoin

Bitcoin is the main crytocurrency in use, with a market share around 52% [32]. Bitcoin has several contrasts with existing currencies. A Bitcoin block is mined on average every ten minutes. Since Bitcoin's formation there have been over 380 million transactions conducted on the platform [17]. This number pales in the face of payment systems like Visa, which processes around 300 million every 48 hours [33]. Part of the reason for the small amount of transactions is the 1 MB limit on transactions in a given block. In an effort to combat this and allow for more transactions, a fork of the Bitcoin blockchain was made in 2017, forming a new cryptocurrency, Bitcoin Cash [34], with an 8 MB limit. However, this has been unsuccessful—Bitcoin's price remains much higher, and still has substantially more transactions than Bitcoin Cash. From November 2018 until March 2019, only 9 blocks in Bitcoin Cash's chain used the extra transaction space [35]. This is weak evidence that most people are holding Bitcoin and cryptocurrencies as an investment vehicle, hoping they increase in value, instead of being exchanged for goods and services.

Remittances—money being sent by immigrant workers back to their home country—are a use case for cryptocurrency widely being considered. There are two ways Bitcoin could be better than the existing system. Either it allows for remittances between countries where there are legal issues with transferring money, or it is cheaper or faster than the current money transfer system. In the first case, there are enough ways to block and deanonymize Bitcoin transactions that if a country wanted to prevent the transfer of money Bitcoin's pseudonymity would not be enough to stop it. For the second case, it is clear that Bitcoin is much slower than the leading payment processors. On the other hand, as Bitcoin transaction fees are flat (around 0.20 USD/transaction, regardless of amount [36]), they are much smaller than the fees being taken by current remittances processing, which the World Bank estimates to be about 7% of the total remittances [37]. Bitcoin could get this number well below the UN's sustainable development goal of 3% by 2030.

Despite one of the hopes of Bitcoin proponents being stability over fiat currency, Bitcoin has been noted for its instability. In 2011, Bitcoin peaked at $31 in July, before falling to $2 at the end of the year. Prices peaked at $1242 in November of 2013, before falling to $600 in December. In December of 2017, Bitcoin reached its max-to-date of $19,783, before falling to $6000 for most of 2018, before starting to fall again in November, and now hovering between $3000 and $4000 [38]. While the magnitude of the changes are not as great as the ongoing hyperinflation in Venezuela, the volatile nature makes it much harder to react to changes in the conversion rate (it is safe to assume that the Venezuelan bolívar will be worth less tomorrow and raise prices accordingly, but will Bitcoin be worth more or less?)

C. Altcoins

Alternatives cryptocurrencies to Bitcoin have attempted to solve some of the issues faced by Bitcoin. While Bitcoin comprises over 50% of the cryptocurrency market, other coins ("altcoins," for alternative coins) have been an important part of the cryptocurrency ecosystem since close to the beginning. The first significant altcoin was Litecoin, which used a different hash function (scrypt) and quartered the time between blocks to an average of 2.5 minutes [39]. In general, altcoins can be divided into four groups: copies, attempted improvements, secondary tokens, and Initial Coin Offerings (ICOs).

The first group, and the majority of altcoins, are simply copies of Bitcoin or other existing protocols in an effort to capitalize on blockchain fever. Dogecoin , for example, was a copy of Luckycoin and Litecoin, and its main purpose was to serve as a joke. Despite this, it was for a time one of the most popular altcoins, and helped raise funds for the Jamaican bobsled team [39]. The second type of altcoins consists of variations of Bitcoin, such as Litecoin [40], that aim to improve on Bitcoin on specific axes such as a different proof protocol, different block size, etc. Monero [22], for instance, attempts to improve the anonymity of using a public blockchain, while SpaceMint [29] uses proof-of-space instead of proof-of-work.

The third category is tokens and coins whose currency use is secondary. These coins come in two forms. They can be functional—Ether is needed to run the smart contract platform Ethereum (see next section)—or purely an incentive to mine the associated blockchain. Namecoin [41], an attempt to put

DNS on a blockchain, needed a coin to incentivize miners to place the DNS info on the chain. Without an external use for the coin, both the price of the coin and the DNS system withered, with only a few valid addresses lasting after two years [42].

Lastly, ICOs are a way to raise capital for a business by starting a cryptocurrency and selling the first several tokens on it to the public. While occasionally these tokens are directly related to the goals of business, they often are unrelated, and exist purely to raise money for the company off the hype of blockchain. Even if the goals are related, ICOs are more like Kickstarter than IPOs, in that they do not give buyers a part of the company, but only a reward for giving the company money. The Security Exchange Commission of the US has started to crack down on ICOs that are attempting to act like securities and ICOs that appear to be scams to get money without producing a product—which is a substantial fraction of them [43].

Network effects occur when the value of an item increases as more people use it. For example, Facebook becomes more valuable when someone joins, since everyone else already on Facebook can now talk to that person. Metcalfe's law says the value of a network scales quadratically with the number of users [44]. Due to network effects, markets with many different competitors will converge to one dominant entity. In cryptocurrencies, there is clear possibility of network effects—as more people use a currency, the more people you can trade with, and so the value of your money goes up. According to a study by economists Neil Gandal and Hanna Halaburda, there are strong network effects in Bitcoins favor that increase its price and decrease the price of altcoins [45]. Indeed, many altcoins that were popular in the early part of the 2010s, like Litecoin and Peercoin, have fallen dramatically, even when compared to Bitcoin's bust [32]. Ethereum [46], which serves a slightly different purpose from other altcoins, has been taking much of Bitcoin's market share recently, however.

D. Economics

Money is defined in mainstream economics by three factors: store of value, medium of exchange, and unit of account. Cryptocurrencies as they currently exist fail to achieve most of these aims. They are poor stores of value, as their prices so far have fluctuated dramatically and unpredictably. This contrasts with fiat currencies (like the dollar or euro) which inflate slowly and mostly predictably, assuming the central bank is doing a good job, or gold or silver, which, until the late 1800s, was worth about the same amount for thousands of years. Cryptocurrencies are also a poor medium of exchange, as most cryptocurrencies are not accepted for goods and services anywhere. While Bitcoin is available for use at more places, the primary way it is used in via systems like Bitpay [47], which automatically trade Bitcoins to USD when a transaction is made, thus making it the equivalent of a Visa gift card that could randomly loose a substantial amount of its value. Due to network effects, it seems like it would be difficult for a secondary currency to get enough traction to be worthwhile. Finally, the unit of account property is a combination of the other two, and can be seen to be lacking in cryptocurrencies most clearly by the fact that the USD value of the currency is by far the most important number attached to it. Prices are not denominated in Bitcoin, but in USD and then convert to Bitcoin on the fly. No one would want to keep prices in Bitcoin, as it could make the value of the item being sold shoot up or collapse overnight.

What are cryptocurrencies being used for? 46% of Bitcoin transactions and 26% of users are associated with illegal transactions according to one estimate [48]. The total amount of illegal activity on the Bitcoin blockchain is estimated at $76 billion, in contrast to $100 billion for the US illegal drug market. While the Bitcoin number is international and including more than just drug funding, it is clear both that Bitcoin is an important part of the drug market and that drugs are an important part of the Bitcoin market. Legitimate use of Bitcoin is occurring—BitPay is used on many websites, including Wikipedia and Overstock.com—but the large amount of illegitimate use is worrying. Many legitimate Bitcoin holders do not want to spend it, for the same reason deflationary currencies are considered worrisome: why spend today when it could be worth more tomorrow? This holding, however, makes it harder for legitimate use to develop and thus for Bitcoin to gain the network effects it needs to prosper.

There are also a worrying amount of scams in the cryptocurrency ecosystem, existing to cash in on the hype. Some consist of ICOs being set up to take people's money with no intent on delivering, and possibly not even an attempt at creating any type of blockchain [39]. Others include scams promoting high returns for small initial investments that turn out to be Ponzi schemes and Twitter phishing schemes of celebrities giving away free cryptocurrencies [49]. While the scams do not remove the utility of cryptocurrency, they are import to watch out for.

If one of the hopes of cryptocurrency proponents is prevent issues related to banking failures and runs on the bank, the amount of recentralization is an issue. Most users of Bitcoin keep their Bitcoins not in their own personal wallets, but in online exchanges, which make trading between USD and BTC easier, as well as making transactions simpler [39]. However, these are just recreating some of the problems faced with banks, without the benefits like providing loans or paying interest on accounts. Multiple exchanges have failed, either due to security or business problems. Mt. Gox, which was for a time the largest Bitcoin exchange by far, went bankrupt in 2014, after losing 650,000 Bitcoin [50]. Bitfinex, Mt. Gox's successor as largest exchange, had 119,756 Bitcoin stolen in 2016 [51]. Unlike banks, accounts in these exchanges are not FDIC insured, and the owners of these Bitcoin lost their money. This is also a good example of where immutability is a negative, as if the blockchain could be changed, it would be much easier to return the lost Bitcoins.

E. Conclusion

It appears that some of the proposed benefits of Bitcoin and cryptocurrencies might be useful and achievable–lower fees on remittances, for example. Other benefits – such as the deflationary pressure – appear to not be beneficial after all. Still others appear to be unachievable by Bitcoin and other current cryptocurrencies. A reduction in fraud in the economy would be helpful, but cryptocurrencies are filled with fraud as much as any other system. The proposal of inevitable instability of fiat currency seems ironic, given the instability of bitcoin while two major sources of proposed fiat instability (the Eurocrisis and quantitative easing in the US) both passed with no major inflation or deflation periods. On the other hand, except for early adopters of Bitcoin, users of Bitcoin have had their money swing drastically in value. What value there might be for remittances, online payments, and other uses cases is hidden by that instability of the value.

VI. Smart Contracts

Among the most exciting and technically challenging applications of blockchains, smart contracts could provide a way for mutually distrusting parties to perform arbitrary interactions. At their core, smart contracts are publicly visible scripts that behave like autonomous agents: they store information and execute actions in response to events. Blockchain-based cryptocurrencies can be viewed as a special type of smart contract system with one primary action, send x units of currency to user y. Smart contracts also support more complex and event-sensitive actions. For instance, a smart contract could operate as a virtual bookie. Users could submit transactions to the contract of the form "I bet x units of currency that team y will win the game tomorrow." The smart contract would then pay out users according to the outcome, with the leftover profit sent to its owner. According to their proponents, there are boundless uses for smart contracts, including managing investment and crowdfunding [52], administering loans [53], and handling property exchanges [54].

Almost any software or platform that manages interactions between entities (human, corporate, digital, or otherwise) can be re-imagined as a smart contract. Different contracts can even communicate with each other, enabling the creation of complex distributed software. For example, contracts can act as data feeds [55], uploading and storing information about real-world events. Then, other contracts can respond to these events by querying the data feed through a transaction. As a concrete example, several bookie smart contracts could rely on the same data feed contract to inform them about the outcome of a sporting event. In this way, contracts can behave like subroutines (or sub-…-subroutines) for other smart contracts.

Furthermore, the correct execution and preservation of contracts can be enforced by storing smart contracts on a public blockchain. When a contract is submitted to the network, every node executes the contract in the process of validating that block. To interact with contracts that are already in a blockchain, participants submit subsequent transactions to the network. Under this model, we are encouraged to imagine a future in which all legal and economic interactions are handled by smart contracts, eliminating the need for expensive and inefficient intermediaries.

This vision is certainly enticing, but the ambitious claims made by smart contract supporters largely ignore the technical and structural difficulties faced by smart contract systems. To understand these difficulties, we'll start by examining the most successful and popular smart contract platform, Ethereum [46], [55]. We will then address some of the challenges faced by smart contracts in general.

A. Ethereum

Since its launch in 2015, Ethereum has been the dominant public smart contract platform [56]. Ethereum supports a distributed virtual machine with a Turing-complete instruction set, which users can interact with through the high-level language Solidity [57]. Miners in the Ethereum network are rewarded with the Ether cryptocurrency for adding contracts to the chain (a process which includes executing the contracts, as mentioned before). Smart contracts on the Ethereum blockchain are also called distributed applications, or DApps.

While Ethereum is an impressive proof-of-concept, it also highlights a multitude of issues surrounding smart contracts. The lackluster list of top DApps running on the Ethereum blockchain provides the first clue that Ethereum is not living up to its potential. In January 2019, 48 of the 50 most used DApps could be classified as online games, cryptocurrency/cryptocollectible exchanges, or gambling platforms [58]. These uses of Ethereum are united by their entirely digital nature. In contrast, examples of smart contracts given in online tutorials often involve the exchange of physical goods and services [59], [60], [61], which would open up the possibility of replacing traditional contracts entirely with their smart counterparts. Ethereum is clearly not living up to this vision of the future, a shortfall which will be more fully addressed in section VI-C.

Moreover, it is not clear that these Ethereum DApps are providing the full theoretical benefits of smart contracts. In the interest of user friendliness, the standard way to interact with one of these DApps is through an interface on their website. Realistically, no one is going to hand-write their own transaction in Solidity to buy a CryptoKitty [62] (one of the most popular cryptocollectibles on the Ethereum blockchain). Rather, a user would log into their account on the CryptoKitties website and click the "buy" button, which would then send a transaction to the blockchain on the user's behalf. This model introduces a new trusted third party, the CryptoKitties company. The user now needs to trust that the website will perform the smart contract action they request. It is unclear how this system is any better than a traditional implementation, in which the user would trust the website to store their CryptoKitties directly. Much of the appeal of these DApps is certainly tied to the mystique of doing things "on the blockchain" and the philosophy of decentralization, even if reality is not in line with these ideals.

In addition to supporting a less-than-impressive suite of smart contracts, Ethereum has also brought to light some of the challenges that any robust smart contract platform would need to be overcome.

B. Technical Challenges

The aspects of smart contracts that make them so promising also introduce significant problems. For instance, using a Turing-complete language like Solidity for smart contracts makes them highly versatile, but it also burdens them with all of the issues faced by traditional software. For instance, it is impossible to know in general whether the execution of a Turing-complete smart contract will terminate [63]. In a blockchain network, non-terminating contracts are a serious issue, since every contract in a block must be run before declaring the block valid. This problem can be dealt with by setting a limit on the running time of a contract, but this only addresses a small instance of a more general problem; namely, that it is impossible to know with certainty that a contract will perform its advertised action. While inspecting its code can provide some degree of insight into a smart contract's behavior, it is all too easy to overlook bugs, back-doors, and potential exploits.

This fact was brought to the fore by an infamous Ethereum hack. In 2016, investors poured an estimated $120 million worth of Ether into a new decentralized investment platform, The DAO, implemented as Ethereum smart contracts [64]. A mere two months after its launch, an unknown hacker made use of a bug to siphon approximately $50 million from a smart contract operating The DAO [65]. For all the talk about smart contracts security, they are still vulnerable to simple programming mistakes. This hack led to a hard fork of the Ethereum blockchain into two versions: one in which the hacker's actions were reversed (Ethereum), and one in which the blockchain was left unmodified (Ethereum Classic). While the fork allowed the stolen money to be returned to investors, it raised questions about how decentralized Ethereum really is. In terms of the smart contract protocol, the hacker worked within the rules of the system. The siphoning was performed on the distributed network, with every node agreeing to execute the contract as written, including its crippling exploit. If the developers of Ethereum can decide what transactions they don't like and manually remove them, then why use a decentralized blockchain at all?

The hack of The DAO also highlights a second related issue. Not only are bugs and exploits difficult (or even impossible) to identify in general, but they are also very hard to fix once deployed to a blockchain. The blockchain protocol is designed to make its data as close to immutable as possible, another attribute that proves to be a liability as well as an asset. If the author of a contract discovers a bug before an attacker, they might be able to disable the contract—if it was written with that eventuality in mind. But what if the bug also affects the portion of the contract that allows it to be disabled? A rogue contract like this might only be stopped by a hard fork, like the one used in the case of The DAO. However, as we argued earlier, hard forks run totally counter to the entire purpose and integrity of the blockchain protocol.

There is likely no fully satisfying and robust solution to these problems. The moral of these stories is that as with all software, smart contracts are vulnerable to error. Moreover, the immutability of smart contracts introduces an additional obstacle when it comes to addressing bugs. These are not necessarily fatal flaws for smart contracts: similar issues exist with all software. However, we must be extremely wary of outlandishly overconfident security promises made by smart contract developers. As with any software, there is always some amount of risk in entrusting vital assets to a smart contract platform. The problem with this risk, in the case of smart contracts, is that there is likely no legal recourse if errors occur. If a bank loses your money, you have a chance of recovering it through appeals to the bank itself or to the government. If a smart contract loses your money, it may be gone forever—in a cryptographically strong sense of the word. This is exactly the issue we will address next.

C. Structural Challenges

Putting aside technical concerns, there are still substantial economic, legal, and structural obstacles to realizing the promise of ubiquitous smart contracts. The crux of the matter lies in the fact that the items being transacted by smart contracts must be entirely representable and storable in a digital system. This is why almost all existing smart contracts perform wholly digital actions, like exchanging cryptocurrencies and interacting with online games. To use a smart contract for a real estate deal, for instance, we would need some representation of real estate that can be stored in a blockchain. This is certainly plausible: we could imagine a digital token linked with the physical asset in some kind of verifiable way (i.e. the GPS coordinates or street address of a plot of land). However, this token would have to be widely accepted as proof of ownership of the land. More specifically, it would have to be legally recognized and enforced to be useful in today's sociopolitical environment.

This line of reasoning brings us back to a similar place as before; once we make smart contracts compatible with our current legal system by having them recognized and supported by a government, we lose the decentralization that is a defining tenet of the system. Perhaps the most fundamental point is that we currently live in a world arbitrated by trusted third-party intermediaries, such as juries, banks, and elected officials. In contrast, blockchain-based smart contracts are founded on the principle of decentralization and the elimination of intermediaries. The question then becomes whether generalized smart contracts are worth the effort when their primary principle is violated.

D. Summary

Perhaps there is a place for smart contracts to be genuinely useful, but it is difficult to find an example that is both practical and not already possible with traditional software or legal agreements. Although we are skeptical of claims that they will revolutionize modern society and government, smart contracts are certainly a fascinating and novel way of thinking about multi-agent interactions and software. However, the central attraction of current smart contract DApps seems to be the very fact that they are using blockchains at all. We hope that further research and development will reveal the ideal uses for smart contracts; there are likely niche proposals already that are feasible and useful, but they are certainly in the minority and do not encompass the vision of ubiquitous smart contracts.

VII. Supply Chain Tracking

Supply chain tracking is a specific instance of a DApp that has garnered widespread interest and significant investment. Modern supply chains are complex webs spreading across companies and continents, with numerous transactions coming together to provide consumers with products from around the globe. This intricacy is not complexity for its own sake, however. Economies of scale and the principle of comparative advantages mean that distributing production internationally grants enormous benefits. Large companies need to maintain global supply chains to remain competitive, but when products fail or contaminated food is sold, it becomes difficult to assign responsibility and track down the original issue. As a product wends its way between suppliers, each involved company must keep track of its own transactions, and obtaining an overview of the entire chain requires information from many different points. This problem bears significant similarities to the issue that blockchains are designed to solve: how to create a trusted record between distrusting parties. Advocates of a blockchain-based supply chain believe that it could be used to create a single distributed ledger recording transactions across all involved parties. This would replace duplicated and possibly unreliable individual ledgers maintained separately by each participant. However, due to the significant differences between a supply chain application and the purposes of the original protocol, various modifications are necessary. Current adoption of blockchains for supply chain management (SCM) is not developed enough to determine if these modifications remove or overshadow the advantages blockchains can bring.

A. Mechanics

The main difference between blockchains for SCM and blockchains for cryptocurrency or smart contracts is the participants in the network. With cryptocurrency and smart contracts, the goal is to create a decentralized, trustless environment. Anonymity is also often lauded as a benefit of blockchain technologies. However, in a supply chain setting, anonymity is not required. The goal is not to create a trustless environment among everyone who cares to join, but to create a trusted record that a group of known peers can come to a consensus on. All the participants should agree on what the distributed ledger says, but it is not necessary to hide their identity from each other. Furthermore, only certain entities are even allowed to participate. This is known as permissioned consensus. Current attempts at SCM using blockchains, such as HyperLedger from IBM [66], focus on achieving this consensus rather than creating a trustless system. Within this permissioned consensus, the transactions that appear in a cryptocurrency blockchain can be replaced by more generalized data about the products being transferred. The ledger could store information about both the source of the products and their status at every point in the process. Each hand-off from one actor to the next would be accompanied by a record and transaction saved onto a blockchain, which would create a trail to the exact point where any malfeasance occurred. Additionally, distributors could use this information to guarantee to their consumers certain characteristics of their product, such as organically grown or ethically mined.

B. Drawbacks

While traditional proof-of-work can be used for permissioned consensus, it is certainly not optimal. The issues with proof-of-work will be discussed later, but one key difficulty particular to private blockchains, such as those used for SCM, is that a 51% attack no longer requires a significant portion of the world's computing resources, but instead only requires as much computing power as that particular blockchain application has. If malicious actors are either already part of a private blockchain, or are able to gain access to it, it is very feasible to devote more computing power than any single company or group of companies has at its disposal for SCM. This represents a significant security risk that cannot be mitigated without devoting excessive resources to supply chain blockchains. Blockchains for SCM will likely require alternative proof methods, which carry their own particular security risks. Beyond the specifics of proof mechanisms, the major remaining stumbling block for blockchain-based SCM continues to be scalability. In order to become an effective substitute for existing tools, blockchain-based tools must demonstrate consistency and reliability when used on a global level. Currently used blockchains such as Ethereum and Bitcoin process only a few transactions per second (tps), with estimates placing Bitcoin between 3.5tps [67] and 7tps [68]. In comparison, VISA achieves $\sim$4000tps on average [68], several orders of magnitude higher. This gulf becomes especially significant in supply chain applications, where millions of items must be tracked and logged worldwide. Efforts to increase the transaction speed of blockchains are ongoing (such as in Bitcoin-NG [67]) and must be resolved before widespread adoption. The final difficulty with blockchain SCM returns to the privacy issue. Even within a specific supply chain there may be partitions and silos, and companies often do not want to disclose their workings and prices to their competitors. With straightforward permissioned consensus, everything is visible to all participants. Attempting to restrict this visibility takes these methods further and further from blockchains, as public visibility and a lack of read restrictions are fundamental characteristics of blockchain designs. Companies' desire to conceal their information to maintain advantages also runs counter to the attempts to verify ethical practices using blockchain SCM. Ultimately, this may be the most significant hurdle for blockchain based SCM. Time will tell if a balance can be struck between privacy and openness in this context.

C. Summary

Supply chain management has significant potential for improvement, and blockchain-based methods offer solutions to a variety of current issues. Especially in food transportation and distribution businesses, a distributed ledger offers both verifiable information on ethical sourcing and traceability in the case of contamination. This has led giants such as IBM, Maersk, and Walmart to devote considerable resources to exploring this potential [66]. If the current flaws can be mitigated, this investment could quickly lead to a future where blockchains for supply chains are common and even necessary to be competitive. In contrast to smart contracts, which have been deployed successfully on the technological side but are still searching for widespread applications, blockchain SCM has immediate and valuable uses but must first overcome a variety of technical difficulties.

VIII. Conclusions

We have analyzed the most influential blockchain implementations, addressed major proposals for future applications, and examined the challenges this data structure faces in general. In particular, we took a close look at cryptocurrencies, smart contracts, and supply chain tracking systems, with a focus on Bitcoin and Ethereum. Turning to the broader issues that blockchain systems have to overcome, we examined privacy concerns, exploits, and environmental considerations.

Our research was complicated by the fact that a substantial portion of public information on blockchains is heavily influenced by special interests. In particular, online blockchain tutorials and explanations are often written by people who have invested money in cryptocurrencies or who are affiliated with companies proposing "blockchain solutions." For this reason, it is extremely difficult to disentangle fact from fantasy when it comes to this subject. This is an unusual situation for a computer science concept—public hype is not typically an issue when discussing stacks and binary search trees. Nonetheless, we sought to provide a critical and balanced view of the current state of blockchains, both at a technical and structural level.

In terms of privacy and security, our most important takeaway is that we should be very wary of any guarantees made by blockchain companies. Indeed, "only a Sith deals in absolutes" [69]. Nearly all blockchain security promises are founded on incomplete game-theoretic intuition and the assumption that supporting protocols (such as network communications) are exploit-free. Like all software, blockchain-based applications are vulnerable to attack; the degree to which any one implementation is secure must be judged on a case-by-case basis.

Next, environmental concerns about proof-of-work energy consumption pose a challenge for the widespread adoption of blockchain systems. We think that proof-of-stake is the most promising and viable alternative so far, although existing methods for addressing the nothing-at-stake problem are more or less ad hoc. Moreover, the rich-get-richer phenomenon would need to be addressed for proof-of-stake to be equitable. A more robust and efficient proof method would certainly go a long way towards making blockchains more practical, although it is not the only weakness of current blockchain systems.

Regarding cryptocurrencies, we found that blockchains provide a truly novel way of structuring a system for monetary transactions. Blockchain-based cryptocurrencies provide some legitimate advantages over traditional currency, including some degree of decentralization and reduced international transaction fees. However, these advantages must be weighed against the technical issues surrounding wallets and deanonymization, as well as economic instability. Additionally, we emphasize that although a system may appear secure and incentive-compatible at first glance, further investigation may reveal subtle loopholes—selfish mining is a prime example.

We also argued that the vision of an economy founded solely on smart contracts is infeasible for several reasons. First of all, technical obstacles prevent generalized smart contracts from being both versatile and provably correct. Even worse, practical considerations often invalidate the trustlessness provided by smart contracts. However, we also stress that smart contracts do represent an innovation in distributed software paradigms. We are hopeful that truly useful DApps will emerge, but for now, we have to recognize that online gambling and cryptocollectible games comprise a significant fraction of the smart contract ecosystem.

Supply chain tracking is one area in which blockchains may prove to be a better fit than existing systems. By avoiding data duplication without resorting to a centralized database, corporations participating in a complex supply chain can trust that recorded data is tamper-resistant and outside the control of any one player. The current efforts to create a scalable blockchain supply chain management system show definite potential and are directed at a very real and pressing issue. It remains to be seen whether the existing technical challenges can be overcome, but if they can, blockchains will be a critical part of any supply chain.

In summary, there are many interesting facets of blockchains to be explored, but we do not believe that the technological world is experiencing a revolution. Blockchain systems face substantial and often unacknowledged challenges. it is all too easy to be swept up in the boundless enthusiasm fueled by Bitcoin's explosive rise, but we should strive to remember the stories of The DAO, Mt. Gox, and Long Blockchain Corp. At the same time, we do not wish to be overly cynical. There are genuinely useful applications of blockchains, such as tracking goods across complex supply chains—and, of course, money laundering, ransomware, and other criminal activities. We believe there is a need for further study of blockchains and their uses. In the meantime, we (and, we hope, our reader) will maintain a healthy dose of skepticism.

References

[1] S. Nakamoto. (2008) Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] A. Tapscott and D. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*, 2016.

[3] P. Vigna and M. Casey, *The Truth Machine: The Blockchain and the Future of Everything*, 2018.

[4] Z. Bernard, "When this ice tea company stuck the word 'blockchain' in its name, its stock skyrocketed by nearly 500%. Now, it's being investigated by the government." [Online]. Available: https://www.businessinsider.com/long-blockchain-company-iced-tea-sec-stock-2018-8

[5] L. Katz. (2018) Long blockchain gets hit with SEC subpoena after nasdaq ouster. [Online]. Available: https://www.bloomberg.com/news/articles/2018-08-01/long-blockchain-gets-hit-with-sec-subpoena-after-nasdaq-ouster

[6] "Looking for love? Three blockchain based dating apps." [Online]. Available: https://blockchain.wtf/2018/04/blog/looking-love-three-blockchain-based-dating-apps/

[7] Mix, "How BitConnect pulled the biggest exit scheme in cryptocurrency," Jan. 2018. [Online]. Available: https://thenextweb.com/hardfork/2018/01/17/bitconnect-bitcoin-scam-cryptocurrency/

[8] A. Hertig. (2019) Blockchain's once-feared 51% attack is now becoming regular. [Online]. Available: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular

[9] (2019) Bitcoin hashrate distribution. [Online]. Available: https://www.blockchain.com/pools

[10] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, Jun. 2018. [Online]. Available: http://doi.acm.org/10.1145/3212998

[11] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the instability of Bitcoin without the block reward," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 154–167.

[12] D. Gutteridge. (2018) Japanese cryptocurrency monacoin hit by selfish mining attack. [Online]. Available: https://finance.yahoo.com/news/japanese-cryptocurrency-monacoin-hit-selfish-205031219.html

[13] E. Cheng. (20201814) Japanese cryptocurrency exchange loses more than $500 million to hackers. [Online]. Available: https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html

[14] E. Larcheveque. (2019) 2018: A record-breaking year for crypto exchange hacks. [Online]. Available: https://www.coindesk.com/2018-a-record-breaking-year-for-crypto-exchange-hacks

[15] P. Vigna. (2014) 5 things about Mt. Gox's crisis. [Online]. Available: https://blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis/

[16] R. McMillan. (2014) The inside story of Mt. Gox, Bitcoin's $460 million disaster. [Online]. Available: https://www.wired.com/2014/03/bitcoin-exchange/

[17] (2019) Blockchain. [Online]. Available: https://www.blockchain.com/

[18] (2019) Coinbase. [Online]. Available: https://www.coinbase.com/

[19] S. Chandler. (2019) Government tracking of crypto is growing, but there are ways to avoid it. [Online]. Available: https://cointelegraph.com/news/government-tracking-of-crypto-is-growing-but-there-are-ways-to-avoid-it

[20] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 15–29. [Online]. Available: http://doi.acm.org/10.1145/2660267.2660379

[21] (2014) Monero. [Online]. Available: https://www.getmonero.org

[22] A. Greenberg. (2019) The dark webs favorite currency is less untraceable than it seems. [Online]. Available: https://www.wired.com/story/monero-privacy/

[23] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," Tech. Rep. 796, 2013. [Online]. Available: http://eprint.iacr.org/2013/796

[24] H. Vranken, "Sustainability of bitcoin and blockchains," *Current Opinion in Environmental Sustainability*, vol. 28, pp. 1–9, Oct. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877343517300015

[25] J. Truby, "Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies," *Energy Research & Social Science*, vol. 44, pp. 399–410, Oct. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214629618301750

[26] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. Bhme, "Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency," in *The Economics of Information Security and Privacy*, R. Bhme, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 135–156. [Online]. Available: https://doi.org/10.1007/978-3-642-39498-0_7

[27] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," *arXiv:1406.5694 [cs]*, Jun. 2014, arXiv: 1406.5694. [Online]. Available: http://arxiv.org/abs/1406.5694

[28] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*. San Jose, CA: IEEE, May 2015, pp. 104–121. [Online]. Available: http://ieeexplore.ieee.org/document/7163021/

[29] S. Park, A. Kwon, G. Fuchsbauer, P. Gai, J. Alwen, and K. Pietrzak, "SpaceMint: A cryptocurrency based on proofs of space," Tech. Rep. 528, 2015. [Online]. Available: http://eprint.iacr.org/2015/528

[30] A. Antonopoulos, *The Internet of Money vol 2*, 2017.

[31] T. Lee, "Five years of bitcoin in one post," *Washington Post*, 2014. [Online]. Available: https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/five-years-of-bitcoin-in-one-post/

[32] (2019) Cryptocurrencies by market capitalization. [Online]. Available: https://coinmarketcap.com

[33] (2019) Visa acceptance for retailers. [Online]. Available: https://usa.visa.com/run-your-business/small-business-tools/retail.html

[34] L. Graham. (2017) A new digital currency is about to be created as the bitcoin blockchain is forced to split in two. [Online]. Available: https://www.cnbc.com/2017/07/31/blockchain-fork-will-create-new-digital-crypto-currency-bitcoin-cash.html

[35] (2019) Bitcoin cash block explorer. [Online]. Available: https://blockdozer.com/blocks

[36] (2019) Bitcoin transaction fees. [Online]. Available: https://bitcoinfees.info

[37] W. Bank, "Remittance prices worldwide Q4 2018," *Remittance Prices Worldwide*, 2018. [Online]. Available: https://remittanceprices.worldbank.org//sites/default/files/rpw_report_december_2018.pdf

[38] (2019) Bitcoin to usd. [Online]. Available: https://finance.yahoo.com/quote/BTC-USD/

[39] D. Gerard, *Attack of the 50 Foot Blockchain*, 2017.

[40] (2011) Litecoin. [Online]. Available: https://www.litecoin.org/

[41] (2011) Namecoin. [Online]. Available: https://www.namecoin.org/

[42] H. A. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of Namecoin and lessons for decentralized namespace design," *Workshop on the Economics of Information Security (WEIS)*, 2015. [Online]. Available: http://randomwalker.info/publications/namespaces.pdf

[43] (2017) Investor bulletein: Initial coin offerings. [Online]. Available: https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings

[44] C. Shapiro and H. Varian, *Information Rules*, 1999.

[45] N. Gandal and H. Halaburda, "Competition in the cryptocurrency market," *CEPR Discussion Paper No. DP10157*, Sep. 2014. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2501640

[46] V. Buterin. (2014) A next-generation smart contract and decentralized application platform. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[47] (2019) Bitpay. [Online]. Available: https://bitpay.com

[48] S. Foley, J. R. Karlsen, and T. J. Putnins, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?" *Review of Financial Studies, Forthcoming*, 2018. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645

[49] A. Cuthbertson, "Elon Musk Bitcoin scam on Twitter sees hundreds of people lose thousands of dollars," 2018. [Online]. Available: https://www.independent.co.uk/life-style/gadgets-and-tech/news/elon-musk-bitcoin-scam-twitter-hackers-cryptocurrency-a8620436.html

[50] (2018) The history of the Mt Gox hack: Bitcoins biggest heist. [Online]. Available: https://blockonomi.com/mt-gox-hack/

[51] S. Higgins. (2016) The Bitfinex Bitcoin hack: What we know (and dont know). [Online]. Available: https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know

[52] M. Chatsko. (2018) Smart contracts and the blockchain, explained. [Online]. Available: https://www.fool.com/investing/2018/03/09/smart-contracts-and-the-blockchain-explained.aspx

[53] N. Gopie. (2018) What are smart contracts on blockchain? [Online]. Available: https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/

[54] A. Rosic. (2017) Smart contracts: The blockchain technology that will replace lawyers. [Online]. Available: https://blockgeeks.com/guides/smart-contracts/

[55] G. Wood. (2014) Ethereum: A secure decentralised generalised transaction ledger. [Online]. Available: https://github.com/ethereum/yellowpaper

[56] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: Platforms, applications, and design patterns," in *Financial Cryptography and Data Security*, M. Brenner *et al.*, Eds. Cham: Springer International Publishing, 2017, vol. 10323, pp. 494–509. [Online]. Available: http://link.springer.com/10.1007/978-3-319-70278-0_31

[57] C. Reitwiessner, A. Beregszaszi, G. Wood, and L. Karapetsas. (2015) Solidity. [Online]. Available: https://github.com/ethereum/solidity

[58] (2019) DappRadar. [Online]. Available: https://dappradar.com

[59] K. Ray. (2018) What is a smart contract? — explanation for beginners. [Online]. Available: https://coincentral.com/what-is-a-smart-contract/

[60] S. White. (2018) What is a smart contract? [Online]. Available: https://www.investinblockchain.com/what-is-a-smart-contract/

[61] R. King. (2018) What is a smart contract and how does it work? [Online]. Available: https://www.bitdegree.org/tutorials/what-is-a-smart-contract/#What_is_a_Smart_Contract_How_Does_a_Smart_Contract_Work

[62] (2017) CryptoKitties. Dapper Labs Inc. [Online]. Available: https://www.cryptokitties.co

[63] M. Sipser, *Introduction to the Theory of Computation*, 1st ed. International Thomson Publishing, 1996.

[64] R. Waters, "Automated company raises equivalent of $120M in digital currency," CNBC, May 2016.

[65] K. Finley, "A $50 million hack just showed that The DAO was all too human," Wired, June 2016.

[66] M. C. Benton, N. M. Radziwill, A. W. Purritano, and C. J. Gerhart, "Blockchain for supply chain: Improving transparency and efficiency simultaneously." ACM Press, 2018, pp. 28–38.

[67] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. Santa Clara, CA: USENIX Association, 2016, pp. 45–59. [Online]. Available: https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal

[68] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "Blockchain: The gateway to trust-free cryptographic transactions," in *ECIS 2016 Proceedings*, May 2016, p. 153.

[69] G. Lucas, "Star Wars: Episode III - Revenge of the Sith," 2005.