Applications of Blockchain Beyond Cryptocurrencies - Value, Systems, and Challenges

Adrian Adduci
Columbia University
Email: FAA2160@columbia.edu

Seong Hun Park
Columbia University
Email: SP3440@columbia.edu

Kofi Amansie-Boateng
Columbia University
Email: KA2461@columbia.edu

Clement Chin
Columbia University
Email: KC3168@columbia.edu

Blockchain technology is most widely known for enabling the creation of crypto-currencies, with some of the most notable examples being Bitcoin and Ethereum. However, since their creation, crypto-currencies have primarily operated as a medium for the storage of value and have seen only peripheral use as a traditional currency. That said, the underlying technology of blockchain could and should have utility in many other domains. In our paper, we have surveyed the spectrum of blockchain solutions implemented in various industries. We've provided a particular focus on applications beyond currencies, looking at the finance industry, healthcare, and politics to understand what systems are used and how the technology will change the current techniques used in the industry.

1 Introduction

Blockchain technology made its public debut back in 2008 when Satoshi Nakamoto first released a whitepaper on Bitcoin. Since then, blockchain technology has developed and evolved into the one which can impact and transform many industries, far beyond its initial crypto-currency application. [1]

It is a common misconception that blockchain is synonymous with bitcoin, and they are one and the same. However, as the news of this technology spreads with the rise of bitcoin, industry players started to take note of the value of this technology. These players have seen the potential in using blockchain to transform existing practices and offerings. More applications are being envisioned with blockchain, and with more applications, the technology itself also experienced many changes. The initial blockchain algorithm introduced by Satoshi only provided a foundation for newer implementations and further variations that have given way to new features to suit the vastly different needs of the industry.

In this report, we seek to highlight the different innovative applications of blockchain in the industry and provide a broader sense of how the blockchain systems are in a non-crypto currency setting. We will describe how these applications differ from the traditional way of performing the transaction without blockchain, along with its benefits and drawbacks. In addition, the report will also bring attention to some of the challenges in implementing blockchain in the industry and some future trends that might shape the industry.

2 Examples of Blockchain Applications beyond Crytocurrency

As blockchain technology gains prominence in the industry, organizations and technology services firms start to realize its potential value and begin to experiment with different interesting applications of blockchain to solve their business pain points (see 2.1 Finance and Banking), improve transparency and efficiency (see 2.2 Supply Chain), or even create entirely new revenue stream (see 2.3 Digital Assets).

In this section, we briefly introduce the innovative ideas which organizations are implementing, on a high level. Then in subsequent sections 4, 5, and 6, we will dive deeper into three specific non-cryptocurrency application of blockchain.

2.1 Finance and Banking

2.1.1 Back office Settlement

Large financial institution are thinking about using blockchain technology to improve the efficiency of clearing and settlement. In clearing houses, it is typically managed through a myriad of messages and manual reconciliation, providing opportunity for blockchain to restructure that process. [2]

In addition, there are also efforts and proposals to use blockchain to automate debt servicing and factoring, insurance, and other labour- and verification-intensive business processes. For example, in niche syndicated loan market, where a group lenders work together to provide funding to a single borrower, blockchain can also be applied to replace the inefficient back-office procedures, by the loan terms and agreement all programmed within the blockchain itself. [3]

2.1.2 Know Your Customer - KYC

Group of banks can create a consortium blockchain, which is ledger that keep tracks about all necessary information about creditors. This information is commonly collected and stored, and once a bank needs the information to assess a customer, the bank can retrieve it from the distributed ledger. Permission to retrieve information from the blockchain can be also be programmed into the system using smart contracts.

Information on the Blockchain can be used by other banks and other accredited organizations (such as insurers, car rental firms, loan providers etc.) without the need to ask the customer to start the KYC process all over again, essentially a form of crowd sharing. This will greatly reduce the administration burden for many of the organizations, and the customer will only need to supply updated information to one channel, and provide consent to each company that would like to access the data. [4]

2.2 Supply Chain

2.2.1 Food Supply

Blockchain can be used to allow retailers and consumers to track the provenance of meat and other food products from their origins to stores and restaurants. Companies like Walmart and IBM are running trials to use blockchain for monitoring of lettuce and spinach. The technology gives them full trace-ability of each item's origin and route to the store, and allows for precise recall management in time of outbreak like E.Coli. This ability could potentially help save costs as the retailer only has to discard food that are at risk. [5]

2.2.2 Pharmaceuticals

The pharmaceutical industry is known to be heavily regulated, as it deals with life savings medicines vaccines. Counterfeit products regularly appear in the market, which could result in adverse health issues. [6] Authorities such as the US FDA are partnering with large pharma is piloting blockchain technology to track and trace the drugs, all the way from ingredients suppliers to manufacturers to logistics partners, to hospitals and pharmacists. [7]

2.3 Digital Assets

2.3.1 Music Distribution

A peer-to-peer blockchain-based system where artists can share their music directly with music fans will remove intermediaries like large label companies and platforms. Through smart contracts, artists can be paid directly upon the purchase or stream of a song. [8]

Blockchain-backed systems can also create monetary incentives for music fans, creating interactive experiences. For example, fans that create the most popular playlists or contributing the latest music events information can be rewarded automatically with Smart Contract. [8]

2.3.2 Video Game Distribution

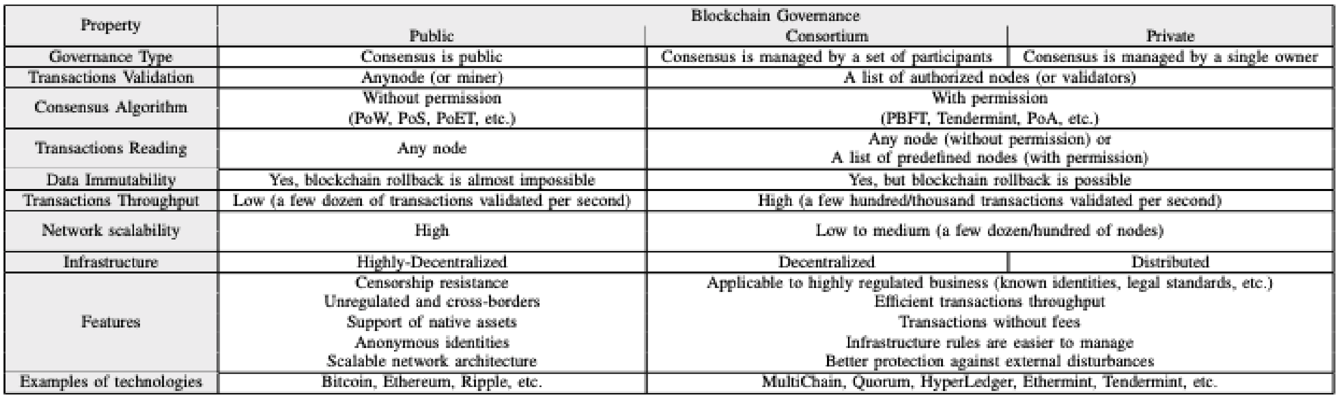
Similar to the music industry, blockchain could redefine the Video Game industry. In this case, apart from just indie developers getting direct access to gamers, there are a plethora of additional functions that could ride on the blockchain system.
One example is to have cryptocurrency tied to in-game currency, enabling ease of virtual assets purchase or sale. Virtual assets can have stable real-world value as the item which resides on a blockchain will no longer have the risk of being tampered with or manipulated by the developers. Blockchain takes in-game assets and makes them as ownable as possible, creating legitimacy and permanent value. Granting immutable ownership of in-game items, solving item theft due to hacking, and the sale of fake in-game assets. [9]

3 Consortium-based Blockchain

3.1 Types of Blockchain

When Satoshi first invented bitcoin, the technology was used mainly for public type blockchain, where there is no restriction for new participants to join. Public Blockchain is by far the most widely adopted type of blockchain where many cryptocurrencies such as Bitcoin (BTC) and Ethereum (ETH) uses [10].

Although the concept of public blockchain has its merits, two other types of blockchain were established to address the industry's needs in implementing blockchain, namely Private and Consortium blockchain, each of these has different features which might be more suitable depending on the application. On one side, there is Public blockchain, which is accessible to everyone, and on the other side, there is Private blockchain, which is usually set up and services only



Property	Blockchain Governance		
	Public	Consortium	Private
Governance Type	Consensus is public	Consensus is managed by a set of participants	Consensus is managed by a single owner
Transactions Validation	Anynode (or miner)	A list of authorized nodes (or validators)	
Consensus Algorithm	Without permission (PoW, PoS, PoET, etc.)	With permission (PBFT, Tendermint, PoA, etc.)	
Transactions Reading	Any node	Any node (without permission) or A list of predefined nodes (with permission)	
Data Immutability	Yes, blockchain rollback is almost impossible	Yes, but blockchain rollback is possible	
Transactions Throughput	Low (a few dozen of transactions validated per second)	High (a few hundred/thousand transactions validated per second)	
Network scalability	High	Low to medium (a few dozen/hundred of nodes)	
Infrastructure	Highly-Decentralized	Decentralized	Distributed
Features	Censorship resistance Unregulated and cross-borders Support of native assets Anonymous identities Scalable network architecture	Applicable to highly regulated business (known identities, legal standards, etc.) Efficient transactions throughput Transactions without fees Infrastructure rules are easier to manage Better protection against external disturbances	
Examples of technologies	Bitcoin, Ethereum, Ripple, etc.	MultiChain, Quorum, HyperLedger, Ethermint, Tendermint, etc.	

Fig. 1. Classifications of blockchain

one enterprise. In between those two, there is the Consortium blockchain, which is a hybrid of the two types. Refer to Fig. 1.

Despite the expected benefits afforded by blockchain design, the Public blockchain, in particular, is not suited for many of the enterprise applications due to its weakness in transaction throughput, inability to rollback, and anonymous identity. A Private blockchain is also not suitable, as it can be seen as just a ”traditional centralized system with a degree of cryptographic auditability attached” [11], abandoning one of the most significant value of the blockchain that is establishing trusted data validated by multiple parties.

With all things considered, a Consortium blockchain type is typically the choice for multi-enterprise collaborative applications, as it has the following advantages [11]:

1. Consortium blockchain has greater privacy since the information from verified blocks is not exposed to the public but is admissible for the consortium members. It creates a larger level of trust and confidence for clients of the platform.
2. A consortium platform is more flexible. The tremendous number of validators in public blockchain leads to troubles with synchronization and mutual agreement. Often, this divergence can lead to forks but not in the consortium.
3. Furthermore, Consortium blockchain is under full control of a particular group but is protected from monopoly. When each member agrees, this control enables us to establish own rules, change or cancel erroneous transactions, modify balances, and perform other actions to foster fruitful cooperation for companies with a common purpose.
4. Proof-of-Vote (PoV) type of consensus requires negligible energy. As there is no mining involved, no energy and resource is wasted on unproductive activities.
5. Furthermore, since the PoV consensus, a relatively small number of nodes are reached in accordance with the governance scheme. This type of consensus is also much less demanding and easier to reach. This in turn, results in Consortium blockchain having higher performance (confirmation time and throughput).

3.2 Rewards

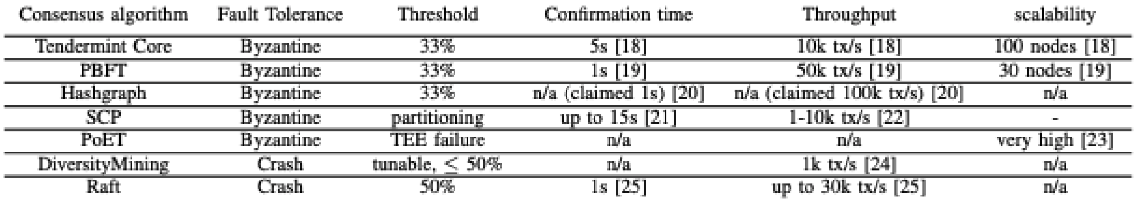
In a typical crypto-currency setting, the Public blockchain protocol consists of a reward mechanism that is used to incentivize participants to perform the necessary action that maintains the liveness and consistency of the chain. Those activities include things like finding the right nonce adding transactions to the block and subsequently adding the block to the main chain. Miners are in a competition to add the next block. For instance, in Bitcoin and Ethereum, the miners have performed a computationally demanding cryptographic puzzle to prove their work. They are then rewarded with the block reward and transaction fee for the effort.

However, with Consortium blockchain, there is typically no such reward mechanism (no block reward, nor transaction fee). This is because validators (instead of miners) in a Consortium blockchain are preliminary known according to the governance scheme and are already trusted to a certain degree. [12]. There are mechanisms to add and remove validators, but those are always under the control of existing validators. Furthermore, in a consortium, each member has an innate incentive to want the chain to remain healthy. For example, in a consortium of banks that collaborate to trade cross borders with blockchain, each member is willing to participate by having their nodes connected and perform the validation without a need for a reward. The reward of participating in the blockchain activity inherently comes in the form of greater business efficiency and transparency.

3.3 Consensus Algorithms

In Public blockchain, the proof of work (PoW) is used to achieve consensus. The PoW algorithm does not require all parties on the network to submit their individual conclusions to reach a consensus. Instead, it creates a condition in which a single participant is permitted to announce their conclusion, which is then independently verified by all other participants. The PoW method allows for easy and broad participation with minimal requirements for each participant, allowing them to remain anonymous. [13]

For Consortium blockchains, since the consortium is permissioned, only a predetermined group of enterprises can participant, which means these participants have some level



Consensus algorithm	Fault Tolerance	Threshold	Confirmation time	Throughput	scalability
Tendermint Core	Byzantine	33%	5s [18]	10k tx/s [18]	100 nodes [18]
PBFT	Byzantine	33%	1s [19]	50k tx/s [19]	30 nodes [19]
Hashgraph	Byzantine	33%	n/a (claimed 1s) [20]	n/a (claimed 100k tx/s) [20]	n/a
SCP	Byzantine	partitioning	up to 15s [21]	1-10k tx/s [22]	-
PoET	Byzantine	TEE failure	n/a	n/a	very high [23]
DiversityMining	Crash	tunable, $\leq$ 50%	n/a	1k tx/s [24]	n/a
Raft	Crash	50%	1s [25]	up to 30k tx/s [25]	n/a

Fig. 2. Variations of the consensus protocol

of trust. Since the consortium is permissioned, each participant's identity is known, so if any of the participants perform fraud or illegitimate transactions and are caught, the reputation of the organization will be impacted. This is a powerful deterrent. Since validation is only conducted by known and identified members of a limited network of nodes, this eliminates the danger of 51% attack. As a rule, violators are identified immediately and lose more than benefit from their dishonest behavior. Moreover, other known attacks are irrelevant to the consortium blockchain, including DDoS, "man in the middle" attack, and SQL injection [11].

Even though the trust is higher (and the risk of fraud significantly lower) among the consortium members vs. an open public group, there can still be inconsistencies during a blockchain network's operation. Therefore some form of Proof-of-Vote type algorithms are still needed to achieve consensus on the blockchain's status, consistent view of the blocks committed.

Referring to Fig. 2, there are several key differences and metrics that we can use to assess the different algorithms.Firstly, is the fault tolerance, where some algorithms can only survive crashes, and some are able to handle rogue nodes that provides contradicting signals (achieving Byzantine Fault tolerance), the threshold by which each algorithm can handle these faults varies as well. Next, the performance of the algorithm is also a differentiator, where some have confirmation time of just a second, and some go up to 15 seconds; the throughput of each also varies by few order of magnitude. Lastly is the scalability of the algorithm, how many nodes can this algorithm handle without breaking.

Considering each algorithm has its pros and cons, it is not surprising that each of them is used in different blockchain platforms.

3.4 Selection of Platform

When a group of organizations get together and decide on building a consortium-based blockchain, a pivotal decision is which blockchain platforms to use as the base to build the application that can serve the needs of the consortium. Each of these platforms uses a different underlying consensus algorithm.

Several criteria for evaluation of the most suitable blockchain system are [14]:

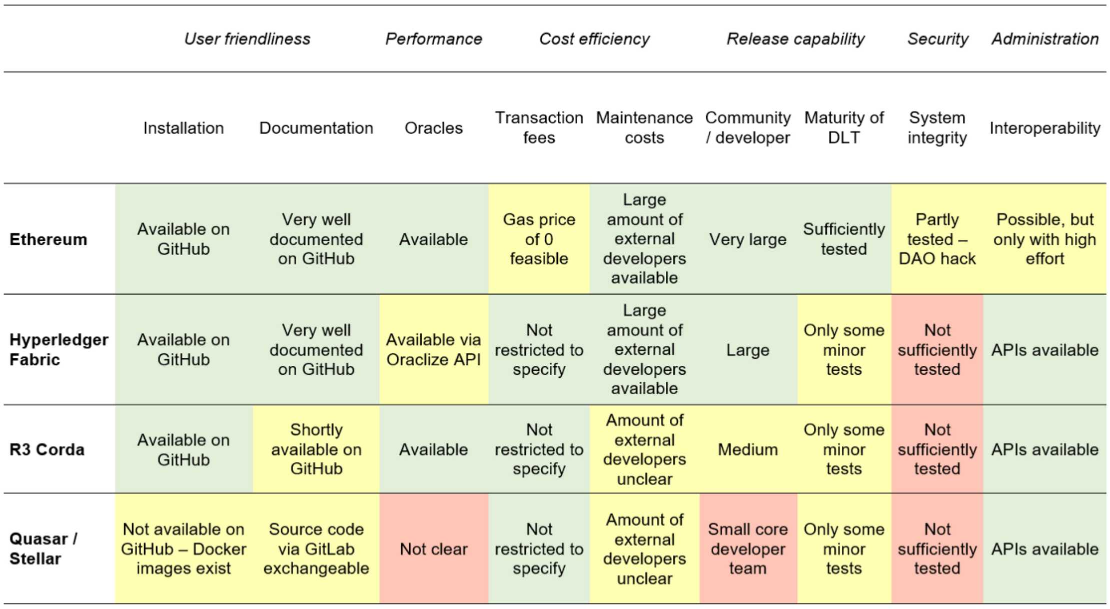
1. **Installation / user-friendliness** - How easy is the installation process? How well is it documented?
2. **Efficiency / performance** - What are maximum block sizes? Can several transactions be conducted simultaneously?
3. **Cost efficiency** - How large are costs for transactions and maintenance?
4. **Release capability / up-to-dateness** - How mature is the technology? How large is the developer community?
5. **Security / safety** - How secure is the blockchain system?
6. **Administration** - How modular is the respective framework? Is interoperability guaranteed?

Each of the blockchain platforms has its strengths and weaknesses, see Fig. 3, usually depending on the application and area of focus of its founders. The more a platform may be generally better in user-friendliness and documentation, due to a more extensive contributor base, creating how-to guides. However, smaller and rising platforms might offer specific niche functionality that might not be available in others.

It is up to the Consortium to jointly decide which best suits their needs—considering the maturity and number of blockchain integration developers the group has, the scalability and performance needs of the application, and whether it has specific requirements such as transaction access rights control.

For example, Hyperledger Fabric allows multiple participants to operate on the blockchain system, while transactions are only visible to relevant stakeholders. By having the channel functionalities, a consortium can use a single blockchain platform like Hyperledger for different use cases and make sure that the individuals' privacy concerns are taken care of. Specifically, in Hyperledger Fabric, it is possible to channel connections between organizations so that the transactions are hidden from other participants on the blockchain. This possibility protects data from unintended sharing with others. [14] Furthermore, Hyperledger comes with a modular system architecture that allows developers to add other modules, such as an identity module, quickly into the system. Another one is called "Membership Service Providers" (MSP), where the rights of each participant can be easily managed. The certificate authority can create, sign, deposit, and revoke X.509 certificates, granting the individual participants certain rights in the network. Further, the MSP can be connected to the organization's identity management system.

All of these unique features that might not exist in other platforms makes Hyperledger Fabric one of the popular choice for permission based blockchains. [**?**]



	User friendliness		*Performance*	*Cost efficiency*		*Release capability*		*Security*	*Administration*
	Installation	Documentation	Oracles	Transaction fees	Maintenance costs	Community / developer	Maturity of DLT	System integrity	Interoperability
Ethereum	Available on GitHub	Very well documented on GitHub	Available	Gas price of 0 feasible	Large amount of external developers available	Very large	Sufficiently tested	Partly tested – DAO hack	Possible, but only with high effort
Hyperledger Fabric	Available on GitHub	Very well documented on GitHub	Available via Oraclize API	Not restricted to specify	Large amount of external developers available	Large	Only some minor tests	Not sufficiently tested	APIs available
R3 Corda	Available on GitHub	Shortly available on GitHub	Available	Not restricted to specify	Amount of external developers unclear	Medium	Only some minor tests	Not sufficiently tested	APIs available
Quasar / Stellar	Not available on GitHub – Docker images exist	Source code via GitLab exchangeable	Not clear	Not restricted to specify	Amount of external developers unclear	Small core developer team	Only some minor tests	Not sufficiently tested	APIs available

Fig. 3. Different frameworks of blockchain

3.5 Governance, Updates, Rules Establishment

In a public blockchain, governance is maintained by a small group of maintainers/contributors. As the code of this public blockchain is usually stored in a public repository such as GitHub, such as Bitcoin [15]. For significant changes, the public blockchain like Bitcoin uses a voting mechanism to decide if the proposed code change should be adopted.
BIP stands for Bitcoin Improvement Proposal, and a BIP instance is essentially a document that proposes changes to the core bitcoin technology. They are the standard way of communicating ideas — given that Bitcoin has no formal means. Miners can vote for or against a BIP by including the appropriate data in their hashed block.
Depending on the BIP "Layer" specification, a BIP acceptance may signal a "soft fork" upgrade wherein the community members (exchanges, companies building payment technologies, exchanges, miners, etc..) must upgrade their versions of the protocol to allow for the newly built functionality. structure. [16]

The situation, however, is entirely different for Consortium blockchain. Consortium blockchain operates under the leadership of a group of entities. Core members of the group (usually the founding members) will form the members of the Governance Board. As the number of members in the consortium grows, it gets difficult to discuss and agree upon changes, hence the board will decide and act on behalf of the consortium, they are tasked to decide on the operating rules and any changes to be implemented to the blockchain, as illustrated in Fig. 4. Nevertheless, every member of the consortium still has a way to communicate their proposals to the committee.

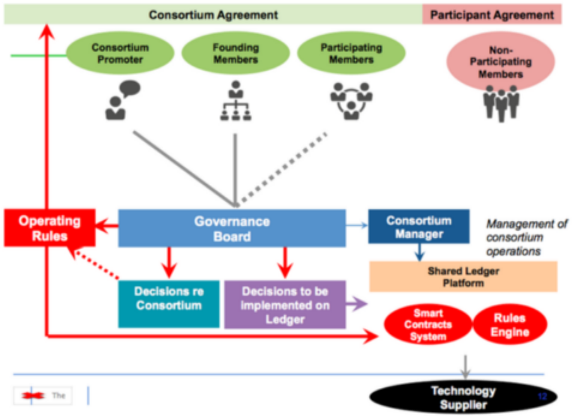


Fig. 4. Consortium Blockchain Strategy

4 Application 1 - Crypto Securities

Crypto currencies and associated payment systems have taken up a substantial amount of focus in the financial industry. That said, an early extension of blockchain beyond currency applications has been in the attempted adoption of 'crypto securities' or adapting traditional financial instruments such as loans, stocks, and bonds to utilized blockchain technology in lieu of conventional capital markets infrastructure.

Like the ubiquitous financial instruments, many investors are familiar with, crypto securities are exclusively the domain of corporations looking for financing from investors. While only a few examples of crypto securities have been publicized for reasons we will address, the motivations for implementing a crypto security are apparent. The current infrastructure that allows for the flow of capital through the financial system is complex and incorporates a multitude of counter-parties that exist to help bridge participants who wish to do business with one another. This leads to both a lack of transparency and added cost and overhead with little benefit to end-users in a transaction (i.e., the parties buying and selling security). This situation has many similarities to those that gave rise to the blockchain.

In this section, we will briefly outline the existing infrastructure that traditional financial securities rely on to give context for an alternative application that relies on blockchain technology. We will then step through one such example, the first 'crypto bond' ever introduced to the market by Overstock.com in 2015, and then outline the challenges and potential catalysts for broader adoption by the financial industry.

4.1 Current Market Participants and Impact of Disintermediation

The global financial system is massive, and the infrastructure supporting financial transactions is equitable in scale. For purposes of relating the implementation of a blockchain to a traditional financial instrument, we'll look at a simplified version of the financial system by splitting the process of transacting into two categories, the movement of cash and the movement of assets (e.g., stocks, bonds). From there, we will focus solely on the movement of assets through a generic version of Capital Markets Infrastructure (CMI). However, one should keep in mind that for every asset movement through the plumbing of the global financial system, there is a complimentary movement of cash in a different part of the banking system.

Figure 5. outlines a generalized Securities Transfer Model (STM) of the various participants in the capital markets, and that help instigate the trading of capital (i.e., money) for the securities such as stocks and bonds in a. Some of these entities may look familiar, but it will become apparent that the pipes and plumbing of financial markets still reflect a patchwork of antiquated layers created to address historical problems of dealing with two entities that want to do business with one another without any assurances of trust.

The specific role that each of the participants above plays goes beyond the scope of our discussion here. That said, for purposes of our discussion, note that these various entities undertake roles such as buying the traditional securities on behalf of an owner, confirming and updating the ownership of existing security, holding capital to transact as well as the actual security, and passing along legal or regulatory notifications. Also, note that many of these responsibilities may be directly replaced with the blockchain. An outline of the potential simplification of the underlying infrastructure has been provided.

For discussion purposes, one technical aspect of security trading that is integral to understanding the importance of leveraging a blockchain solution for the finance industry is the concept of an Alternative Trading System (ATS). An ATS is a trading system that meets the definition of "exchange" under the United State's federal securities laws but is not required to register as a national securities exchange. [18]

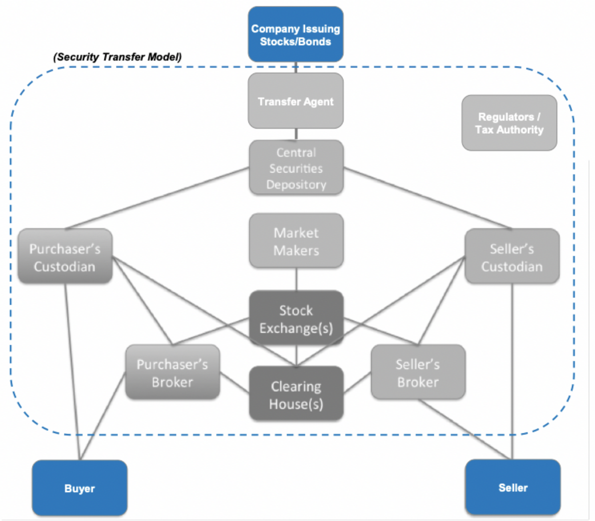


Fig. 5. Example of parties involved in the transfer of securities [17]

Crypto securities are not yet recognized under a specific legal framework in securities law's highly regulated space. It is essential to realize that buying and selling securities is being done in an alternative forum designed for esoteric assets that do not fit neatly existing frameworks. Importantly, it limits participants to only large, sophisticated investors. This discussion will focus solely on the Security and Exchange Commission's (SEC) version of an ATS and does not address similar frameworks that may exist in other jurisdictions.

4.2 Overstock.com's 2015 Inaugural Crypto Bond

The first crypto bond issuance was driven by Overstock.com (OSTK) and OSTK's CEO Patrick Byrne in 2015. At the time, Byrne's goal was "[to build] things that replace what Wall Street does... [do] them far cheaper, and with far more transparency, and without any of the opportunity for rigging" [19]. With the ultimate belief that " crypto technology can do for the capital market what the internet has done for consumers." [20]

The crypto bond OSTK issued that we will discuss ultimately designed as a proof of concept [21]. It was smaller in scale, at only $5 million in total size, and pre-arranged to be distributed to an investor, FNY Managed Accounts. Additionally, there were complementary arrangements in place in case the underlying technology failed in some fashion. That said, Byrne and OSTK still did more than leverage existing technology in a novel way. They built a platform with the expectation that this application could be replicated and hopefully built upon in the future.

4.3 Implementation and Execution of the Application

To marry blockchain technology with the existing systems built for trading financial products, OSTK first acquired an ATS, which would allow them the legal ability to match buy and sell orders from market participants. The ATS, known as PRO Securities LLC, gave OSTK the legal power to buy and sell their crypto bond as a financial instrument.

Additionally, as an ATS is a regulated framework for securities trading, OSTK also implemented a front-end trading system that users could utilize submit actions such as buy and sell orders. It could also handle pertinent issues to both the blockchain and securities law, such as Know Your Customer regulations. This front-end order management system is known as DriveWealth. The requirement that users are registered with DriveWealth effectively makes the OSTK system a permissioned space. The system which coordinates between the ATS and DriveWealth is known as TØ. Lastly, there remains a third party entity responsible for validating ownership of financial securities known as the Trustee. While there is no physical delivery of a security under the OSTK system like there would be in traditional financial security, OSTK still utilizes a Transfer Agent. In this case, Continental Stock Transfer Trust Co., to validate the proprietary ledger of cryto bond owners against the public blockchain [22].

4.4 Technical Details of Implementation

Here, we will walk through the life cycle of a transaction, from a participant registering with DriveWealth, entering an order, and finally matching an order (e.g., buying a crypto bond) with an offer (e.g., selling a crypto bond).

4.4.1 On-Boarding

As this is a closed system where trading partners must be validated for regulatory purposes, the first step to implementation is on-boarding. Here, the user is opening an account and ensuring legal compliance as a participant on the ATS. Importantly, two digital wallets are also created. A Portfolio Wallet and a Committed Wallet, along with unique customer [22]. Technical details of the digital wallets are not discussed in detail throughout the rest of this paper. However, to understand the TØ ecosystem, they may be viewed as equivalent to other known digital wallets that tracks a user's account balances and transactions across the Bitcoin blockchain.

4.4.2 Placing an Order

Placing an order for the crypto bond looks analogous to any securities trading software. A user logs into the DriveWealth front-end system, validating their permission to participate on the ATS and buy or sell the crypto bond. The front-end system pulls and displays information from the ATS, including eh current market prices of the security, current account holdings. Importantly, all market data is anonymous, which means parties trading with one another on the ATS do not know who their counterparty is, similarly to a traditional securities exchange [22]. At this point, a user may enter a trade.

After the user enters a trade for the cryto bond, the DriveWealth system validates the customer's identification and availability of fundings as well as the user's Committed Wallet. The Committed Wallet at this stage represented both the current holdings of the user as well as pending transactions. From here, the order is routed to the ATS for matching with a complimenting order from another party.

4.4.3 Matching

After the ATS receives the order, the ATS reviews the current list of available securities willing that can be bought or sold and at what available price. This process is identical to what may be found in a typical securities exchange, with some additional nuances for identifying the best match given potentially less availability of securities for sale or willing to be bought. When a suitable match is found, for example, a buy order for a specific quantity of crypto bonds at a particular price finds a complementary sell order of the same amount. At the same price, the order moves on to execution.

4.4.4 Execution

Once a match has occurred, the ATS identifies the Committed Wallet's unique identifications and Portfolio Wallets of the participating parties. A deduction is made in the buyer's Committed Wallet, and the security is moved to the portfolio wallet, and a complementing transaction is made in the seller's wallets. The trade is then recorded in the ATS's proprietary ledger. At this point, the ATS creates what's known as the Anchor Data which will be included in the public blockchain of Bitcoin. In bitcoin's case, this anchor data will be included in an upcoming transaction in the 'op-return' field. While specifics of the anchor data are not available, it is likely that the system uses something akin to a Merkel root to represent the transactions on the ATS's proprietary ledger

At this point, the ATS makes a small de minimus transaction on the public blockchain, transferring a small amount of Bitcoin between two wallets owned by the ATS and including the Anchor Data as part of this transaction. At that point, the public blockchain will now have a record of the activity that occurred on the ATS. However, only the ATS and, subsequently, the users of the front-end system will be able to interpret the activity through the proprietary ledger.

Once the transaction is added to confirmed by the public network and added to Bitcoin's blockchain, the ATS confirms the transaction on its proprietary ledger. At this point, a snapshot of the proprietary ledger is provided to the Transfer Agent who is able to compare against the public blockchain. If the transaction is not confirmed, it is held as pending until either cancellation or confirmation.

Figure 6 below is a diagram representing the interaction of the ATS concerning Bitcoin's blockchain and subsequent steps for validating a transaction.

At this point, subsequent trade confirmations followed protocols akin to typical financial securities settlement. The Transfer Agent would take responsibility for confirming payment, confirming ownership of individual securities, and adhering to other financial compliance and regulatory provisions.

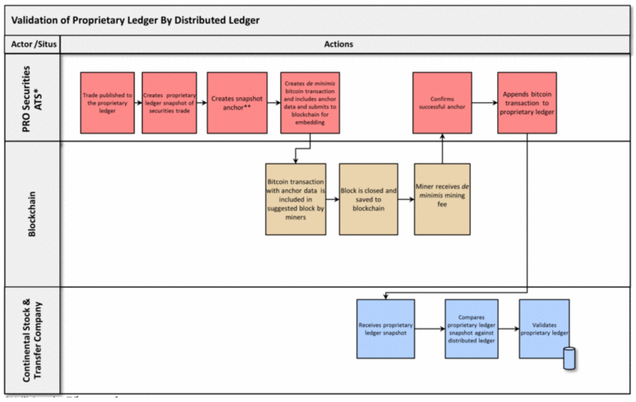

Validation of Proprietary Ledger By Distributed Ledger
Actor /Situs
Actions
PRO Securities ATS*
Trade published to the proprietary ledger
Creates proprietary ledger snapshot of securities trade
Creates snapshot anchor**
Creates de minimis bitcoin transaction and includes anchor data and submits to blockchain for embedding
Confirms successful anchor
Appends bitcoin transaction to proprietary ledger
Blockchain
Bitcoin transaction with anchor data is included in suggested block by miners
Block is closed and saved to blockchain
Miner receives de minimis mining fee
Continental Stock & Transfer Company
Receives proprietary ledger snapshot
Compares proprietary ledger snapshot against distributed ledger
Validates proprietary ledger

Fig. 6. Validating a crypto bond transaction [22]

4.5 Challenges and Successes of Implementation

As discussed, the system was developed as a template that could be scaled up into a true model for transacting around crypto securities. Underpinning this template is Bitcoin's original blockchain, which introduced many similar limitations to OSTK's system.

Firstly, certain limitations parallel's bitcoin's capacity to validate transactions across the blockchain. With a new coin being minted approximately every ten minutes, it may be challenging to publicly validate a market which sees tens if not hundreds of billions worth of transactions per day in the United States alone [23]. That said, OSTK's system does address this limitation successfully through its proprietary ledger, which is the accurate record of crypto bond transactions. As the public blockchain is used only for validating, not executing a successful transaction, there may be some ability to leverage this design to scale. Furthermore, even if a trade were to take the mining of several blocks to be recognized by the blockchain, this is a vast improvement in the typical three day settlement period the U.S. bond market currently operates under [22].

The second limitation relates to making pricing and market data a truly non-permissioned system. The gating factor for a market participant in OTSK's system is that they must be a sophisticated investor who must be vetted and validated before participating. This factor will inherently limit the total number of participants that can transact in the system, which will limit the amount of trading activity that can be accomplished. Furthermore, because you be approved to buy or sell the crypt bond, the current market prices and trading volumes be executed are not truly public data. This will limit the amount of perceived value in the crypot bond market, as it undercuts one of the core tenants of blockchain, which is transparency inactivity.

Ultimately the technical limitations on issuing crypto securities such as a crypto bond appear to be surmountable. The primary restriction remains the highly regulated nature of the financial industry as market participants are closely scrutinized for a myriad of reasons ranging from suitability of the investment (i.e., does this investor understand what they are doing) to law enforcement (e.g., money laundering). At this point, it is unclear where the current state of play is across global markets and the patchwork of regulatory agencies that oversee both individual markets (such as the bond and stock markets), individual exchanges, and national jurisdictions.

Lastly, what has not been addressed as another potential limitation is the ability to disintermediate the existing infrastructure, which drives financial markets. To move completing from the current system that leverages infrastructure from existing venues such as exchanges to banks that operate as the buys and sellers of securities for their clients (i.e. Broker-Dealers) and offering the plumbing to move traditional money across the globe may be challenging. The existing players are well embedded in a system that is already trusted to move vast sums of money and assets across the globe. Changing this system does not mean circumventing a few key players but an entire industry.

4.6 2020 Crypto Security Offering

While the original 2015 offering was meant as a proof of concept, OSTK has continued to further refine its blockchain solutions for crypto security trading. In 2018, Overstock.com amended one of its key regulatory filings to allow for the issuance of not just crypto bonds, but the tokenization of its preferred stock [24], demonstrating not only the commit to further leveraging blockchain to replace current financial infrastructure, but interest in the market to do so. In late 2020, the tokens went live and began trading on the T0 platform for accredited investors [25].

5 Application 2 - Electronic Health Records Using Blockchain - MedicalChain

Blockchain technology has also been employed in the space of medicine to keep secure electronic health records. In this section of the paper, we will be discussing how blockchain technology powers MedicalChain. MedicalChain is a decentralized platform that helps stakeholders such as doctors, hospitals, insurance providers,pharmacies and laboratories to interact with medical records securely and transparently. The blockchain technology used to power MedicalChain also ensures a single true version of a user's medical data. Users can also determine how the various stakeholders interact with the medical records since to a large extent the users can make certain fields in their health records visible and others invisible to different stakeholders (i.e., doctors, hospitals, etc). The underlying blockchain technology behind the MedicalChain infrastructure is the permission-based Hyperledger Fabric architecture, which allows varying access levels- this is the reason why the patient can control who is able to interact with his medical records, and for how long a stakeholder (doctor,pharmacy,etc) is able to interact with his record. Whenever there is any form of interaction with a user's data, it is recorded as a transaction on the distributed ledger of MedicalChain. This ensures that all such interactions are transparent and secure and can be audited at a later date.

5.1 Generic flaws with the mainstream healthcare infrastructure in general:

Building a permission-based blockchain network for electronic health records solves several of the mainstream healthcare industry's challenges. In this subsection, we detail a couple of the obstacles the mainstream healthcare industry faces.

5.1.1 Consistent hacking of medical records

Mainstream healthcare records today are mainly centralized and this is a recipe for a cyber attack on patient data. Storing health records in a centralized database, as is largely the case today, requires us to trust a single entity to keep medical records safe. Given the fact that medical records are in fact much more valuable than credit card numbers on the black market, there is a consistent effort by hackers to target the centralized databases of medical records. This causes the healthcare sector to consistently face data breaches . What makes the system worse is the fact that many countries around the globe have laws that force centralized health databases, which makes this risk even more rampant.

5.1.2. Insurance fraud:

Insurance claims are one of the major ways in which health care stakeholders (eg doctors, pharmacists) make a lot of money from patients. In the current mainstream healthcare infrastructure, it is easy, and also common for healthcare professionals to exaggerate a patients medical conditions such that their insurance claims go up. This has several negative effects on not only the patient, but his company who may be sponsoring his health insurance. The patient is forced to pay more for his healthcare due to his exaggerated medical conditions, and in many cases, that may mean that these patients, if they are poor, cannot afford healthcare. What is worse, entering a false information about a patients health may follow that patient as long as he lives, as it becomes a part of his insurance record for life. Thus the health insurer's record on a patient may not accurately reflect the medical records of a patient.

5.1.3.Varying versions of a patients health records, depending on the stakeholder

Healthcare records of old legacy systems are usually in different formats. This means that it is hard for one stakeholder, say a doctor, to share the healthcare records of a particular patient with a pharmacist, due to the different legacy systems. What this means is that each stakeholder usually keeps their own version of the truth concerning a patients health records. Thus a single patient's health record may vary from one stakeholder to another. This could easily lead to a situation where one stakeholder makes a bad prescription for a patient because he (the doctor) had an incomplete picture of the customer's health record over the years.

5.2 MedicalChain Solutions:

MedicalChain's electronic health record solution is mainly built on a blockchain structure to control and regulate how health stakeholders (the patient, doctors, pharmacies etc.) access health records. It is built using Hyperledger Fabric.

Hyperledger Fabric is a distributed ledger software that can be used for developing applications with a modular architecture. It is known for its unique approach to consensus that enables performance at scale while preserving privacy. [26]. The blockchain network is permissions-based. A new customer is required to sign up.

Patients consider their medical records as very highly confidential, and such highly confidential data must be kept as such. The Hyperledger Fabric allows such a high level of confidentiality concerning the patient's health data. The beautiful thing with this solution is that the patient himself can regulate how private his health records are. He can do so by controlling which part of his health records are visible to certain stakeholders (e.g., doctors, pharmacists, etc.).

A very important requirement for an electronic health record system is that it must successfully prevent hackers from impersonating other users or stealing their identities. To prevent identity theft, MedicalChain employs Civic's user authentication services to identify users uniquely. Civic is a personal identity verification protocol that leverages distributed ledger technology to manage better digital identities [26].

Its decentralized nature makes it ideal for blockchain protocols. MedicalChain employs Civic's biometric identification system, which provides a safe way of ensuring user privacy. This biometric verification makes it virtually impossible for a hacker to impersonate another user of MedicalChain.

5.3 Technical details of MedicalChain solution :

5.3.1 Encryption Cryptography:

Due to the high level of privacy required for electronic health records, encryption is a significant part of MedicalChain's infrastructure. Symmetric key encryption is used on medical records. Symmetric key encryption is a type of encryption where only one key is used to both encrypt and decrypt electronic information. The symmetric key encryption ensures that a stakeholder who does not possess the key cannot understand/decrypt the encrypted data. Thus only stakeholders for whom the data is meant will be able to decrypt the data.

In MedicalChain, the symmetric key is encrypted with the public key of a 2048-bit RSA key pair. When a patient grants a stakeholder (e.g., doctor, pharmacist) access to his records, the following steps take place:

1. MedicalChain decrypts the record with the patient's private key

2. Then, the symmetric key is encoded with the public key of the stakeholder that was given access [26]

When a stakeholder (e.g., doctor, pharmacist) who has been given access to a patients record requests the patient's record, the following steps take place:

1. The symmetric key for the electronic health record (EHR) is decrypted by the private key of the requesting stakeholder (eg doctor)

2. The decrypted symmetric key is then used to decrypt the patient's electronic health record [26]

Figure 7 shows a more detailed view of the encryption cryptography flow of medicalchain.

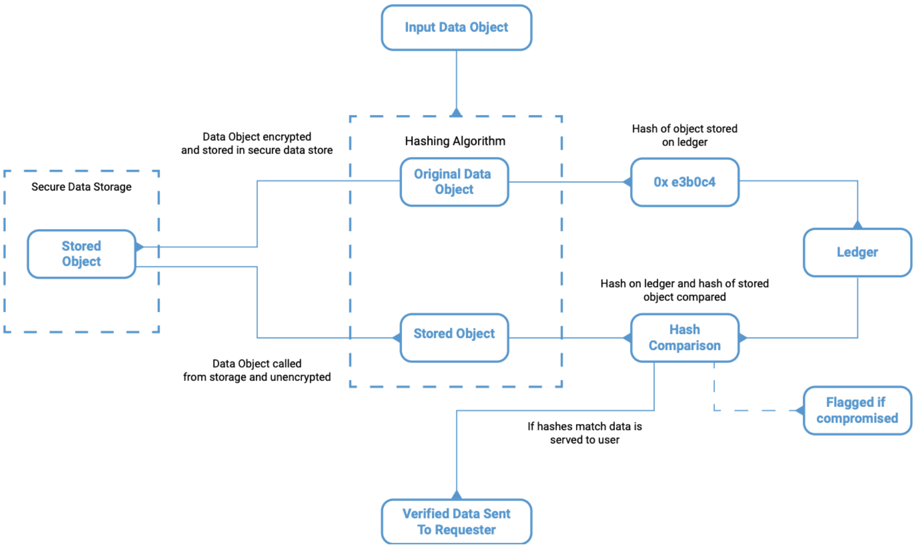

Input Data Object
Data Object encrypted and stored in secure data store
Hashing Algorithm
Hash of object stored on ledger
Secure Data Storage
Original Data Object
0x e3b0c4
Stored Object
Ledger
Hash on ledger and hash of stored object compared
Stored Object
Hash Comparison
Data Object called from storage and unencrypted
Flagged if compromised
If hashes match data is served to user
Verified Data Sent To Requester

Fig. 7. Encryption Cryptography flow of MedicalChain [26]

As we have stated earlier on, in the MedicalChain world , the patient is able to restrict/revoke a stakeholder (eg doctor's) access to his data. Whenever a patient requests that another participant's access to his electronic health record be revoked, the following takes place:
"1. The symmetric key is decrypted with the private key of the patient who owns the EHR
2. The EHR is then decrypted with the symmetric key
3. The EHR is reencrypted with a new symmetric key
4. The new symmetric key is then encrypted with all the other stakeholders (e.g doctors) that who's access have not been revoked by the patient." [26]
It is easy to see that with this mechanism , the stakeholder whose access was revoked will no longer be able to access that patient's EHR.

5.3.2 Transactions:

In this subsection, we take a detailed look at how transactions are defined within the MedicalChain EHR system. Interactions with medical records on blockchains are recorded as transactions. Using blockchain technology for electronic health record management ensures that once there is an update/change on a patient's health data, it cant be maliciously altered in the future.
We now take a detailed look at the most common transactions on a MedicalChain network - a patient granting a stakeholder (e.g doctor) access to his EHR, and a patient revoking his doctor's access to his EHR. To describe this flow, let's assume we have a patient called Adam, and a doctor called Paul.
Flow 1 : Patient Adam Granting Access to Doctor Paul: When Patient Adam grants access to his EHR to Doctor Paul, Adam's ID gets appended to Paul's authorized asset on the ledger.Paul's ID also gets appended to Adam's authorized asset on the ledger. The next step is that the symmetric key for patient Adam's electronic health record is then decrypted with patient Adam's private key. Afterwards, the symmetric key is encrypted with doctor Paul's public key. [26]

Flow 2 : Patient Adam Revoking doctor Paul's access to his EHR : When patient Adam revokes doctor Paul's access to his EHR, Adam's ID is deleted from Paul's authorized asset on the ledger, and so is Paul's ID deleted from Adam's authorized asset on the ledger. Patient Adam's EHR is then decrypted with his private key, and simultaneously encrypted with a new symmetric key. This new symmetric key for patient Adam's EHR is then encrypted with Adam's public key,and the public keys of everyone Adam has given access to read his records (except Paul). [26]

5.3.3 Data structures :

In this section we seek to explain the internal data structures that makes MedicalChain work. Hyperledger's modeling language is used to define the domain model for the network. We detail how within the .CTO file , models are defined and stored

Participants:
In the medicalchain ecosystem, there are two main types of participants- the patients and the practitioners. Below, we show how these participants are defined internally. Their model definitions rely other data structures such as medicalrecords (also defined below)

Participant Type 1 : Patient [26]

Variable Type	Variable	Description
String	ID	unique identifier
Asset	PersonalDetails	Structure defined in asset
String(Array)	authorised	participant ID's allowed to read EHR
Asset	MedicalRecord	Structure defined in asset

Variable Type	Variable	Description
String	ID	unique identifier
Asset	PublicProfile	Structure defined in asset
String(Array)	authorised	array of patient ID's he's allowed to read
Asset	MedicalRecord	Structure defined in asset

Participant Type 2 : Practitioner [26]

Assets:

Below we describe the model definitions of three assets of medicalchain - the personal details asset , the practitioner's public profile asset , and medical record asset. The personal details asset is used to describe patients and practitioner's public profile asset is used to define practitioners such as doctors.

The medical record asset defines a medical record, and links the patient to a list of practitioners who have access to read the EHR records of that patient. The ID's of all such authorized practitioners for the patient are stored in the permissions array within the medical record data structure.

Asset type 1 : Personal details [26]
Relationship: Patient(Participant)

Variable Type	Variable	Description
String	ID	unique ID for asset
String	FirstName	Patient's given name
String	LastName	Patient's last name
String	EmailAddress	Patient's email
Int	Dob	Unix timestamp of DOB
concept	Address	Address of participant
Super-Type	Owner	Extends Patient (Participant) asset

Asset type 2 : Practitioner's public profile [26]
Relationship: Practitioner(Participant)

Variable Type	Variable	Description
String	ID	unique ID for asset
String	FirstName	first name of user
String	LastName	User's last name
String	EmailAddress	User's email
Int	Dob	Unix Timestamp of DOB
concept	Address	See concepts section
String	Identification ID	unique ID of practitioner
Array	Qualification	Degrees of Practitioner
String	Image URL	pointer to practitioner's image
Super-Type	Owner	Extends practitioner

Asset Type 3 : Medical Record [26]

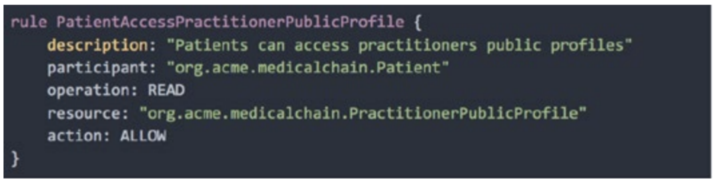
Variable Type	Variable	Description
String	ID	unique string
Super-Type	Owner	Extends Patient asset
Super-Type	Author	Extends practitioner asset
Array	Permissions	Array of participant ID's
String	File Hash	SHA-256 hash of latest file
Float	Version	file version
String	Pointer	points to external storage of record

5.3.4 Permission definitions :

Remember that a major part of the MedicalChain EHR system is that a user is given the ability to chose which part of his record a practitioner sees. In this sub-section, we will give some examples of how these rules are defined.

MedicalChain is powered by Hyperledger Fabric, which includes an access control language (ACL) which defines access over the elements of the .CTO domain model defined in the previous section. It is these ACL rules that enable participants to be controlled as to what they see on a patients data. The first ACL rule we will look at (Fig 8) is one which allows patients to read the public profiles of practitioners.

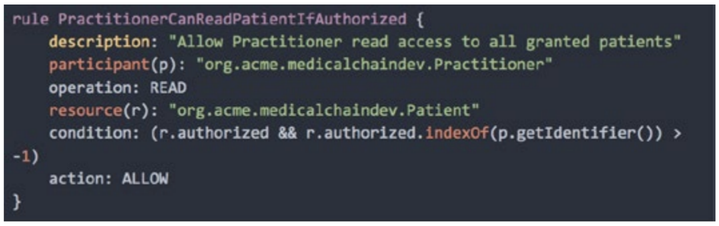
In the ACL rule defined below, the READ operation is ALLOWED for any patient on the practitionerPublicProfile resource.



```
rule PatientAccessPractitionerPublicProfile {
    description: "Patients can access practitioners public profiles"
    participant: "org.acme.medicalchain.Patient"
    operation: READ
    resource: "org.acme.medicalchain.PractitionerPublicProfile"
    action: ALLOW
}
```

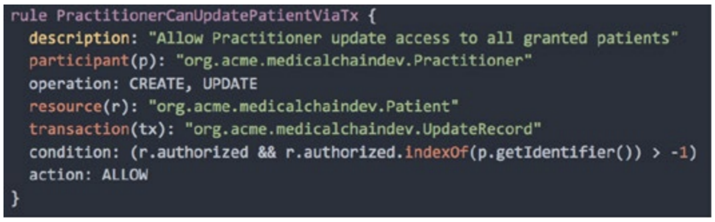
Fig. 8. Patient accessing practitioner's public profile ACL rule [26]

Access control language also allows conditional clauses. For instance, it is necessary to ensure that the only practitioners who can read a patient's electronic health record are those to whom that patient has granted permission. To do this, we regulate the READ access with a conditional clause. In Fig 9, only practitioner IDs in r.authorized (where r stands for the patient) are ALLOWED read access.



```
rule PractitionerCanReadPatientIfAuthorized {
    description: "Allow Practitioner read access to all granted patients"
    participant(p): "org.acme.medicalchaindev.Practitioner"
    operation: READ
    resource(r): "org.acme.medicalchaindev.Patient"
    condition: (r.authorized && r.authorized.indexOf(p.getIdentifier()) >
-1)
    action: ALLOW
}
```

Fig. 9. Practitioner can read patient if authorized ACL rule [26]



```
rule PractitionerCanUpdatePatientViaTx {
  description: "Allow Practitioner update access to all granted patients"
  participant(p): "org.acme.medicalchaindev.Practitioner"
  operation: CREATE, UPDATE
  resource(r): "org.acme.medicalchaindev.Patient"
  transaction(tx): "org.acme.medicalchaindev.UpdateRecord"
  condition: (r.authorized && r.authorized.indexOf(p.getIdentifier()) > -1)
  action: ALLOW
}
```

Fig. 10. Practitioner can update patient ACL rule [26]

The access control language used in medicalchain also allows other operations such as creating and updating records. Fig 10 shows the ACL rule that empowers practitioners (e.g doctors who have been granted access to a patient's record) to create and update those records. For a given participant/doctor p, and a given patient r, The condition (r.authorized && r.authorized.indexOf(p.getIdentifier()) >-1) is true if that patient r has given access of his EHR to doctor p . If that condition is true/satisfied, the doctor is ALLOWED to CREATE or UPDATE patient r's records.(See fig 10)

6 Application 3 - Online Voting System

An electronic voting system, currently utilized by some of the developed countries around the world, is a system which digitalize the process of an election, affording both efficiency and convenience. Although it offers several benefits, there exists some problems as well. For instance, some of its weakness are the security vulnerabilities which are closely related to the manipulation of voting results and skepticism by voters.

Some of these issues can be resolved by integrating blockchain with the electronic voting system. A blockchain enabled voting system is able to guarantee the reliability of the voting system, and reduce inefficiency. "Solidity" is one of such Smart Contract Trusting language used to make the voting system possible.

To establish a fair voting system, it is necessary to define several conditions, and tackle some of the issues relating to a blockchain integrated voting system. In this section, we will highlight a number of solutions which satisfy the conditions, as well as address the issues in question.

6.1 Current Electronic Voting System

[27] To consider a blockchain voting system, it is necessary to know why it is something that is needed as well as how this can complement current solutions. At present, electronic voting systems are utilized. Prior to considering the blockchain voting system, it is necessary to take a look at current solutions for electronic voting.

First of all, there is a method referred to as REV. REV is an abbreviation of Remote internet E-Voting. By utilizing REV, users are able to connect to the internet regardless of whatever device they are using, including PCs and mobile devices. Websites and SMS voting are considered to be under the umbrella of REV. REV is also able to be utilized for smaller forms of voting, such as voting among shareholders. However, REV also has its limit. This is due to that within this electronic voting system, it would be possible to display the votes to others. Also, it would be possible that someone affects others' votes. That is, this could destroy the secret vote. In other words, fairness is not maintainable.

Secondly, there is another system called PSEV. This is an abbreviation of Poll Site E-Voting. This system is similar to our current paper-based system. Much like the current voting system, if we use this solution, voters would need to go to a polling place and vote not on paper, but using an electronic device on location. To avoid the issue of Hijacking and Hacking, the device is disconnected from the network. When voting is completed, the date in the machine is sent directly to the counting device or place. By using PSEV, the counting can be accelerated as compared to the current paper-based voting system. However, this alone cannot solve the issue of fairness. Voters are unable to be sure that their votes would be delivered correctly. To address this issue, PSEV uses paper receipts. When a voter enters an input into the machine, the machine prints out a receipt.

Considering these two varying voting systems, an electronic-based system would be more efficient. However, there still are major disadvantages, such as questions of security or fairness, and elections such as a presidential election cannot utilize an entirely electronic voting system.

6.2 Blockchain : Change the online voting system

If something is written on the blockchain, it is almost impossible to change the input value and it is far easier to validate the data. Owing to this characteristic of the blockchain, there exists diverse trials for utilizing the blockchain as the underpinning of a voting system. Mostly, in this paragraph the usage of the blockchain as a voting system through smart contracts shall be explained. Voting factors.

Commonly, within the blockchain voting system, there must be election administrators, voters, regional nodes and boot nodes. The Election administrators should create the type of vote to be run, and define it at first. Moreover, the factors on the ballot shall be decentralized and voter registration is the role of the administrators. At this point, the voter can prove their profile and proceed with voting and eventually verifying his or her vote.

The District Node will have access to the polling places in the defined region. Only a vote that has been verified by multiple local nodes and is agreed upon by said nodes will actually be placed on the blockchain. Each local node can host a boot node. Boot nodes serve the role of helping local nodes find and communicate with each other, and they do not store blockchain transactions separately.

6.3 Online Voting System : Election Process

Elections using a typical blockchain voting system are carried out across five stages: Voter registration, Election creation, Vote transaction, Telling results, and Vote verification

6.4 Online Voting System: Voter Registration

Public and private keys are created only for voters whose identities have been verified. First of all, it is assumed that government-level identification services are involved for confirming identification and verification. Tokens are given to each verified key pair, which is purposed to prevent duplicate voting.

Table 1. Figure of an example of voting transaction

Transaction ID	Block	To	Value
0xblockchainvoting	1345	Smart Contract	No.1

For example, suppose Hong Gil-dong, who has been certified, receives a token. If Hong Gil-dong votes for a particular candidate, a token unit is sent to the candidate of their choice. Their profile dispersing the vote token is registered on the blockchain, thus preventing duplicate voting.

The list of eligible voters is a non-changeable, decisive list during the election period and is used in the election-creation process, as below. Wallets are created to hold public and private keys only for proven voters, and methods such as NIZKP (Non-dialogue Young Knowledge Proof) can be employed to prevent the system from knowing if a particular Wallet belongs to a particular voter.

6.5 Online Voting System : Election Creation

First, voting managers execute election creation contracts. An election-generated contract provides a list of candidates and voting areas. Specific to the list of voting regions specified in the election-generating contract, a ballot is generated and distributed across the blockchain by region. Here, the term ”voting ballot” refers to implementation as a smart contract, not a physical paper ballot. For ballot contracts, the Voting District has parameters and lists of candidates belonging to the voting area specified. At the beginning of the election, each local node will have authority over the ballot region specified by the corresponding voting area parameter.

6.6 Online Voting System : Vote transaction

Voting under a blockchain system refers to calling a ballot contract with parameters of one’s voting area. As mentioned earlier, if a voter votes, a token will be dispersed from their wallet, and the voting ballot contract will access the blockchain through the local node in the area to which the voter belongs. Once the majority of local nodes reach an agreement on the voter’s vote, the vote will be recorded on the blockchain.

Voting is stored on the blockchain in the form of a transaction, and voters can verify their vote using the transaction ID. The portion of the vote verification is specifically described in the voting verification section.

6.7 Online Voting System : Verifying Votes

For voters who have cast their votes, the transaction ID may be used to verify their vote. After the voter goes to a government office in their area and proves their identity, they can then present a transaction ID. The person in charge then finds the block containing the transaction ID after activating the local node, and the verification is completed by checking the voting value entered within the block. The Blockchain-based voting system offers the advantage of blocking the possibility of forgery, and if the above process is implemented, many of the necessary conditions for fair elections can be satisfied. But for two reasons that follow, this is also hardly a fool-proof voting system.

1. **Full verifiability is unachievable.** A voter may individually verify that their votes are properly recorded, but not directly for the full count results. This is because voting data for secret voting is managed only by the governing body.

2. **Complete anonymity is not achievable.** The governing body may match the identity of the voters with the value of the vote. No matter how trusted a management institution is, the fact that it has data that tells an official who a given ID selected is not easy to resist.

At first glance, it seems impossible to achieve both full verifiability and full anonymity at the same time. This is due to that it would mean that everyone can see the total ballot count data and never know the voting price of anyone but them-self. However, this article attempts to propose a mechanism for achieving full verifiability and full anonymity. In other words, under the voting system proposed in this article, anyone can access the ballot counting database and verify their own vote and the total ballot count. No one but an individual voter them-self can know his or her voting value and prove it to others. Based on the election components described above and the election process, this voting system intends to randomly print public keys upon the voting receipts.

Voting transactions will include transaction IDs, blocks containing transactions, voting ballot contracts that send transactions per head, and voting totals. The above table displays the transactions of voters who voted for No. 1 in Gwanak-gu. It is important to note that this transaction contains only the location and the value of the vote, but does not contain any information regarding the voter.

6.8 Online Voting System : Process

Voting proceeds through three main stages: identification, voting, and receipt issuance. And there is a pre and post stage to allocate key and tabulate the results.

1. **Allocate Key Pairs**
   Issue public-to-private key pairs by the number of eligible voters. Each public key account will be provided a single vote token (one for each vote).
2. **Identification card**
   Voter visits polling stations designated by the governing body and certifies his identity with the voting manager. If the voter’s identity is confirmed, the manager will randomly extract a pair of private keys from the Blockchain DB holding the voting token, and provide them to the voters. At this time, random sampling is performed off-chain.
3. **Voting**
   Voter sends the token of the public key address he has just received through the voting device to the region of the desired choice. The process of entering public and private keys into voting devices is based on the premise

that QR codes are used quickly and efficiently.

4. **Issuing receipts**
   The voting device randomly extracts and prints one public key that registers a vote for each candidate from among the public keys on which the vote was recorded. However, this must include the public key address that the voter has just used to vote. For example, let's say there are three candidates. The ballot receipt shows the public key used by the person who voted for Candidate No. 1, the public key used by the person who voted for Candidate No. 2, and the public key used by the person who voted for Candidate No. 3. Further, one of these is the public key that the voter who just voted received randomly following his identity card. These devices are intended to prevent vote-buying, which is able to achieve both full verification and full anonymity. At the beginning of the election, there may be candidates who have not yet received votes due to that there are not enough voters. In view of this, the system presupposes that candidates vote for themselves. That is, for those who voted for the first time since the election began, the public key that they used to vote and the public key that each of the remaining candidates used to vote will be printed on the receipt.
5. **Counting stage**
   Counting is performed by checking the number of tokens collected in each option contract following the closing of the polls. During the counting stage, anyone can check the data recorded on the blockchain. Thus, each 'voter' can find the public key he or she used to vote on the receipt in the blockchain and verify that the vote was recorded correctly (individual verifiability) and that anyone can verify that the vote count was correctly recorded based on the entire set of data (total verifiability).

The above process is described in detail, using the following example:

1. Let's assume an election in which candidate number one and number two are running opposed to each other. Below are some of the data recorded on the current blockchain where voter Choi visited the polling station. 'Voting status' is the candidate number from each public key that sent the token, and the public key that has not yet voted is marked as 'zero'. Refer to Table 2.

2. When Mr. Park certified his identity at the polling station, the manager provided him with the public key IJKL and the corresponding private key through random sampling among the public keys with no vote registered to them. At this time, the custodian does not know what key pair he has provided to the voter. Park sends a token to candidate No. 1 with the secret key IJKL, which was then recorded on the blockchain by voting devices. After Park's vote, the voting status is altered as in Table 3

3. The voting device will print out the following receipt. IJKL, the public key that Park used to vote for his candidate, and QRST, one of the public keys that Park used to vote for two candidates, will be printed out. Refer to Table 4.

Table 2. status of the keys

Key	status of vote
ABCD	0
EFGH	1
IJKL	0
MNOP	0
QRST	2

Table 3. status of the keys

Key	status of vote
ABCD	0
EFGH	1
IJKL	1
MNOP	0
QRST	2

Table 4. status of the keys

Key	status of vote
IJKL	1
QRST	2

4. The polls close and all public key voting values recorded in the Blockchain are disclosed as in Table 5.

5. Mr. Park can confirm that his vote was correctly recorded by checking the voting value corresponding to the IJKL identifier written on the receipt. However, others who saw Park's receipt only know that there is a public key that Mr.Park used to vote, but they do not know which candidate he selected. In this way, there is a limit to having to trust the polling manager for safe storage of public keys — pairs of private keys. However, since all voters can transparently verify their own votes being correctly recorded through data released on the blockchain, no vote manager who keeps private and public keys will risk punishment and falsifying the voting prices.

6.9 Real Case : Follow my Vote

[28] In reality, there are real applications for online voting systems using blockchain technology. The company managing it is called Follow-My-Vote. According to Follow My Vote's website, this service brings the entire pro-

Table 5. status of the keys

Key	status of vote
ABCD	2
EFGH	1
IJKL	1
MNOP	1
QRST	2

cess of current paper-based voting systems online by utilizing the blockchain. One difference with the current system is flexibility. To be more concrete, voters are able to change the votes before the end of election day if they change their minds.

6.10 Real Case: TTP using a blockchain voting system

[29] In accordance with Kibin Lee, a professor at Korea University, research into a blockchain voting system by utilizing a multi-chain solution points to a system using TTP. Professor Lee argues that TTP authorizes voters to vote by choosing who they want to vote for. Each vote is equivalent to the asset in the multi-chain and the transaction. Here, it is necessary for the system to restrict the multi-chain asset in order to process the maximum of one transaction between multiple parties. The system may be capable of restricting either multi-votes that go directly to the same candidate or voting for multiple contenders.

6.11 Online Voting System : Conclusion

We have highlighted the components and processes inherent to the blockchain voting system that could serve to resolve the trade-off issue of the PSEV method of verification and anonymity among the existing electronic voting systems, all while devising a voting system that cannot be falsified. To be verifiable and achieve full anonymity, we mentioned that a device could be used, which would randomly shuffle the remaining open keys.

Among the security technologies that have emerged thus far, blockchain is considered as one of the only technology that could guarantee verifiability, transparency, and security of the vote all simultaneously. Even though substantial measures have already been derived to make this process plausible, further research will be necessary to ensure that a blockchain-based voting system is complete enough to replace the existing electoral systems, in a more widespread basis.

7 Challenges in Blockchain Adoption

Although the technology has been around for close to a decade, the practice of applying blockchain to solve business problem is still fairly new and many industries are still at its infancy when it comes to adoption. [30]

There are several notable reasons why adoption of blockchain in the industry is still few and far between. For example in the case of supply chain tracing using blockchain, one key impediment is the lack of IT infrastructure and Internet speed in the entire supply chain for the solution to work properly. This means that every stakeholders in the chain, from the supplier of ingredients, producers of the goods, logistics partner, warehouse operator, wholesaler and retailer must have sufficiently good IT infrastructure, for the whole supply chain be accurately monitored. This in turns, mean that organizations have to put in sizeable resources to develop the infrastructure needed to facilitate this application [30]. This especially difficult for facilities in remote locations or suppliers located in low-income regions.

In the financial sector, industry players does have some skepticism relating to the technological side of blockchain, concerns about ability to scale, security, privacy leakage, and energy consumption are some of the issues raised. Although most of these technical concerns already have corresponding solutions, the industry will need time to acknowledge that and to accept them. [31] Besides the technical issues raised, the biggest hurdle to financial industry's adoption of blockchain is arguably on the regulatory front, in many countries the regulator are concerned about blockchain enabling frauds and other illegal activities that hurt the interests of consumers and the market. This resulted in some regulators not approving the use blockchain in the financial sector, fearing that taxation and trading rules could be circumvented with this technology. [31]

Furthermore, for consortium based blockchains, building the platform requires cooperation between multiple institutions and stakeholders, hence proper governance model is required. In turn, this challenge poses a need to transform the organization in order to reach benefits from the distributed nature and the need for making design choices for applications based on blockchain technology. All of these things add another layer of complexity to the already complicated and bureaucratic nature of many companies. [32]. These organizational transformation often leads to unfavorable reactions within the organization and as such become another challenge in adopting the new technology, which might further exacerbate the poor acceptability of the technology, as the technology is relatively new and its reliability has not convincingly been proven yet. Furthermore, some stakeholders in the organization might view this technical as a threat to their job security. [32]

Apart from the above, detractors of blockchain technology also frequently bring up the issue of potential abuse of power. Although blockchain is supposed to democratize assets ownership, providing a decentralized and more libertarian system, critics who oppose the technology argues that it will bringforth greater imbalance of power between developers and ordinary users [33]. An "invisible power structure" might appear as a result, where blockchain coders enjoy an advantage over users, effectually acting as sovereign authority of their platforms. For example in a world where physical digital assets are all managed through blockchain, power users can obfuscate their transactions better through clever coding, make use of smart contract in intricate ways. This could potentially result in greater disparity, where from an end-user perspective, this could look more like a burden than an advantage. This notion has plagued some potential industry adopters.

As with any revolutionary technology, there is bound to be challenges, from a technical standpoint, operational standpoint, and also mindset standpoint. Therefore, it is imperative for advocate of the blockchain technology to bring together the right people, to establish roadmap, key milestones and framework to bring this technology forward, and make it more accessible and acceptable by a broader audience. In our next section, we will cover some of these advances.

8 Future Trends and Advancements

Regulatory sandboxes will most likely be a normal trend in the blockchain world, in the near future. In the financial industry space, "crypto regulatory sandbox is a metaphor to describe a space where financial technology companies are exempt from some kinds of regulation so that they can innovate new products without fear of breaking the law." [34] Back in July 2020, the Financial Conduct Authority (FCA), the regulator of the financial services industry in the United Kingdom, granted access to 22 companies to its sandbox service. [35] We foresee such legal sandboxes which give the ability of blockchain projects to be tested, with some exemptions from some kinds of regulations, will spring up in many parts of the world in the immediate to near future.

Another prediction for massive future use of blockchain technology is in cybersecurity. Blockchains are a distributed ledger, able to maintain the identical copies of the same ledger across different nodes on the network. This feature and many others give blockchains a high level of security. In the near future, with the increasing trends of hacking , we predict with the move away from centralized vulnerable systems, blockchain technologies will be central in helping to prevent such attacks.

Another area where blockchain technology may pick up dramatically in the future is, in maintaining records of real world assets (moving beyond digital asset record), to hard assets such as land ownership. In many developing countries, land ownership is subject to a myriad of disputes. "Land ownership is primarily established through a registered sale deed. This document is not a government guaranteed title to the property, but only a record of the transfer of property – and hence subject to challenge. " [36]. Thus it is very common to find that in many of these countries, the government body in charge of land sales usually have to manually search through many years of land records and documents to find who owns a piece of land, and trace all transactions on those lands. This obviously is a tiring and very inefficient situation . In addition, there is a lot of litigation on land due to the inefficient systems for maintaining land ownership rights. It is interesting to note that blockchain technology lends itself perfectly to creating and maintaining immutable records of land ownerships and transfers over several years. All transactions happening across the blochcain of digitized land assets will be visible and immutable, and visible to all stakeholders , including land insurers. We believe using blockchains to maintain records of land ownership is a very plausible large scale use of blockchain technology in the future, especially for developing countries who have many issues of fraud with respect to the land ownership industry.

Another possible future trend of blockchain is in the issuance of certificates, where in India, the Government is considering using blockchain to combat fraudulent education credentials. "A paper-based certification is fallible to manipulation and susceptible to fraud. According to a report by First Advantage, a background screening company, there are more than 7,500 organisations that provide fake employment and educational certificates. There are usually two problems at play: degrees from fake universities and fake degrees from real universities." [36] This means that several companies that decide to employ graduates will have to make a lot of monetary investments in investigating the credentials and certificates of prospective employees. Many institutions have now adopted digital certificates with digital signatures , however those also lend themselves easily to fraud and malicious attacks "– as seen in the 2018 case of CEO of CA Trustico mailing the private keys of 23,000 certificates, forcing the Root CA to invalidate the certificates" [36]. The major root causes of fraud with educational certificates is that it is centralized, meaning there is a huge dependence on some central certificate dispatcher. Thus a solution to educational certificate fraud is a permission based blockchain , which is a decentralized system, which guarantees the immutability of certificates once issued. We project that these permission based blockchains will be very common in future, amongst issuers of digital certificates, in order to reduce the fraud in the system. Furthermore, with the recent COVID-19 pandemic, there are conversation about the creation of a vaccination passport to proof immunity for travel purposes, and agencies are considering the usage of blockchain to enhance the transparency and authenticity of such passport. [37]

We see these push by governments in wanting to solve unique problems using blockchain, as a strong signal of validation and support. Apart from India and the UK making such advances, many Governments around the world, such as Singapore [38], Canada [39], Australia [40] and Japan [41] have realized the value of blockchain, and created roadmaps, sandboxes and frameworks which will help to accelerate the growth of the blockchain ecosystem in their respective country. With these initiatives and the highest level of support in placed, with more to come in the near future, is it clear that the adoption of blockchain in the industry will grow in the years to come, despite the challenges.

9 Conclusion

We have no doubt that crypto currencies will remain at the forefront of conversations regarding blockchains in the near-term. The immediate value that is brought to market participants, coupled with the enclosed ecosystem that a currency market create incentives to keep participants engaged around crypto currencies.

That said, we have looked across a multitudes of different industries to understand how blockchains are being leveraged to either makes increment improvements in underlying industries or position new players to attempt to make revolutionary advancements. It is apparent more then ever that blockchain technology is not necessarily a solution in search of a problem, but the tenants of blockchain that Satoshi Nakamoto first brought to the world's attention are truly attractive enough to warrant investigation in a multitude of different formats.

Specifically, the transparency that can be provided through a blockchain solution is key to its attractiveness. Whether in a permissioned or public setting (or hybrid of the two), giving participants a view into what is happening in the underlying transaction is an attractive proposition. Too often intermediaries that have taken on this role themselves, where financial institutions, medical record providers or voting system, add a layer of opaqueness which ultimately hampers the the total trust into the network. This transparency also bring forth greater efficiencies as the verified data are appropriately and seamlessly shared among the participants.

What is holding back the wider spread of blockchain adoption, can largely be attributed not to the technology itself, but practical issues in getting large, complex and well embedded industries to make wholesale changes in how they under go business. The larger the addressable market, the more minds you need to change to make an effective change. Furthermore, the legal frameworks that currently exist for many of these industries, which can be highly regulated, can be slow to adapt. Few regulations or laws have adequately considered and assessed the implications of moving into distributed systems. It will take a considerable lead time to build not only the correct frameworks, but for precedent's to be established and best practices found, tested and adopted.

Nevertheless, it is exciting to anticipate the paradigm shift that could happen by these promising blockchain solutions. What remains to be seen, is which industries will ultimately reap the largest benefit, evolving from the traditional silo ways of doing things to a much more open and transparent way of operating, fostering collaboration and paving the way for a truly connected ecosystem.

References

[1] Marr, B., 2018. A very brief history of blockchain technology everyone should read, Mar.

[2] Arnold, M., 2017. Five ways banks are using blockchain, Oct.

[3] Kaminska, I., 2015. Blockchain promises back-office ledger revolution, Oct.

[4] Shumsky, P., 2020. How to enhance kyc systems with blockchain, Jun.

[5] Corkery, M., and Popper, N., 2018. From farm to blockchain: Walmart tracks its lettuce, Sep.

[6] McCauley, A., 2020. Why big pharma is betting on blockchain, Aug.

[7] Treshock, M., 2020. How the fda is piloting blockchain for the pharmaceutical supply chain, May.

[8] Madeira, A., 2020. Blockchain to disrupt music industry and make it change tune, Jun.

[9] n.d., 2020. How blockchain could redefine the gaming industry, Sep.

[10] Sharma, T. K., 2019. Public vs. private blockchain : A comprehensive comparison, Aug.

[11] Denys, 2019. How the consortium blockchain works, Sep.

[12] Dib, O., Brousmiche, K.-L., Durand, A., Thea, E., and Hamida, E., 2018. "Consortium blockchains: Overview, applications and challenges".

[13] Hammerschmidt, C., 2017. Consensus in blockchain systems. in short., Sep.

[14] Gross, J., 2020. Which blockchain to choose in a consortium?, Feb.

[15] Bitcoin development.

[16] Galea, A., 2018. Bitcoin development: who can change the core protocol?, Sep.

[17] Brown, R., 2019. "A simple explanation of how shares move around the securities settlement system".

[18] Securities, and Commission, E., 2020. "Alternative trading system ("ats") list".

[19] Schaffler, R. "Overstock's ceo wants crypto technology to clean up wall street".

[20] Metz, C., 2015. "Overstock will issue a private bond powered by bitcoin tech". *Wired.com*, Jun.

[21] Cordell, D., 2015. "Overstock.com to offer world's first cryptosecurity on bitcoin blockchain".

[22] Byrne, P., 2015. "Amendment no. 1 to registration statement on form s-3/a".

[23] Mizrach1, B. "Analysis of corporate bond liquidity".

[24] T0.COM, I., 2018. "Confidential private placement offering memorandum".

[25] Fries, T., 2020. "tzero security tokens officially begin live trading".

[26] Medicalchain, 2018. Medicalchain whitepaper 2.1.

[27] DongHeon, L., 2019. Proposal of a blockchain-based electronic voting system for fair elections, Apr.

[28] follow my vote information.

[29] Kibin, L., 2018. Electronic voting system using blockchain.

[30] Queiroz, M. M., and Fosso Wamba, S., 2019. "Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in india and the usa". *International Journal of Information Management,* **46**, pp. 70 – 82.

[31] Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., and Arami, M., 2020. "How blockchain can impact financial services – the overview, challenges and recommendations from expert interviewees". *Technological Forecasting and Social Change,* **158**, p. 120166.

[32] Batubara, F. R., Ubacht, J., and Janssen, M., 2018. "Challenges of blockchain technology adoption for e-government: A systematic literature review". dg.o '18, Association for Computing Machinery.

[33] Kosmarski, A., 2020. "Blockchain adoption in

academia: Promises and challenges". *Journal of Open Innovation: Technology, Market, and Complexity,* **6**(4), Oct, p. 117.

[34] Frankenfield, J., 2020. Crypto regulatory sandbox, Dec.

[35] Authority, F. C., 2020. Regulatory sandbox - cohort 6, Dec.

[36] Roy, A., Kumar, A., and Mahindru, T., 2020. Blockchain: The india strategy towards enabling ease of business, ease of living, and ease of governance, Jan.

[37] Ummelas, O., 2020. Blockchain app may solve virus passport puzzle.

[38] IMDA Singapore, 2020. Blockchain innovation.

[39] Government of Canada's Sectoral Initiatives program, 2020. Building canadian consensus: Our maturing blockchain ecosystem, Mar.

[40] Australia Government, 2020. The national blockchain roadmap: Progressing towards a blockchain-empowered future, Feb.

[41] Japan Government, 2020. How the japanese government's new "sandbox" program is testing innovations in mobility and technology - sponsor content from the government of japan, Feb.