A use case centric survey of Blockchain: status quo and future directions

Srinath Perera, Paul Fremantle, and Frank Leymann

WSO2 Inc.

Corresponding author:
Srinath Perera

Email address: srinath@wso2.com

ABSTRACT

This paper presents an assessment of blockchain technology based on the Emerging Technology Analysis Canvas (ETAC) to evaluate the drivers and potential outcomes. The ETAC is a framework to critically analyze emerging technologies.
The assessment finds that blockchain can fundamentally transform the world. It is ready for specific applications in use cases such as digital currency, lightweight financial systems, ledgers, provenance, and disintermediation.
However, Blockchain faces significant technical gaps in other use cases and needs at least 5-10 years to come to full fruition in those spaces. Sustaining the current level of effort (e.g. startups, research) for this period of time may be challenging. We also find that the need and merits of decentralized infrastructures compared to centralized and semi-centralized alternatives is not always clear. Given the risk involved and significant potential returns, we recommend a cautiously optimistic approach to blockchain with the focus on concrete use cases.
The primary contributions of this paper are a use case centric categorization of the blockchain, a detailed discussion on challenges faced by those categories, and an assessment of their future.

1 INTRODUCTION

This document presents our assessment of Blockchain technology. It uses the Emerging Technology Analysis Canvas (ETAC) discussed by Perera (2018), which is a framework to critically analyze emerging technologies. ETAC includes questions that bring out different aspects of emerging technologies, a narrative that connects those questions to a coherent whole, and a visual representation of both. You can find more information about ETAC from https://github.com/wso2/ETAC/.

Having analyzed blockchain technology using the ETAC methodology, we make the following assertions:

- Blockchain's potential impact is both, real and transformative.
- Blockchain is ready for limited applications in use cases such as digital currency, lightweight financial systems, ledgers (of identity, ownership, status, and authority), provenance (e.g. supply chains and other B2B scenarios) and disintermediation, which we believe will happen in the next three years.
- However, blockchain faces significant challenges such as performance, irrevocability, need for regulation and lack of census mechanisms. These are hard problems and it will likely take at least 5-10 years to find answers to those problems.
- It is not clear whether blockchain can sustain the current level of effort for an extended period of 5+ years until breakthroughs occur. There are many startups and they run the risk of running out of money before markets are ready. Failure of startups can inhibit further funding and investments. For example, there is a strong correlation between investment in blockchain research and the value of various blockchain-based currencies.

- Value and need of decentralization compared to centralized and semi-centralized alternatives is not always clear, which confuses our approach to the blockchain.

- Given the risk involved as well as the significant potential returns, we recommend a cautiously optimistic approach for blockchain with the focus on concrete use cases. Investments must consider sustainability for 5-10 year horizon before significant returns.

We define blockchain as a technology that creates and maintains a shared, distributed, append-only immutable digital record that uses hash chains and operates according to a consensus algorithm

Let's consider a land registry as an example of a digital record that can be transformed with a blockchain. In a land registry, a single set of owners must own a plot of land at any given point in time, and only they can transfer it to a new set of owners; and only once. Buyers need to be able to verify ownership. Owners need to be able to demonstrate their ownership. Currently, the land registry handles these requirements through complex and expensive documents and processes executed by professional lawyers doing rigorous background checks. However, availability of a permanent digital record that can't be tampered with or disputed can replace these complex processes. The permanent and tamper-proof digital record will show the owners, and only they will be able to sell land.

In the above example, the consensus algorithm provides the agreement among participants and makes blockchain possible. Furthermore, often, blockchain based systems create incentives to attract participants to take part in the algorithm by offering coins (a token that can have value), which ensures the sustainability of the algorithm. Such participants are called miners.

Blockchains create such digital records. These digital records support many use cases such as electronic cash, ownership ledgers, lightweight financial systems, and a distributed internet. Frisby (2018) provides an excellent introduction to blockchain and its use cases.

Blockchain has received extensive attention, is often cited as one of the most impactful technologies, and has attracted many startups, venture investments, and academic research.

The rest of the document discusses the rationale for the above assertions. It follows the narrative structure introduced in the ETAC, which is used to generate analysis and conclusions. We start with the opportunity, then discuss the impact of the blockchain, followed by its feasibility. Finally, we present our assessments of blockchain future.

The primary contributions of this paper are a use case centric categorization of the blockchain, a detailed discussion on challenges faced by those categories, and an assessment of their future.

Since blockchain is applicable across a wide range of use cases, to ground the discussion, we first identify ten classes of blockchain use cases. As we discuss the impact, feasibility, and future, we consider each of these use cases separately while highlighting crosscutting concerns.

2 RELATED WORK

There have been many efforts to survey the blockchain technology. Zheng et al. (2018) is closest to our work, which provides a discussion on a wide range of applications, a taxonomy, consensus algorithms, and challenges. The primary differences are that our categorization is use case focused as oppose to the taxonomy proposed by Zheng et al. (2018) and we provide a systematic discussion on how each challenge affects use case category and asses it's future.

Same differentiations apply to the following work as well.

Yli-Huumo et al. (2016) and He et al. (2017) discusses limitations, current research, and future research directions of the blockchain.

Furthermore, Hamida et al. (2017) discusses enterprise applications and El Ioini and Pahl (2018) discusses four different blockchain implementations.

Also, there are several surveys of specific application subdomains of the blockchain. For example de la Rosa et al. (2017) discuss blockchain applications in open innovation platforms, Sternberg and Baruffaldi (2018) discusses blockchain in supply chains, Lin and Liao (2017) discusses blockchain security issues, and Panarello et al. (2018) discusses blockchain and IoT.

The primary contributions of this paper is a use case centric categorization of the blockchain, a detailed discussion on challenges faced by each category, and an assessment of each category's future.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

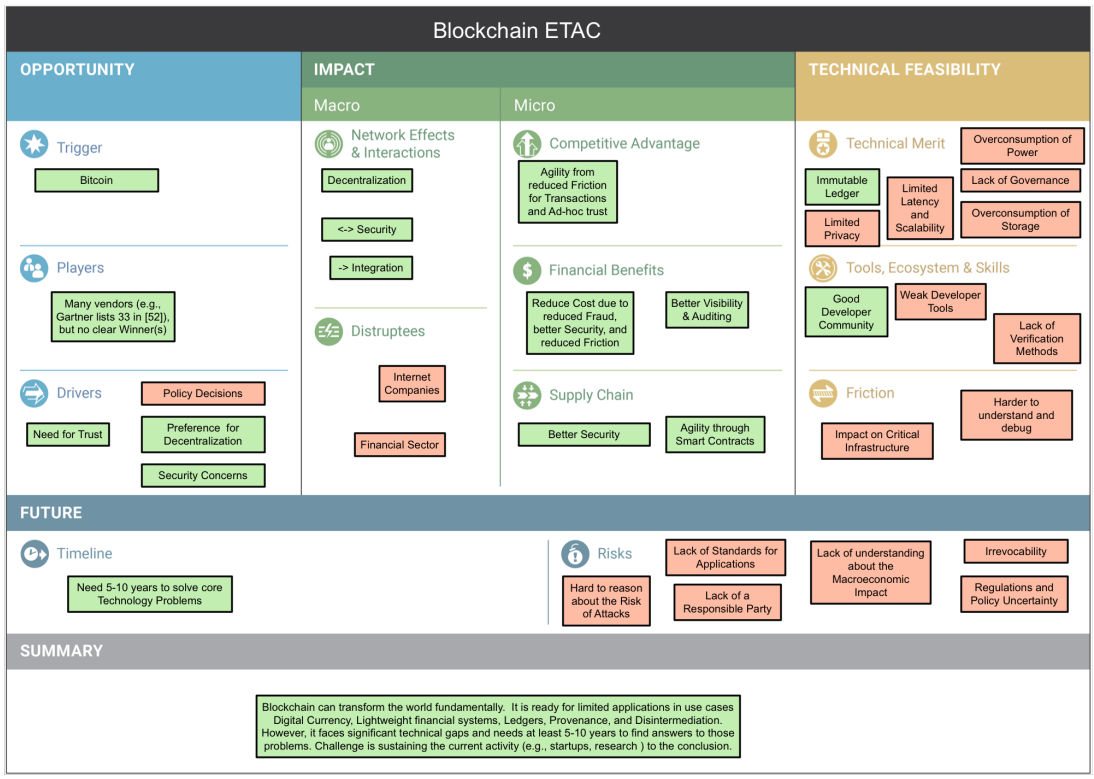

Figure 1. ETAC for blockchain

3 ETAC FOR BLOCKCHAIN

3.1 Opportunity

The rise of the well-known digital currency—Bitcoin—kick-started blockchain. Economic incentives resulting from the appreciating bitcoin price attracted many and created awareness. Ensuing news following the booms and bust of the Bitcoin price kept blockchain on top of the minds of many. The US government identified Bitcoin as property in 2011 and as a currency in 2013 (see Zakon (2018)). Other governments soon followed suit (see Zakon (2018)). One by one Internet companies started accepting Bitcoin (e.g. Zynga, Expedia, Dell, Microsoft).

By 2015-16, it was observed that the impact of Bitcoin extends beyond cryptocurrency. The real value of blockchain is its shared, distributed, and immutable ledger, which enables decentralization and other use cases. The Bitcoin is followed by new blockchain implementations such as Ethereum in 2015 and Hyperledger in 2016.

In her book "Blockchain: Blueprint for a New Economy"(Swan (2015)), Melanie Swan identifies three generations of the blockchain.

- The first generation deploys cryptocurrencies in applications related to cash (e.g., currency transfer, remittance, and digital payment systems).
- The second generation deploys contracts. They are the economic, market, and financial applications of cryptocurrencies such as stocks, bonds, futures, loans, mortgages, titles, smart property, and smart contracts.
- The third generation deploys cryptocurrencies beyond currency, finance, and markets (e.g. government, health, science, literacy, culture, and art).

Initial blockchains were public where anyone can interact with the blockchain. Later other variations

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

of private blockchains are introduced. Based on who can write to it and who can read from it, blockchain implementations can be categorized in four ways:

- Public - Permissionless: Anyone can join the network and any node in the network can participate in the consensus algorithm (could validate transactions). Or in other words, anyone can read or write. (e.g. Bitcoin, Ethereum).
- Private - Permissionless: Only a selected set of nodes can read but no restrictions on who can write to. (e.g. Hyperledger Sawtooth).
- Public - Permissioned: Anyone can read from the Blockchain, but only a selected set of nodes are allowed to write. (e.g. Sovrin Ledger, IPDB).
- Private - Permissioned: Only a selected set of nodes can read or write. (e.g. Hyperledger Fabric, Hyperledger Iroha, R2 Corda, CU Ledger).

In addition to the above four models, in some cases, the private-permissioned model is extended into two more categories:

- Consortium: Only a selected set of nodes can read or write. But anyone or a selected set of participants can submit transactions.
- Private - Permissioned (enterprise): Only a selected set of nodes can read or write.

Often permissions blockchain are built to support enterprise use cases (see Masters (2019)) and based on more relaxed consensus mechanisms.

Some argue that private blockchains, given their centralized nature, are useless. However, they do provide stronger guarantees than a centralized system. To commit fraud in a permissioned blockchain, the culprit needs help from several people, which is hard to come by in most practical cases. For example, in the case of a consortium of banks, to commit fraud, a bank would need a majority of other banks to cooperate (see Permissioned (2018)), which is unlikely to happen. Hence permissioned blockchains are useful for at least some use cases.

By 2018, a significant blockchain ecosystem is active, which includes developers, miners, black markets, and investors. There are ongoing investments from IBM (HyperLedger), Google (e.g. Kharif and Bergen (2018)), Microsoft, financial institutions, banks, governments, and the United Nation among many others. Gartner has listed 32 blockchain platforms in a report (see Gartner (2019)). Blockchain has also received significant venture capital (VC) investments (e.g. VC (2017), Reiff (2018), and Stark (2017)]). A16z crypto fund is an example (see A16z-crypto (2017)). Furthermore, many researchers are exploring new blockchain based research ideas. Examples of that research are available from the curated paper list on blockchain (see BlockchainPapers (2019)). Unlike many other emerging technologies, large tech giants such as Google, Facebook, Amazon, and Apple have little influence on the blockchain although some investments are already underway. Although there are many players, the core technology is still under active development, and consequently, the playing field is still wide open.

The need for decentralization, the need to establish trust, and the need for security are positive drivers for blockchain. Among these three, the need for trust is the major driver. Sometimes the same is described as “trustless transactions”, where “trustless” means that no preexisting trust is needed and trust is provided by the platform.

Although Bitcoin has drawn mixed responses from regulators and policy-makers, blockchain technology has received a favorable response. In terms of bitcoins, as Hatmaker (2018) reports, the US government has taken a cautiously optimistic stance. However, China, Russia, and some countries have either banned or imposed limitations on cryptocurrencies. As Zakon (2018) points out, some companies that accepted Bitcoins have reversed their position (e.g. Dell, Stripe). On the other hand, the government’s response to blockchain has been positive. For example, many US states have passed or are preparing legislation supporting blockchain (see Legislation (2018)).

4 IMPACT

It is worth noting that the following impacts are not based on the current state of the technology but based on a future where core technologies required to deliver blockchains has been realized.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

4.1 Blockchain Use Cases Categories

Potential impacts of blockchain are far-reaching and many. The following shows some categories of those use cases.

4.1.1 Ledgers (of identity, ownership, status, and authority)

As Berg et al. (2017) points out, both, governments and organizations maintain ledgers of identity, ownership, status, and authority. Corresponding blockchain implementations can replace them.

Following are some advantages of blockchain based replacements:

- It improves data integrity and security. It also builds security and privacy protocols into the ledger operations, which makes it harder to defraud the system.
- It can reduce operational and processing costs. For example, it can reduce the documentation required for government and corporate processing (e.g. loans) through tamper-proof record keeping. Among examples of records are education records, birth, and death certificates, and criminal records.
- It can improve visibility and accountability. For example, it can track public spending and aid money.

In summary, these systems make fraud harder, which enables us to remove expensive safeguards that guard against fraud, both of which leads to reduced cost. Decentralization improves security further. Increased automation and accountability provided by blockchain also improve agility.

4.1.2 Digital currency & lightweight financial system

As pointed out by Greenspan (2016), Meola (2017), and Tapscott (2017), blockchain can build a lightweight financial system. In some cases, it removes some intermediaries, and in others, it makes current models efficient and secure. Some examples are Nexus Mutual, Stellar, Celsius, BABB, and Omisego.

Following are some advantages:

- It provides better integrity and sharing and reduces or removes financial costs. Mortgages, loans, credit scoring, escrow crowdfunding, widely accepted gift cards, widely accepted loyalty points, and local currencies are among a few of the use cases.
- It can offer efficient and cheap micropayments.
- It can enable many who are currently disconnected from banking systems due to costs or loan criteria (e.g. micro-financing).
- It can disaggregate and enable many new business models.

In summary, just like with the earlier use case, lightweight financial systems reduce costs by reducing fraud and safeguards required to avoid fraud. Decentralization improves security further. Increased automation and accountability provided by blockchain also improve agility. It is worth noting that the high value of cryptocurrencies poses challenges due to significant transaction costs of blockchain, which must be solved to enable this use case.

4.1.3 Smart contracts

- As pointed out by Berg et al. (2017), blockchain through smart contracts enables businesses or individuals that do not trust each other to create agreements, do transactions, and build value without intermediaries. For example, a smart contract can provide an escrow, a trusted third party that hold the funds while the transaction takes place to reduce risks. It can be triggered by actions such as timeout, acceptance of goods, or a stock tick. Another common example is that of a car lease whereupon a missed payment, the car automatically locks and returns the control to the lender. In these cases, the immutability of blockchain replaces the need for trust. Furthermore, due to the reduction of costs, smart contracts would enable complex financial instruments to a wider audience. However, the assertion that smart contract can broadly replace legal instruments has been challenged due to lack of "court of appeal". This use case is still evolving.

These use cases provide high agility and, in some cases, reduced costs.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

4.1.4 New internet

As described by Meola (2017) and Dixon (2018), a new decentralized internet can be built using the decentralized nature of the blockchain. Such an internet is independent of governments and corporate entities.

Following are some examples of its services.

- A decentralized DNS services, routing, and other internet services
- A global identity that is safe and decentralized - users can own their identity and it can't be tampered with by an outsider (e.g. Blockstack).
- A global reputation that is safe and decentralized - this will enable users to take their reputation in one ecosystem to another. Also, this will create incentives for people to behave (e.g. DREP). Limit or control the anonymity of the Internet. For example, if every node or user need to be registered with the blockchain and identities verified, we can block bad actors/fraudsters.
- Decentralised content: the ability to create and offer websites and information without requiring central servers.

Such a decentralized internet is motivated by many that are concerned about the growing arbitrary power of GAFA (Google, Apple, Facebook, Amazon) over the Internet and concerned about the interference by governments on the Internet. Among examples are recent algorithm changes by Facebook that significantly changed the traffic patterns (see Chaykowski (2018)) and government surveillance bills (see Savage (2018)). There have been earlier isolated efforts (e.g. Johnson (2018)) to build a truly decentralized internet, and many believe that blockchain is a perfect path to make further progress.

Another possibility is to use blockchains to move away from advertisement based internet economy. For example, today most free services (Google, Gmail, Twitter etc etc.) provide their services through advertisement revenue. The consumer is their ultimate product. An alternative to this approach is enabling the end users to pay creators a small amount of bitcoin or crypto coin instead of liking their content. The same is already happening to some extent via Patreon accounts, although this a decentralized implementation of the same model.

These use cases provide privacy and decentralization.

4.1.5 Autonomous ecosystems

Meola (2017) points out that blockchains can create decentralized alternatives for ecosystems and marketplaces such as Amazon, eBay, and Uber. Such ecosystems and marketplaces will not have an organization that has arbitrary power over all participants. Furthermore, this can also replace many ranking systems and rating agencies (e.g. hotel ranking, college ranking, bank rating, sports ranking).

Following are some of the potential use cases.

- Social networks (e.g. SocialX)
- Ridesharing (e.g. Dylyver)
- Marketplaces, auctions, and reputation (e.g. LO3 Energy, Greeneum, Tracer)
- Stock exchange without an exchange
- Prediction markets (e.g. Augur)
- Reputation verification and ranking (e.g. The World Table (Open Reputation) and ThanksCoin).
- Decentralized Autonomous Organizations (DAO) (e.g. Dash, Bitshares)

This use case increases decentralization.

4.1.6 Disintermediation

As pointed out by Greenspan (2016), blockchains enable many untrusted parties to safely share a single database without an intermediary. For example, this can be used to audit critical communication between parties in healthcare, legal domains, or negotiations (e.g. Legaler). For instance, a secure email system where all transactions are verified and hence cannot be denied.

This use case provides better security and agility.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

4.1.7 Provenance

Provenance tracks the origin, history, or movement of anything and make those auditable. As pointed out by Greenspan (2016), capturing provenance of artifacts using blockchain will provide better security and simplify processing.

Following are examples of some use cases.

- Tracking high-value items such as luxury goods, pharmaceuticals, cosmetics, diamonds, art, and electronics through the supply chain to verify their authenticity and to make sure they are sourced or built the way they are advertised. (e.g. FarmaTrust)
- Tracking cars and other items, their ownership, their operations history, and their service history will enable a stable second-hand market for those items.
- Creating new markets for special origin goods such as organic food making their supply chain auditable as described in the first use case (e.g. CargoX, ShipChain, Paket).
- Tracking software lifecycle such as what libraries are used, what version, who build it for a given distribution to enforce security.
- Tracking aid money to ensure transparency and accountability.
- Avoiding double payments in insurance claim processing.
- Managing content and copyrights by using blockchain to track use, propagate credit, and collect royalty payments for content (e.g. music, articles, images)
- Potentially removing intermediaries. (e.g. Choon, Audius)
- Tracking perishable items (e.g. produce, medicine) and their chain of custody

This use case will provide reduced cost and agility.

4.1.8 Initial Coin Offerings (ICO)

ICOs (see ICO (2017)) provides a new way to raise money. Tapscott (2017) also recognizes this as an important blockchain use case. They can be used to attract initial capital or to attract contributions.

Another variation is that instead of raising money for a project, one can bootstrap a project by offering coins for contributions. For example, a software project may attract developers by offering coins for feature implementations, bug reports, and patches. If the project is successful, those coins may become valuable. Even now, many developers see contributions to the missing open source projects as investing their time in return for reputation and potential recognition. Blockchain-based coins formalize these informal interactions. For example, Walden and Zuegel (2018) argues blockchain related technologies as the next evolution of open source.

This use case can provide agility. However, as Partz (2018) points out, since ICOs sidestep current regulations, they increase the risks of fraud. Recently, US Security and Exchange Commission (SEC) has defined ICO tokens as securities(see SEC (2018)), in which case it is less attractive as a funding mechanism. However, it may still be valuable as a way to track contributions done by different people to a project.

4.1.9 Voting

As Meola (2017) points out, blockchain can be used to build secure and fast voting systems. Such a system reduces the cost of conducting elections, which enables us to use elections more frequently thus increasing people participation in governance. Among examples is the US state West Virginia (see Desouza and Somvanshi (2018)) and Swiss City Zug (see Mayer (2018)). In its logical conclusion, voting becomes easy and cheaper, if we choose, we might even be able to replace the representative democracy with direct democracy.

It is worth noting that this is an evolving use case. For example, Dunietz (2018) questions the readiness of blockchain for voting.

This use case provides reduced cost and agility.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

4.1.10 Healthcare

As pointed out by Gens et al. (2017), Greenspan (2016), and Meola (2017), blockchain can be used to support many healthcare use cases such as handling medicine providers' supply chain, managing prescriptions, and health data sharing.

The last use case warrants further analysis due to its impact. Efforts are underway to use blockchain to record health data securely in a manner that gives complete control over the data to its owners (patients) while enabling portability between providers. This use case might also allow anonymous analytics that will provide better population health indicators as well as the ability to track the effect of medication on individuals as statistics.

This use case provides reduced cost and agility.

The following table 1 explores each of the use cases in terms of their applicability in public and private settings.

None	Public	Private
Ledgers	Yes	Yes
Digital currency & lightweight financial system	Yes	Rare
Smart contracts	Rare	Yes
New internet	Yes	Rare
Autonomous ecosystems	Yes	Rare
Disintermediation	No	Yes
Provenance	Yes	Yes
Initial Coin Offerings (ICO)	Yes	No
Voting	Yes	Rare
Healthcare	Yes	Yes

Table 1. Applicability of use cases in public and private settings

The next section will look at the above use cases in terms of the ETAC.

Let us start with the impact.

4.2 Macro Impact

We use the term "network effects" to describe a phenomenon where the value of a system to its users increases as the size of the system increases(see Griffin (2016)). Most of the above use cases benefit from network effects as more and more users join those systems, they become more and more effective. However, as discussed by Griffin (2016), the success of those use cases depends on the ability to create a critical mass.

Blockchain affects security and integration middleware segments. The blockchain is tightly bound with security middleware and the success of blockchain likely makes systems much more secure and extends their applications. At the same time, blockchain may disrupt or change some prevailing security solutions. The fraud detection subsegment of security will be significantly affected. Blockchain will reduce or remove some of the common fraud scenarios. It will also make available a wide array of data about transactions, which will enable us to detect much more complicated fraud.

Blockchain-based systems may replace systems built by current internet companies. Some examples are social networks like Facebook, and Twitter, and marketplaces like Amazon, and eBay. They may also disrupt large public clouds by replacing them with decentralized crowdsourced computation platforms. Furthermore, blockchains can significantly change many financial systems, trade, and government operations.

4.3 Micro Impact

Blockchain can affect an individual company in several ways. By integrating with blockchains, organizations that have requirements for ad-hoc transactions with untrusted parties can use blockchain to achieve a competitive advantage due to agility enabled by reduced friction for transactions and ad-hoc trust. For example, W3C specifications Decentralized Identifiers (Reed et al. (2017)) and Verifiable Claims(Burnett et al. (2017)) enable user to identify a user and verify claims about him. Furthermore, organizations can

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

reduce cost due to reduced fraud, better security, and reduced friction. Also, blockchains enable new business models hence enabling new products and services.

Furthermore, blockchain can increase the efficiency of the supply chain due to reduced fraud, better security, and faster transaction term negotiations. It is likely that organizations will have to support demand from the rest of the supply chain for integration with blockchain.

In summary, common themes of blockchain impact include better security, decentralization, reduced cost, and agility. The impact is both substantial and transformative. This yields our first assertion of the document.

5 TECHNICAL FEASIBILITY

5.1 Technical Merit

A long-standing challenge while building digital cash is "the double spending problem", which is the need to stop the owner of digital cash from reusing the money he has used to pay a transaction. Blockchain provided a new decentralized solution to the problem, created incentives to keep it going, and made it work in the real world. These are significant contributions to the state of art.

However, blockchains have many limitations. Let us explore some of the technical challenges.

- Limited scalability and latency - As pointed out by Kasireddy (2017b) and Yli-Huumo et al. (2016), blockchain systems have limited scalability and high latency. At the time of writing, a bitcoin transaction takes about 8 minutes and can support only about 2-3 transactions per second (i.e. Chepurnoy (2016)). Furthermore, Croman et al. (2016) argue that independently of consensus algorithms, this limit is about 50 seconds and 27 transactions per second. Most use cases that we discussed under impact are infeasible under these limits. For example, to handle global scale systems such as a decentralized internet, blockchain needs to handle tens of thousands of transactions per second. However, it is worth noting that it is decided by the choice of consensus algorithm. Private blockchain implementations have proposed faster algorithms although they provide lesser guarantees.

- Limited privacy - as pointed out by Kasireddy (2017b) and Yli-Huumo et al. (2016), although blockchain provides pseudo anonymizations, by analyzing the transaction graph and other related information, it is often possible to link users to transactions. Once one transaction is linked to a user, all his transactions become known. When blockchain transaction data are public or shared across a larger group (in the case of permissioned-blockchain), this means blockchain is riskier than using a credit card in terms of privacy. Furthermore, since blockchain transactions are public information, user identification via analysis is not prohibited under privacy laws.

- Storage constraints - As pointed out by Kasireddy (2017b) and Yli-Huumo et al. (2016), with current algorithms, each node must store the full history of the blockchain. This leads to high transaction latencies. The need to store full history also forestalls lightweight nodes, such as IoT devices, from joining a blockchain network. As time passes, the history becomes larger aggravating the problem.

- Unsustainable consensus - As pointed out by Kasireddy (2017b) and Yli-Huumo et al. (2016), Bitcoin website (see Bitcoin-Problems (2019)), and Ethereum website (see Ethereum-Problems (2019)), the current consensus method is cumbersome and consumes a significant amount of energy. For example, as pointed out by Bitcoin-Energy-Consumption (2019), Bitcoin energy consumption, if considered as a country, would be 39^{th} in the world and higher than Australia.

Among other challenges are inadequate tooling pointed out by Kasireddy (2017b), and Sybil attack (where an attacker attempts to fill the network with clients that they control). Furthermore, Ethereum problems page (see Ethereum-Problems (2019)) and the Bitcoin Problems page (see Bitcoin-Problems (2019)) lists other issues.

These challenges affect the blockchain ecosystem. For example, in 2018, when the startup Coinprism (see De (2017)) stopped operations, the founder quoted some of the aforementioned challenges.

It is worth noting that most of the above challenges mainly affect public permissionless blockchains due to their deployment size, although even private large deployments may be affected. Table 2 depicts

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

how blockchain use cases are affected by four main technical challenges. Empty cells suggest no challenges are identified.

	Public	Private
Ledgers of identity, ownership, status, and authority	Limited scalability and latency, Limited privacy, Storage constraints * Unsustainable consensus	OK for most use cases
Digital currency & lightweight financial system	Limited scalability and latency, Limited privacy, Storage constraints, Unsustainable consensus	
Smart contracts without a central authority	N/A	OK for most use cases
New internet	Limited scalability and latency, Limited privacy, Storage constraints, Unsustainable consensus	N/A
Autonomous ecosystems/ marketplace	Limited scalability and latency,Limited privacy, Storage constraints, Unsustainable consensus	N/A
Disintermediation	N/A	OK for most use cases
Provenance	OK for most use cases	
Initial Coin Offerings (ICO)	OK for most use cases	N/A
Voting	OK for most use cases	N/A
Healthcare	Limited scalability and latency, Limited privacy, Storage constraints, Unsustainable consensus	Limited privacy, Storage constraints, Unsustainable consensus

Table 2. Technical challenges by use case

Notwithstanding significant challenges, there is hope. Best minds are working on these problems. Progress is being made. For example, Zamani et al. (2018) presented a RapidChain algorithm that can perform 7500 transactions/ second. Furthermore, Kasireddy (2017a) discuss some of the approaches used to handle these problems and the curated blockchain papers list (see BlockchainPapers (2019)) records many relevant publications addressing some of the problems.

5.2 Tools, Ecosystem, and Skills

Developers with Blockchain skills are scarce. However, fueled by high demand, many developers are acquiring blockchain skills. We have observed students master key ideas within a few weeks. Many education materials are already available. Therefore, we believe skills will not be a significant obstacle.

Tooling support for blockchain is limited. Most use cases are currently geared for highly technical users (i.e. Kasireddy (2017b)). However, this can be fixed only after core technology has stabilize.

5.3 Friction:

Following are some of the technical challenges that lead to friction.

- Lack of methods to verify and limit risks - As pointed out by Kasireddy (2017b), lack of such tools is a major inhibitor to the blockchain. Among approaches that have been considered are formal contract verification, testing and simulation environments, and means to undo operations or limit the associated risks (e.g. by specifying upper limits). Although most software development happens without formal verification, irrevocability and the automated nature of blockchain transactions (e.g. smart contracts) increase associated risks to a new level. Therefore, we believe this is significant friction.

- Lack of governance and standards - As pointed out by Tapscott (2017), there are no clear regulatory processes for public blockchains. Among open challenges are how to evolve the blockchain, when

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

to fork, what is the process to accept a fork, and how to handle human errors. They pose significant security risks. Solutions themselves must be decentralized not to undermine the goals. Finding a technical solution or finding a process to solve the problem is a pressing need.

- Blockchain-based applications are often complex (e.g. smart contracts). Current blockchain ecosystems do not provide tools that help users to debug those applications.

Hence, in its current state, technical limitations and friction can significantly reduce blockchain adoption. Progress mandates new and significant technological breakthroughs.

6 FUTURE

6.1 Risks

There are significant risks associated with blockchains. Blockchain's high impact potential in replacing many critical systems such as financial systems, cash, land registries, voting, further exacerbates those risks.

6.1.1 Irrevocability

- As Stinchcombe (2018) points out, the irrevocability of transactions is a significant risk.

For use cases such as Bitcoin and land registry, a resource is passed from an owner to an owner and only the current owner has the capability to assign it to a new owner. For this and similar use cases, irrevocability can have devastating consequences. However, for most other use cases, this can be addressed via a recovery transaction that undoes the transaction.

Following are example cases where irrevocability is problematic.

If a credit card is lost or bank account is hacked, money can often be traced, found, and returned. However, as pointed out in the Bitcoin projects problems page (see Bitcoin-Problems (2019)), no recourse is possible with blockchain. There is no possibility of appeal. A person or an organization can lose all the money because their account is hacked or because their hard disk has crashed. For example, Zakon (2018) cites an incident where a user threw away a hard drive with keys to 7500 bitcoins. The same article approximates that about 25% of all Bitcoins are already lost.

Most ecosystems and markets built with blockchains are complex systems. They have emergent behaviors. For example, consider a hypothetical ChainBook, a Facebook alternative built on top of the blockchain. ChainBook's underlying algorithm will be designed to distribute traffic equitably, to manage accounts, and propagate updates to all users based on some criteria. Since ChainBook is a complex system, we do not have techniques to analyze or understand those algorithms fully. Instead, they are designed using heuristics and empirical experiments, just like current social network algorithms. It is possible for such algorithms to have loopholes, which enables an attacker to hijack some accounts or hijack traffic. Unlike with Facebook, which has central control and can undo the change, it is not clear how this can be handled in ChainBook.

Vulnerabilities are already challenging. Coupled with irrevocability they are dangerous. Unlike with Facebook, we can't fix the problem even when we know the problem as changes are irrevocable. The emergent behaviors are often hard to foresee fully. Ultimately, the outcome could be systems that no one understands. Anyone who would figure out a weakness in the decentralized algorithms would wield a vast amount of power. Risks are very high. We can lose control of our creation.

Let's now also consider smart contracts. Smart contracts bring in automation. Automation and irrevocability are a poisoned combination. A simple mistake in a smart contract can lead to disasters, and outcomes can't be revoked. Mistakes and unexpected scenarios are bound to happen, and blockchain technology needs to handle how to detect, contain, and recover from those scenarios.

Any hijacked accounts or a resource is irrevocable unless more than 50% of participants are willing to accept a fork to the code (a.k.a. hard fork). For example, as described by Castillo (2016), Ethereum returned funds lost due to an attack using a hard fork. However, it is not clear what is the criteria to accept such a hard fork. Also, it is possible that the next attack can be hidden inside the hard fork. Also, as the blockchain adoption and hence transaction rates increases with time, it becomes harder and harder to enforce a hard fork without affecting correct transactions.

Before broad adoption, blockchain needs algorithmic changes to handle problems or needs a way to contain the impact via some form of upper limits, sandboxes, or insurance. As an alternative, many

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

private blockchains provide the organization or consortium the ability to do admin operations such as change rules, undo transactions, and modify balances.

6.1.2 Regulator Absence

Another risk is regulator absence. A regulator plays a key role in some use cases. For example, in the case of a stock market or share offering, oversight makes sure that all parties are protected. Without a regulator, it might not be easy to detect and avoid schemes like pyramid schemes. Although not popular, regulators play a crucial role in many systems.

Regulator role is also important to ecosystems. For example, decentralized social networks might do a bad job of controlling hate speech, bias, and targeted attacks than a centralized system. For example, if a fake news scenario developed with a decentralized social network, there is no one to hold accountable. Further, this may be a perfect medium for an attacker to introduce bias and other unexpected behaviors to the system via updates while hiding his tracks.

Blockchain-based systems, in their current form, do not support a regulator. Also given irrevocability, it can either be impossible or expensive to fill the missing regulator's role.

At the same time, one could argue that the web does not have a regulator. For example, no one curates what goes on the web. Regardless, the web is one of the most successful systems humans have built. At the same time, with scenarios such as fake news and hate speech, we are seeing the limitations of the web.

Where a regulator is needed and where it is not needed is a debate that will continue. However, blockchain based decentralized systems make it hard to introduce a regulator if needed.

6.1.3 Misunderstood Side-effects

Thirdly, the impact of blockchain extends beyond computer science. We need to understand the economics, social, and political side effects of the blockchain. For example, blockchain may enable chap voting, enabling us to even replace representative democracy with direct democracy but we do not know whether that will be a good or a bad. Another risk is macroeconomic impacts. For example, lack of inflation is often lauded as a significant feature in the blockchain. However, inflation is often used as a monetary instrument by countries: for example, to absorb the shock of a downturn (see Ross (2018)). Some theorists believe that inflation is necessary for growth (see Mallik and Chowdhury (2001)). Removing such instruments would be risky without understanding its repercussions. Economics, Marketplaces and Trust sections in blockchain papers (see BlockchainPapers (2019)) lists some of the current work in this area.

6.1.4 Fluctuations in Bitcoin Prices

Another risk is fluctuations in bitcoin prices. However, many believe that this is because it is new and its intrinsic value is hard to judge and it will stabilize over time (see Barker (2017)). With high bitcoin values, transactions charges are also high, which would turn off many use cases such as micropayments. It seems that the deflationary nature of Bitcoin and broad transformative use cases are in conflict due to transaction costs. This problem will aggravate with time. This only affects Bitcoin and financial use cases but does not affect other use cases.

6.1.5 Quantum Cryptography

As pointed out by Kasireddy (2017b), one of the looming threats to cryptocurrency and cryptography is the issue of quantum computers. They can break most current cryptography operations including hash functions which provides blockchains immutability. However, quantum resistant hash functions are known and in some cases already implement. Hence, it is likely we can just switch hashing algorithms. Therefore, the effect on the blockchain by quantum computing is not different from the effect on other aspects of computing[Quantum-computing-And-Bitcoin (2019)]. Aggarwal et al. (2017) discuss some techniques for protecting against quantum attacks.

At the same time, such a shift to quantum blockchain will take time. Even at its initial stages, where only governments and large organizations have access to quantum computers, quantum computing undermine all benefits of decentralization, in which case, the problem is worse as governments or organizations can act algorithmically without detection as opposed to current centralized systems that are regulated through transparent processes.

6.1.6 Regulatory Response

Finally, as we discussed under impact, blockchain changes many things that are currently governed by regulation and law. Therefore, likely, there will be future regulations and the law governing blockchains

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

and its use. The response of those institutions are not clear, and the associated uncertainty creates risks. However, blockchain carries significant first-mover advantages to countries if they can adapt it in a significant manner. Therefore, governments will be ready to give it a fair chance.

Some of these challenges, such as irrevocability, regulation and lack of census mechanisms are not present in private blockchains. On the other hand, private blockchains provide less decentralization. Consequently, there is a tradeoff between those challenges and amount of decentralization. At the same time, private blockchains are intended to be used in closed environments and can't be widely applied to public blockchain use cases.

The table 3 explores the effect of the aforementioned risks on blockchain use cases. Empty cells suggest no risks are identified.

	Public	**Private**
Ledgers of identity, ownership, status, and authority		
Digital currency & lightweight financial systems	Irrevocability, Unpredictability, Economical, social, and political side effects, Regulatory response	N/A
Smart contracts without a central authority	N/A	Irrevocability, Unpredictability
New internet	Irrevocability, Unpredictability, Lack of a regulator Economical, social, and political side effects	N/A
Autonomous ecosystems or marketplace	Irrevocability, Unpredictability	
Lack of a regulator, Economical social, and political side effects	N/A	
Disintermediation	N/A	
Provenance		
Initial Coin Offerings (ICO)		N/A
Voting	Regulatory response	N/A
Healthcare	Regulatory response	

Table 3. Risks by Use Cases

6.2 Timeline

Up to this point, the blockchain outlook presented facts that are supported by either citations or arguments, not opinions. This last section weighs those facts and provides our expert observations and opinions on evolution and future of blockchain.

Concerning impact, Blockchain easily falls into the disruptive (transformative) category. If successful, it will transform financial systems, the way people and organizations establish trust (e.g., when doing business, when working towards a common goal), and underline information platforms like internet, marketplaces, voting systems.

Let us consider Roger's five factors (see Rogers (2010)) that evaluate technology adoption. Blockchain has two factors that help technology in their adoption: technology delta (relative advantage to existing technology) and observability (ability for other users to see blockchain in use). However, blockchain in its current state fails in simplicity (easy to understand and use), and trialability (easy to show it working). Also, compatibility(Ease of technology to integrate with day to day lives of users) is weak for blockchain as it assumes understanding about advanced computing techniques (e.g. cryptographic keys). Future systems might hide some of these complexities. Overall, Roger's five factors suggest weak adoption. However, wide awareness and hype associated with blockchain may counterbalance above.

The table 4 summarizes use cases, challenges, and risks they face, and our conclusions. In the

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

548 conclusion column, EU-TRL shows EU technology readiness level (see EU-TRL (2019)).

Use case Category	Public	Private	Conclusion
Ledgers	**Challenges**: Scalability, Latency, Privacy, Storage, consensus concerns	Feasible	This category applies to both public & private blockchains, with EU-TRL levels 4-6, and it is feasible for small deployments (e.g. throughput about 2-3 TPS).
Digital Currency & Lightweight financial systems	**Challenges**: Scalability, Latency, Privacy, Storage, consensus concerns. **Risks**: Irrevocability, Unpredictability, Lack of a regulator, Unknown side effect	N/A	This category is mainly public, with EU-TRL levels 5-8, and feasible for small deployments. Breakthroughs are needed for future performance and handling risks.
Smart contracts	N/A	Risks: Irrevocability, Unpredictability	This category is mainly private, with EU-TRL levels 2-4 and breakthroughs needed for handling risks.
New internet	**Challenges**: Scalability, Latency, Privacy, Storage, consensus concerns. **Risks**: Irrevocability, Unpredictability,Lack of a regulator, Unknown side effect	N/A	This category is mainly public, with EU-TRL levels 1-2, and breakthroughs are needed for performance and handling risks.
Autonomous ecosystems	**Challenges**: Scalability, Latency, Privacy, Storage, consensus concerns. **Risks**: Irrevocability, Unpredictability,Lack of a regulator, Unknown side effect	N/A	This category is mainly public, with EU-TRL levels 1-2, and breakthroughs needed for performance and handling risks.
Disintermediation	N/A	Feasible	This category is mainly private, with EU-TRL levels 5-7, and feasible for small deployments (e.g. need throughput about 2-3 transactions per second)
Provenance	Feasible	Feasible	This category is both public and private, with EU-TRL levels 5-7, and feasible for small deployments (e.g. throughput about 2-3 TPS)
Initial Coin Offerings (ICO)	Feasible	N/A	This category is mainly public, with EU-TRL levels 5-7, and feasible for small deployments (e.g. throughput about 2-3 TPS). However, as ICO also comes under regulatory control, the advantage over other fundraising mechanisms is being reduced

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

Voting	**Challenges**: Privacy	N/A	This category is mainly public, with EU-TRL levels 3-5, and privacy is a challenge. Otherwise, it is feasible for small deployments
Healthcare	**Challenges**: Scalability, Latency, Privacy, Storage, consensus concerns	**Challenges**: Scalability, Latency, Privacy, Storage, consensus concerns	This category is both public and private, with EU-TRL levels 2-3, and breakthroughs are needed for performance.

Table 4. Use Case Category Feasibility

In summary, this yields the second assertion of the document that the following use cases are feasible within the next three years.

- Bitcoin becomes an asset and black market currency, but it will not become a fiat currency as a replacement for existing fiat currency
- Lightweight financial systems
- Both public and private Ledgers (e.g. significant public records, notary and KYC services)
- Provenance (e.g. supply chains and other B2B scenarios) and Disintermediation.
- Although we believe ICOs are feasible, classification of coins as securities by US SEC remove most of its attractions as an investment medium.

Except for the aforementioned use case, technology is not yet ready to deliver the vision. Even then, they are feasible only for deployments where the load is limited. We see significant gaps in both core technology as well as its applications. Among the challenges are limited scalability and latency, limited privacy, heavy storage and energy requirements, unsustainable consensus mechanisms, lack of methods and tools to verify blockchain-based applications and smart contracts, and lack of governance and standards.

However, some of the best minds are trying to solve these problems. There is significant academic participation, and a large amount of VC money has also been deployed. We believe most of these challenges can be addressed. However, we believe we are looking at the 5-10 year time frame before it happens. For example, Iansiti and Lakhani (2017) argue, based on their technology adoption model, that transformative use cases for Blockchain are decades away while more simple, specific use cases that have limited novelty may be realized faster.

While we do believe that blockchain's fundamental challenges could be addressed, there is a chance that current technology is the limit of the blockchain. If that is the case, the impact of blockchain would be very limited.

This yields the third assertion of the document that blockchain faces significant challenges in many use cases and it will likely take at least 5-10 years to find answers to those problems.

It is not clear whether blockchain can sustain the current level of effort for an extended period of five or more years. Academic research and funding are often long-term. However, startups work against the time; they run out of funding; further funding is often not possible without demonstrating revenues. If a few startups fail, that will likely limit further investments in the area, starting a domino effect. For example, we saw Coinprism (see De (2017)) shutting down in March 2018. We believe the fate of startups will be paramount to the fate of blockchains. Given the technical challenges, startups should choose use cases that can be addressed within current limitations. Furthermore, the economy does not need too many blockchain unicorns before technology challenges are addressed because if there are too many too early, their potential failures can trigger an economy-wide correction like the dotcom bubble. This is the fourth assertion of the document.

Even after technology challenges have been addressed, adoption has to be carefully planned and executed. Blockchain will replace critical systems on a notch above what we used to, and any misstep

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

can have devastating consequences. Blockchain proponents have to find multiple use cases that start with simple problems and progressively tackle harder problems while hashing out problems. We believe the use cases we have identified and assessments provide a good starting point for this process.

Governments and policymakers face an interesting challenge. Due to the transformative power of blockchain, it can't be ignored. If blockchain is banned and later successful, nations might find they live in the last age. At the same time, reckless adoption creates many other problems and carries risks.

Finally, it is not obvious we understand clearly what we want from blockchain. Charlon, the Coinprism founder, argued that unless decentralization and censorship resistance is required, blockchain is a suboptimal choice for most use cases due to scalability and latency limitations. Given the challenges faced by blockchain and a potentially long wait to address those challenges, it is worth questioning the need for decentralization.

What is the need for decentralization? It is true that people, when asked, are concerned about the arbitrary power of governments as well as large organizations. Do they understand tradeoffs? Asked in isolation, we need everything. People are concerned about privacy, but most of us share data with GAFA. However, if Facebook comes up with a paid account where they do not touch your private data, how many would buy it?

As the article Centralized-Wins (2018) argues, in most cases, given a problem, the centralized or semi-centralized solutions are faster, have more throughput, and are cheaper than the decentralized solution when considered holistically. Are we willing to pay for delays and duplication? How much?

For years we have handled concerns about centralization using policy, law, and auditing through institutions. Can our concerns be solved by strengthening those institutions? We are effectively trying to replace those institutions with algorithms. What makes us think that we can figure out those algorithms if we can't make those institutions work with much human involvement? By handing control to algorithms, aren't we handing over the control to whoever that has right to fork and change algorithms? Unlike institutions, those algorithms changes are tough to audit. This challenge is shared by both blockchain and AI.

Presumably, we could support semi-decentralized solutions much faster than full decentralization. Already, a significant amount of money has been already deployed to the blockchain. Blockchain could run out of time while trying to solve full decentralization. The clock is ticking. If the quest for a full decentralized solution did take too long, that risks future of blockchain. One could argue that we should first make blockchain work with a semi-decentralized version to avoid the risk and strive for a full decentralization solution as the second stage. of its demise while striving for a fully decentralized solution.

It is not clear whether people care enough about decentralization to accept limitations that come up with it. If decentralization is not necessary, most use cases can be addressed much easier with centralized systems (likely private blockchain technologies), accepting guarantees weaker than blockchain but stronger than earlier centralized systems. Furthermore, some use cases might have less risky alternatives for blockchain use cases. For example, a micropayment platform can collect and make monthly payments of micropayments without a blockchain.

Confusion about the right level of determination is the fifth assertion of the document.

It will take time for us to find the answer to these questions.

7 CONCLUSIONS

The primary contributions of this paper are a use case centric categorization of the blockchain, a detailed discussion on challenges faced by those categories, and an assessment of their future.

In conclusion, we made six assertions and discussed them in detail.

- Blockchain potential impact is real. If successful, Blockchain technologies can transform the way we live our day to day lives.
- We believe technology is ready for limited applications in Digital Currency, Lightweight financial systems, Ledgers (of identity, ownership, status, and authority), Provenance (e.g. supply chains and other B2B scenarios) and Disintermediation, which we believe will happen in next three years.
- However, with other use cases, blockchain faces significant challenges such as performance, irrevocability, need for regulation and lack of census mechanisms. These are hard problems and

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

likely it will take at least 5-10 years to find answers to those problems.

- It is not clear whether blockchain can sustain the current level of effort for extended period of 5+ years. There are many startups and they run the risk of running out of money before markets are ready. Failure of startups can inhibit further funding and investments.

- Value and need of decentralization compared to centralized and semi-centralized alternatives is not clear.

Given the risk involved as well as the significant potential returns, we recommend a cautiously optimistic approach for blockchain with the focus on concrete use cases. Investments must consider sustainability for 5-10 year horizon before significant returns.

There are clearly areas of research to solve the most pressing challenges, such as performance. These are already underway. However, we identified some areas that seem less well explored. Firstly, the immutability of the blockchain ledger is a significant advantage in many use cases. However, there are scenarios where the immutability makes smart contracts and other use cases unpredictable. Secondly, there is a clear need for better frameworks to assess the impact of centralized vs decentralized approaches for any given domain. This would greatly help understand the value of using blockchains in different spaces.

ACKNOWLEDGMENTS

Many thanks to Prabath Siriwardena and Guy Harrison who have provided significant and useful feedback.

REFERENCES

A16z-crypto (2017). Introducing a16z crypto. https://a16zcrypto.com/. [Online; accessed 01-2019].

Aggarwal, D., Brennen, G., Lee, T., Santha, M., and Tomamichel, M. (2017). Quantum attacks on bitcoin, and how to protect against them. *arXiv preprint arXiv:1710.10377*.

Barker, J. T. (2017). Why is bitcoin's value so volatile? https://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp#ixzz5VV75q2jW. [Online; accessed 01-2019].

Berg, C., Davidson, S., and Potts, J. (2017). The blockchain economy: A beginner's guide to institutional crypto economics. https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4. [Online; accessed 01-2019].

Bitcoin-Energy-Consumption (2019). Bitcoin energy consumption index. https://digiconomist.net/bitcoin-energy-consumption.

Bitcoin-Problems (2019). Bitcoin list of problems. https://en.bitcoin.it/wiki/Weaknesses.

BlockchainPapers (2019). Blockchain papers. https://github.com/decrypto-org/blockchain-papers. [Online; accessed 01-2019].

Burnett, D. C. et al. (2017). Verifiable claims data model. *Verifiable Claims Working Group, W3C Editor's Draft*.

Castillo, M. (2016). Ethereum executes blockchain hard fork to return dao funds. "https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds.

Centralized-Wins (2018). What do you believe now that you didn't five years ago? centralized wins. decentralized loses. http://highscalability.com/blog/2018/8/22/what-do-you-believe-now-that-you-didnt-five-years-ago-centra.html. [Online; accessed 01-2019].

Chaykowski, K. (2018). Facebook's latest algorithm change: Here are the news sites that stand to lose the most". https://www.forbes.com/sites/kathleenchaykowski/2018/03/06/facebooks-latest-algorithm-change-here-are-the-news-sites-that-stand-to-lose-the-most/#7c4aca7134ec. [Online; accessed 01-2019].

Chepurnoy, A. (2016). Some open problems in blockchains. https://www.slideshare.net/AlexChepurnoy/some-open-problems-in-blockchains. [Online; accessed 01-2019].

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., et al. (2016). On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*, pages 106–125. Springer.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

De, N. (2017). Colored Coins startup Coinprism is shutting down. https://www.coindesk.com/blockchain-startup-coinprism-to-shut-down-in-2-days.

de la Rosa, J. L., Torres-Padrosa, V., el Fakdi, A., Gibovic, D., Hornyák, O., Maicher, L., and Miralles, F. (2017). A survey of blockchain technologies for open innovation. In *4rd Annual World Open Innovation Conf. WOIC*, pages 14–15.

Desouza, K. C. and Somvanshi, K. K. (2018). How blockchain could improve election transparency. https://www.brookings.edu/blog/techtank/2018/05/30/how-blockchain-could-improve-election-transparency/. [Online; accessed 01-2019].

Dixon, C. (2018). Why decentralization matters. https://medium.com/@cdixon/why-decentralization-matters-5e3f79f7638e. [Online; accessed 01-2019].

Dunietz, J. (2018). Are blockchains the answer for secure elections? probably not. https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probably-not/. [Online; accessed 01-2019].

El Ioini, N. and Pahl, C. (2018). A review of distributed ledger technologies. In *OTM Confederated International Conferences on the Move to Meaningful Internet Systems"*, pages 277–288. Springer.

Ethereum-Problems (2019). Ethereum/wiki: Problems. https://github.com/ethereum/wiki/wiki/Problems.

EU-TRL (2019). Technology readiness level. "https://en.wikipedia.org/wiki/Technology_readiness_level ".

Frisby, D. (2018). Blockchain technology will revolutionize far more than money. https://aeon.co/essays/how-blockchain-will-revolutionise-far-more-than-money. [Online; accessed 01-2019].

Gartner (2019). Reviews for blockchain platforms. https://www.gartner.com/reviews/market/blockchain-platforms.

Gens, F., Prete, C. D., Matsumoto, S., and Carter, P. (2017). Idc futurescape: Worldwide it industry 2018 predictions. https://www.idc.com/getdoc.jsp?containerId=US43171317. [Online; accessed 01-2019].

Greenspan, G. (2016). Four genuine blockchain use cases. https://www.coindesk.com/four-genuine-blockchain-use-cases/. [Online; accessed 01-2019].

Griffin, T. (2016). Two powerful mental models: Network effects and critical mass.

Hamida, E. B., Brousmiche, K. L., Levard, H., and Thea, E. (2017). Blockchain for enterprise: overview, opportunities and challenges. In *The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017)*.

Hatmaker, T. (2018). Senate cryptocurrency hearing strikes a cautiously optimistic tone. https://techcrunch.com/2018/02/06/virtual-currencies-oversight-hearing-sec-cftc-bitcoin/. [Online; accessed 01-2019].

He, P., Yu, G., Zhang, Y., and Bao, Y. (2017). Survey on blockchain technology and its application prospect. *Comput. Sci*, 44(4):1–7.

Iansiti, M. and Lakhani, K. (2017). The truth about blockchain. https://hbr.org/2017/01/the-truth-about-blockchain. [Online; accessed 01-2019].

ICO (2017). Initial coin offering (ico). https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp. [Online; accessed 01-2019].

Johnson, S. (2018). Beyond the bitcoin bubble. https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html. [Online; accessed 01-2019].

Kasireddy (2017a). Blockchains don't scale. not today, at least. but there's hope. https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a. [Online; accessed 01-2019].

Kasireddy (2017b). Fundamental challenges with public blockchains. https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428. [Online; accessed 01-2019].

Kharif, O. and Bergen, M. (2018). Google is working on its own blockchain-related technology. https://www.bloomberg.com/news/articles/2018-03-21/google-is-said-to-work-on-its-own-blockchain-related-technology. [Online; accessed 01-2019].

Legislation (2018). Blockchain state legislation. http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx. [Online; accessed 01-2019].

Lin, I.-C. and Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *IJ Network*

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

Security, 19(5):653–659.

Mallik, G. and Chowdhury, A. (2001). Inflation and economic growth: evidence from four south asian countries. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.516.9478rep=rep1type=pdf. [Online; accessed 01-2019].

Masters, C. (2019). Ethereum hard fork explained. https://cryptovest.com/education/ethereum-hard-fork-explained/.

Mayer, D. (2018). Blockchain voting notches another success—this time in switzerland. http://fortune.com/2018/07/03/blockchain-voting-trial-zug/. [Online; accessed 01-2019].

Meola, A. (2017). The growing list of applications and use cases of blockchain technology in business & life. https://www.businessinsider.com/blockchain-technology-applications-use-cases-2017-9. [Online; accessed 01-2019].

Panarello, A., Tapas, N., Merlino, G., Longo, F., and Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. *Sensors*, 18(8):2575.

Partz, H. (2018). SEC launches mock ico to show investors warning signs of fraud. https://cointelegraph.com/news/sec-launches-mock-ico-to-show-investors-warning-signs-of-fraud. [Online; accessed 01-2019].

Perera, S. (2018). Emerging technology analysis canvas (etac). https://github.com/wso2/ETAC/blob/master/ETAC.md. [Online; accessed 01-2019].

Permissioned (2018). The case for permissioned blockchains. https://blocksplain.com/2018/02/07/permissioned-blockchains. [Online; accessed 01-2019].

Quantum-computing-And-Bitcoin (2019). Quantum computing and bitcoin. https://en.bitcoin.it/wiki/Quantum_computing_and_Bitcoin .

Reed, D. et al. (2017). Decentralized identifiers (dids). *W3C, Credentials Community Group*.

Reiff, N. (2018). Top blockchain startups to watch in 2018. https://www.investopedia.com/news/top-blockchain-startups-watch-2018/. [Online; accessed 01-2019].

Rogers, E. M. (2010). *Diffusion of innovations*. Simon and Schuster.

Ross, S. (2018). How can inflation be good for the economy? https://www.investopedia.com/ask/answers/111414/how-can-inflation-be-good-economy.asp. [Online; accessed 01-2019].

Savage, C. (2018). Congress approves six-year extension of surveillance law. https://www.nytimes.com/2018/01/18/us/politics/surveillance-congress-snowden-privacy.html. [Online; accessed 01-2019].

SEC (2018). How SEC's paragon ruling could send many crypto icos to bankruptcy. https://www.ccn.com/how-secs-paragon-ruling-could-send-many-crypto-icos-to-bankruptcy/. [Online; accessed 01-2019].

Stark, H. (2017). Keep an eye on these blockchain startups throughout 2018. https://www.forbes.com/sites/haroldstark/2017/12/12/keep-an-eye-on-these-blockchain-startups-throughout-2018/#6e3efd0413e6. [Online; accessed 01-2019].

Sternberg, H. and Baruffaldi, G. (2018). Chains in chains–logic and challenges of blockchains in supply chains. In *Proceedings of the 51st Annual Hawaii International Conference on System Sciences*, pages 3936–3943.

Stinchcombe, K. (2018). Ten years in, nobody has come up with a use for blockchain. https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100. [Online; accessed 01-2019].

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. "O'Reilly Media, Inc.".

Tapscott, A. T. D. (2017). How blockchain is changing finance. https://hbr.org/2017/03/how-blockchain-is-changing-finance. [Online; accessed 01-2019].

VC (2017). Blockchain venture capital. https://www.coindesk.com/bitcoin-venture-capital/. [Online; accessed 01-2019].

Walden, D. N. J. and Zuegel, D. (2018). Crypto and the evolution of open source. https://a16z.com/2018/08/20/crypto-evolution-open-source-libraries-services/. [Online; accessed 01-2019].

Yli-Huumo, J. et al. (2016). Where is current research on blockchain technology? a systematic review. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5047482/. [Online; accessed 01-2019].

Zakon, R. H. (2018). Hobbes' blockchain timeline 0.1. https://www.zakon.org/robert/blockchain/timeline/.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019

[Online; accessed 01-2019].

Zamani, M., Movahedi, M., and Raykova, M. (2018). Rapidchain: scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 931–948. ACM.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4):352–375.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27529v1 | CC BY 4.0 Open Access | rec: 11 Feb 2019, publ: 11 Feb 2019