

Fall 2018

Building Blocks of Commercial Crypto-Technologies Solutions

William Kincaid
Iowa State University

Follow this and additional works at: <https://lib.dr.iastate.edu/creativecomponents>



Part of the [Computer and Systems Architecture Commons](#)

Recommended Citation

Kincaid, William, "Building Blocks of Commercial Crypto-Technologies Solutions" (2018). *Creative Components*. 73.

<https://lib.dr.iastate.edu/creativecomponents/73>

This Creative Component is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Creative Components by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.

Building Blocks of Commercial Crypto-Technologies Solutions

CPRE/INFAS 599, Summer 2018

July 8, 2018 – William C Kincaid

Blockchain Technology has been a darling on Wall Street for a few years now. Bitcoin, a blockchain based crypto-currency has shot up in value from under \$600 in October 2014 to over \$19,000 December 2018 and then falling to nearly half that at under \$10,000 May of 2018 (Ref#1). Along the way, several other crypto-currencies have joined the fray with 30 entities reported as having a market capitalization of over one billion dollars (Ref#2). Where is blockchain going? Some have estimated the Global Blockchain Technology market is anticipated to exceed 60.7 billion dollars in 2024 (Ref#3).

With all the excitement and seeming hyper ventilation over blockchain it is important we understand blockchain capabilities and pitfalls.

This document will explore the technology behind blockchain, describe practical commercial applications of blockchain, suggest legal and effective uses for crypto-technologies and define a set of criteria that should be built in to commercial crypto-technology solutions.

What is Blockchain?

The phrase “Blockchain Technology” generally refers to a distributed software solution that is used to build and maintain an immutable ledger that contains a full history of transaction data that can be validated and/or authenticated.

No one really knows who or whom created blockchain technology. There is evidence to suggest attribution to a person or character named Satoshi Nakamoto, but no one really knows if Nakamoto is a man or woman, a single person or group of people or necessarily where Nakamoto resides. The software Nakamoto created was unique in that rather than using a centralized host for managing data a decentralized design was implemented. The original focus for the solution was crypto-currency and specifically what is now known as Bitcoin, however the software can be modified to deliver new and exciting functionality, presuming one knows what they are doing.

In electronic payments, we had seen this decentralized design before with smartcard technology. Today, the major Card Brands have settled on a “Host is Master” concept where POS transactions performed remotely are validated, finalized and settled (paid) from hosts rather than transferring value from the Card to the POS Terminal as is the case with the “Card is Master” concept. While the “Card is Master” design utilizes a central host for reporting, the actual transfer of value was done at the precise time a successful transaction occurred at a merchants POS.

Building Blocks of Commercial Crypto-Technologies Solutions

An example of a Card is Master solution first appeared for the major card brands (VISA, MasterCard, American Express and Discover) during the 1996 Summer Olympics in Atlanta. All Smartcard based transactions performed authenticated the card and card holder with the merchant acquirer who provided the POS Terminal funding merchant accounts based on transactions reported from the POS Terminal. Needless to say, there were several lessons learned during the Summer Olympics in Atlanta many of which we see resolved in some manner today using crypto currencies, with one major exception. During the Olympics it was observed that using a distributed smart card model if a card holder loses their card, or if the merchant terminal breaks or is stolen, the cardholder and merchant stand to lose their money. Similarly, today with crypto-currencies, when one loses their private key the crypto-currency could become inaccessible forever. This potential loss of access to crypto-currency accounts has spawned several crypto-currency wallet companies that manage private keys and credentials on behalf of the crypto-currency account holders to reduce the risk of loss due to a lost private key.

The concept behind the distributed aspect of blockchain software is a sort of “crowd validation” idea where each node running the software validates and re-validates the blockchain and associated data on a constant basis, thereby providing notice if data integrity is lost. This process is called “Consensus”, where each node validates the same data before it is accepted as a transaction and added to the ledger.

Consensus, if properly implemented and securely managed, leads to other reported key benefits such as Provenance, Immutability, and Finality. Provenance refers to participants knowing where an asset came from. Immutability suggests that no participant can tamper with a transaction after it’s been recorded, which culminates in Finality where the shared ledger provides a way to validate the completion of a transaction. (Ref#4)

In practice, blockchain solutions apply cryptographic methods to encrypt data and create a hash of each transaction stored in the ledger which is then added to the base transaction with each subsequent transaction storing a hash of the prior transactions. Thus, a chain of blocks (transactions) of data becomes a “Blockchain” which is where the acronym gets its name. See Figure Below.

Building Blocks of Commercial Crypto-Technologies Solutions

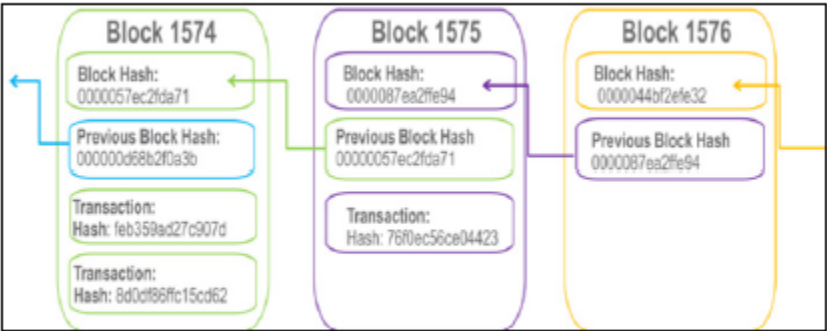


FIGURE 2-1: Blockchain stores transaction records in a series of connected blocks.

In theory, blockchain solutions are able to offer the building blocks of commercially viable crypto-technology solutions by incorporating key characteristics, such as data confidentiality, integrity and availability. However, whether these key characteristics are successfully implemented, secure and effectively maintained is another story for discussion below.

Some additional concepts blockchain technology presents is similar to how object-oriented programming added the ability to combine data and code to create a single object to act upon data, blockchain solutions are able to control transaction and data logical access controls and permissions such that access rights providing confidentiality can be built into the solution. For example, data on the blockchain can be encrypted such that only those with appropriate keys (often certificates) can access transaction details, enter, modify or view data while blocking visibility or modification by others accessing the same data. This feature allows a potential group of companies to share a blockchain while also maintaining integrity and confidentiality on chosen data to only those with appropriate access to the contents within the blockchain.

There are also options in terms of whether to make a blockchain public, keep it private, or even create a hybrid. A public blockchain is one that is accessible via the world wide web or Internet. A private blockchain is one that is not public, meaning none of the nodes managing the ledger are publicly-accessible or modifiable via public access. A hybrid solution is one where both a public and private blockchain can coexist such that the public aspect may announce the existence of a transaction and include the date and time, however the transaction details, such as the transaction participants, could be sealed in a private blockchain that is kept secret from the public.

Existing Commercial Blockchain Solutions and Applications

- 1) Crypto-Currency
- 2) Smart Contracts
- 3) Payments, Money Transfer

Building Blocks of Commercial Crypto-Technologies Solutions

Crypto-Currency

Perhaps the most publicized application of blockchain is crypto currency, such as Bitcoin mentioned earlier, although there are new crypto currency entities popping up all the time. Crypto-currencies are digital currencies generally built upon either a public or private blockchain ledger. Some of these crypto currency systems allow for mining while others do not. Bitcoin Mining is the process of being rewarded, in digital currency such as bitcoins, for performing computationally difficult math.

Bitcoin is a public blockchain crypto-currency that incorporates mining and is notorious for allowing Bitcoin holders the ability to be anonymous. More on anonymity later. Ethereum is more of a platform but is also a public blockchain and has its own crypto-currency, in Ethereum's case "Ether", and allows for mining. Stellar, primarily performs foreign money transfer and micro payments has a digital currency called Lumens, however Stellar does not incorporate Lumen mining and for the most part uses a Lumen as a currency intermediary. Ripple, is another digital currency calling their unit XRP. Similar to Stellar, Ripple does not incorporate mining.

For the most part, the existing crypto-currencies are able to be traded like a real currency on recently established digital currency exchanges (DCE) (Ref#7), however none of these digital currencies have any value of their own, only perceived value. These digital currencies can also be exchanged for fiat currencies as well. Perhaps the largest DCE in the United States is Coinbase headquartered in the Bay Area in California. Coinbase allows a digital currency holder to exchange one digital currency to another but also provides a way to convert a digital currency to a fiat currency such as US Dollars.

Smart Contracts

Another notable application of blockchain technology is smart contracts, where details and documents of a contract, its participants and payment are stored within a data structure and included in the blockchain. Ethereum provides this capability. In 2015, DocuSign developed and showcased their own Digital Transaction Management (DTM) Platform based on blockchain (Ref#8) in cooperation with Visa. There has not been any material updates since 2015 from Visa or DocuSign with regard to blockchain, nonetheless, smart contracts is certainly a viable and easy to understand application of blockchain technology.

It is easy to surmise that in designing a smart contract solution there could be utilization of both public, private and possibly also hybrid blockchain elements. This would be determined by the amount of public and private data maintained within a given solution as well driven by the sources and authentication mechanisms deployed for a given solution.

Payments, Money Transfer

Building Blocks of Commercial Crypto-Technologies Solutions

Micro Payments are loosely defined as a payment of \$10 or less and a foreign payment is one traditionally serviced by Western Union with their “MoneyGram” product that involve a currency conversion from one fiat currency to another. Both micro payments and small value foreign currency transfer lend themselves to blockchain and digital currencies being used as an intermediary much like a world bank might. Companies performing these services include Stellar and Ripple. In order to facilitate and execute a foreign currency transfer both Stellar and Ripple partner with local, in country, banks, (Stellar calls them Anchor Banks) to perform fiat currency conversion. In the case of Stellar, the Anchor banks allow the receiver of the funds to decide whether they would like their funds delivered in Lumens or in a fiat currency. In general, these solutions do not appear to support multi-party asset-based transactions and assume same day or instant clearing and settlement (meaning, there is not float risk with conversion rates defined prior to or at transaction time). From the marketing literature these solutions seem to target consumers conducting relatively low value money transfers.

What are the counter arguments and known pitfalls using blockchain?

- 1) Early Adoption – Blockchain Hyper Ventilation
- 2) Fraudulent Initial Coin Offerings (ICO’s)
- 3) Criminal Element
- 4) System Failure
- 5) Threat of Government Shutdown
- 6) Taxation requirements
- 7) Cryptocurrency not worth anything, keys lost = money lost let alone fraud
- 8) Can we count on privacy, reliability, integrity, etc.

Early Adoption – Blockchain Hyper Ventilation

Businesses are popping up all over the world that deal in some way with blockchain and money is pouring in from private and now public sources.

It is clear, based on the roller coaster ride of BitCoin’s value, and by combining recent history of technology leaps such as Dot Com era the market for blockchain solutions is in Hyper Ventilation mode creating a crypto-bubble and investors should be very careful.

During the Dot Com era several fraudulent companies accepted investments and never really had a product or solution, yet investors continued to pile in money into the Internet craze. All you needed back then was Dot Com, Online or Web Anything to a name and the same seems to be true now with crypto-currency and/or blockchain although this time the phrases are “Blockchain” or “Crypto-Something”. More than likely, we will see a bubble and then that bubble will burst disappointing thousands of investors.

There has been a real fervor over Bitcoin value which peak at nearly \$20,000 several months ago to today the value is half that. In BitCoin’s case there never was any value to Bitcoin and

Building Blocks of Commercial Crypto-Technologies Solutions

other than what people gave it. There is no government backing or guarantee of any kind and it is possible to completely lose all your Bitcoins. Dr Jacobson, an Iowa State University Professor and Director of ISU Information Assurance Center refers to using Bitcoin as an investment strategy as very risky, resembling a Ponzi scheme (Ref#9).

It appears to the writer that any blockchain solution that delivers anonymity would be of highest risk because it could get shutdown at any moment by a government or group of governments rendering the value useless due to lack of liquidity. Similar to due diligence required during the Dot Com era, it is important to validate revenue and earnings prior to investment or participating in using a given solution.

Fraudulent Initial Coin Offerings (ICO's)

I find it interesting that many crypto currency startups have headquartered, incorporated, and/or have legal residence in some very strange places around the globe. Some of these are in countries where the Europe and the U.S. have no substantial diplomatic relationship and have legal reciprocity. This should be a red flag to any investor. The only logical reason to do this seems to be for the founders and those responsible to hide and escape responsibility of defrauding investors. One of the techniques used in defrauding investors is rather than get investors buying stock or options they buy initial coin offerings (ICOs). The fine print says the ICO is a work product of the company but does not represent ownership of the company and therefore provides no legal recourse or ownership to the investor. Of course, if one invested in Bitcoin early on the investor would have seen massive profits, but it is hard to call that investing it is more like gambling and is purely speculative.

The Securities and Exchange Commission recently warned investors on crypto currency exchanges (Ref#11) risk operating illegally because they don't disclose how they prioritize investors orders that trade on their markets. The SEC went on to say they are going to regulate not only the products but the places where they traded who trades them. At the time of this writing there were virtually no laws passed governing crypto-currencies, their usage or exchange.

So all the while Switzerland expresses a desire to be the crypto-currency capital of the world and boasts 4 of the 10 biggest ICO's in the last year (Ref#11), regulators around the world are working toward clamping down on crypto currencies (Ref#12) because of the investor fraud and criminal attraction.

Criminal Element

In the early years of Bitcoin there is a well documented (Ref#13) level of criminality referred to as "Silk Road" but also others where Bitcoin was used to anonymously purchase all sorts of illegal items such as drugs, endangered species of animals and birds, and was also used in illegal activity, such as human trafficking and conspiracy to commit murder, and so on.

Building Blocks of Commercial Crypto-Technologies Solutions

It is fairly easy to understand why criminals would be attracted to anonymous purchases and a digital currency, perhaps this is why Bitcoin might be called the currency of the dark web.

Because of criminal activity, or in this case lack of financial regulatory compliance, money transfer business was suspended in the Philippines, and a Venezuelan based crypto-currency site attempting to operate in the United States was banned by President Trump (Ref#14).

The criminal activity continues with hackers recently discovered trying to obtain crypto-currency credentials through a Chrome Extension using Facebook (Ref#15) and this one is not the first or only example of hackers trying to get to crypto-currency, nor will it be the last.

System Failure

There are some technological limitations to a public blockchain and it has been postulated that a government entity or nation state could potentially foul up the blockchain works by setting up and running more than 50% of the operating nodes on a network and then falsely approve transactions. Doing so could not only undermine a crypto-currency but potentially could be so devastating the currency would be useless. Just because the design includes a distributed redundant solution does not mean it cannot be attacked or a solution is impervious to attack. Assuming such would be reckless, in fact, it is probably better to assume that sometime in the future a system will be successfully attacked and stage a plan to recover gracefully and without error.

Whether a system incorporates a public, private or hybrid blockchain there are certainly risks from a system, user and network perspective.

One of the fastest ways to hurt yourself would be to lose your keys or credentials to a crypto-currency wallet provider and have not backup. You may technically still own coins but in a practical sense you may find yourself in an unrecoverable state. Similarly, if the wallet service provider is offline or hacked you would then also lose access to your accounts which is akin to throwing your money in a sewer drain.

Actually, the system failure could occur due to exploitation of a vulnerability, DDOS attack, a human act or a software bug. A system failure could occur simply due to a loss of data integrity and it may not be immediately abundantly clear how to restore the system. As the saying goes, don't put all your eggs in one basket if you do choose to invest or speculatively trade digital currencies.

Threat of Government Shutdown

As stated prior, the SEC is stating it is planning on regulating and monitoring investments into ICO's which is probably in the public interest. That said, a non-conforming digital currency solution such as Petro from Venezuela could be shut down with little or no warning or recourse. Law Enforcement around the world is quite aware of digital currencies being used to support or

Building Blocks of Commercial Crypto-Technologies Solutions

carry out criminal activity and it is the writer's expectation we will reach a breaking point one day where a multi-country solution must be found with standards set and operational requirements provided to give law enforcement full visibility to criminal transactions and data so that criminals can be apprehended and charged, evidence secured and documented, which will likely also result in systems being shut down or unavailable for a serious amount of time.

We don't get all the details but it would not surprise me if terrorist organizations use an anonymous digital currency to carry out their criminal agenda either directly or indirectly. Because of this and other document criminal activity the writer assumes for the greater good of society we will force digital currencies to comply or face being shut down.

Taxation Jurisdiction

At some point the author expects government jurisdictions and taxing authorities to understand and tax Blockchain transactions where the taxing process may follow the ever-evolving world of online internet purchases which were not initially taxed.

When the value of transactions and/or the number of transactions gets interesting for taxing authorities it is the expectation of the writer that new laws and operating procedures will be established virtually banning anonymous transactions so that all transactions can be identified, a jurisdiction established and taxed with assessment going to correct individuals and/or entities. So, for those people that think Bitcoin and other digital currencies allow people to avoid taxes, well today that may be true, but it can't last forever and could certainly not get to the point where a digital currency replaces a fiat currency without changes to the existing laws and regulations.

Cryptocurrencies are not actually worth anything

Remember, crypto-currencies are not actually worth anything in and of themselves. There is no bank or government standing behind digital currencies, there are no guarantees by entities of substance that are accessible, and there are no protections or recourse in anonymous transactions. Crypto-currencies, instead, wholly rely on user confidence or "Belief in the System".

Crypto-currencies simply do not have intrinsic value nor a guarantor, not to mention the inherent operational risk of 100% unrecoverable losses due to fraud, system failures, DDOS or loss of access, or even government shutdown any of which can drive real or perceived value to zero in the blink of an eye.

There could be value in anonymous transactions enabled by crypto-currencies for those that "Believe in the System" that can deliver untraceable exchange of digital currencies for items of real value, such as a fiat currency, good or service. This same capability can be exploited by criminals to perform money laundering or enable a criminal underground financial network and thus the author of this paper does not hold anonymous transactions of value.

Building Blocks of Commercial Crypto-Technologies Solutions

The building blocks of a Commercial Crypto Technology Solution

- 1) Confidentiality
 - a. Must not be compromised
 - b. Public v Private Blockchain
- 2) Integrity
 - a. Secure, not hacked or allow unauthenticated manipulation
 - b. Sufficient Nodes
- 3) Availability
 - a. Maintain Control
 - b. Online Operation Requirement
- 4) Non-Repudiation
- 5) Other Requirements
 - a. No Anonymity
 - b. Compliant
 - c. Provide users legal recourse

In the writer's view, the building blocks of a commercial crypto technology solution must provide confidentiality, integrity, availability, non-repudiation, must not support anonymous participants, must be compliant with existing laws and regulations and must provide users legal recourse.

Confidentiality, Integrity and Availability

A pillar to building any commercial crypto technology solution is maintaining data confidentiality, integrity, and availability.

A commercial solution must be maintained in a secure manner so that data is secure and not compromised, while also keeping private data private, the solution must ensure private data is not exposed to unauthorized users, hacked or leaked regardless of using a public, private or hybrid blockchain.

This should include a complex multilevel authentication solution that identifies and authenticates systems, acceptable nodes, users and rights management, and data level encryption unique to control access. The solution should also be able to prevent and report potential data leaks.

The commercial crypto technology solution must also maintain data integrity and must not be open to hacks or unauthorized manipulation of data. If a commercial solution employs a consensus methodology to accept and post transactions to the ledger then the number of

Building Blocks of Commercial Crypto-Technologies Solutions

participating and authenticated nodes in the solution must be sufficient based on the design of the solution relative to public and private ledgers.

Maintaining system availability is another critical aspect of a successful commercial crypto technology solution. The design and implementation must have performance metrics that define an acceptable level of performance whether public, private or a hybrid approach. Consideration must be given to expansion, user access (public and private) and the depth of blockchains and data in calculating impact into processing requirements in order to maintain a successful crypto technology solution working well into the future.

An important attribute of ledger transactions is non-repudiation, in short, the participants cannot be allowed to later deny the authenticity or intent of a transaction. Therefore, it is recommended a commercial crypto technology solution properly authenticate users and confirm understanding and intent of transactions, as well as, comply with existing laws relative to rights of rescission such that at the point in time when a transaction is final it cannot be undone except by a court of law or some other legal means.

Additional requirements include not allowing or supporting any transactions that accommodate anonymity. Anonymity simply invites the wrong crowd and is not welcome in a commercially viable crypto technology solution.

It is important to understand and maintain compliance within all operating locals as well as remain compliant where users utilize the solution as well as where business (exchange of value) may actually be conducted.

Lastly, a successful crypto technology solution must provide participants legal recourse. This will require identifiable and validated participants as well as data, but in addition, sufficient details and clarity of terms, conditions, sufficient asset condition and descriptions, and so forth in order to provide participants full knowledge and also allow courts to establish responsibility in the case of legal recourse.

Considering the above and the current state of blockchain solutions, what are some examples of potentially innovative crypto technology solutions and applications?

Near Term

- 1) Authentication of Things (AOT)
 - a. Devices
 - b. People
 - c. Software
 - d. Data
- 2) Document Management
- 3) Supply Chain Management

Building Blocks of Commercial Crypto-Technologies Solutions

Future

- 1) Voting
- 2) Stocks and Commodities
- 3) Energy Supply
- 4) Peer to Peer Global Transactions
- 5) Government, such as FDA, CDC

Authentication of Things (AOT)

In the near term, with relative ease, it is the writers opinion that we will see an expansion of crypto technology solutions focused in the Authentication of Things (AOT). We have had a way to mutually authenticate technological things using keys or certificates much in the way the TLS 1.2 protocol describes. However, many of the deployed solutions were not universally accepted and used as much as initially thought, such as PGP, and several authentication solutions were not made available to the public. Why can't we create a mobile phone application that authenticates the ATM one is about to use, or authenticates or rejects callers to our IP based phones and do so using a public blockchain?

Perhaps we can establish and authenticate a structure and hierarchy of relationships between devices, people, software and data such that we can associate and authenticate data to software, software to a device, and a device to a person such that changes to our authenticated structure are either not allowed or provide the authenticated person a chance to validate an action...such as someone else using their cell phone or laptop.

This new industry of AOT should focus on practical time savings and security and bring to the individual, whether in a personal or professional situation, commercially viable crypto technology solutions.

Document Management is a layup for a crypto technology solution. Today, we have DocuSign and Adobe providing document management solutions, however these are generally used in the B2B or B2C realm. The writer envisions a commercially viable personal C2C solution based on a hybrid blockchain where the user can establish a private blockchain within a public one and choose to share authenticated documents created and edited by validated users using authenticated systems and software and share publicly, privately or elements of both.

With the struggles of Facebook and other online providers it seems a C2C crypto technology solution could be used as a subcomponent offering or made to be compatible with a General Public Licensed solution to better protect individual information and limit exposure.

Lastly, it appears to the writer that multi-level, multi-entity supply chain solutions are well suited for crypto technology adoption where governments, corporations, distributors and users can all be utilizing the same solution for information while also keeping private information

Building Blocks of Commercial Crypto-Technologies Solutions

private. For example, an egg producer needs to manage feed, inventory, inspections, etc, in joint efforts with suppliers, buyers, distributors, and government and regulatory agencies. Today, many of the participant systems are built and managed separately and do not share information directly, if at all. Such that, if an issue is discovered during inspection it can take quite a while to link sufficient data to take action. The writer envisions Crypto Technology Integrations as part of plan to reduce cost and share information while also maintaining security, confidentiality, integrity, etc. This concept may best begin with a third party integration firm working in tandem with participants staff to design, develop and set rule sets and from there a consortium can maintain the joint systems.

There are several other applications of crypto technology solutions that today seem more difficult, either technically or politically, such as using blockchain in voting systems, and additional governmental management solutions which can be used by the CDC, FDA, FNS, and more. The writer expects an explosion of crypto technology solutions to hit the market, whether known or invisible to reduce cost and risk to fundamental transactions in life whether that be buying a house or sharing a picture of your family with loved ones.

In summary, this document reviewed blockchain technology, current and potential future commercial crypto technology solutions, and defined the building blocks for a commercial viable solution as well as presented innovative ideas for new crypto technology solutions and applications.

Thus far, crypto currency has taken the lions share of the publicity, it is the writers opinion that will change in the coming years and well into future as more and more applications and solutions are developed and deployed.

Building Blocks of Commercial Crypto-Technologies Solutions

Resources and References

Ref#1 <https://charts.bitcoin.com/chart/price>

Ref#2 <https://coinmarketcap.com/>

Ref#3 <https://techstartups.com/2018/02/26/global-blockchain-technology-market-to-reach-60-7-billion-in-2024/>

Figure #1 From IBM Blockchain for Dummies, Manav Gupta

Ref#4 IBM Blockchain for Dummies, Manav Gupta

Ref#5 <https://ercim-news.ercim.eu/en110/special/distributed-access-control-through-blockchain-technology>

Ref#6 <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/>

Ref#7 https://en.wikipedia.org/wiki/Cryptocurrency_exchange

Ref#8 <https://www.docuSign.com/press-releases/docuSign-showcases-smart-contracts-payments-prototype-built-for-visas-connected-car>

Ref#9 <https://wallethub.com/blog/is-bitcoin-safe/32920/#doug-jacobson>

Ref#10 <https://www.wsj.com/articles/sec-warns-investors-on-cryptocurrency-exchanges-1520457355>

Ref#11 <https://www.wsj.com/articles/switzerland-wants-to-be-the-world-capital-of-cryptocurrency-1524942058>

Ref#12 <https://www.wsj.com/articles/regulators-worldwide-are-cracking-down-on-cryptocurrency-indias-next-1523008125>

Ref#13 [https://en.wikipedia.org/wiki/Silk_Road_\(marketplace\)](https://en.wikipedia.org/wiki/Silk_Road_(marketplace))

Ref#14 <https://techcrunch.com/2018/03/19/trump-bans-venezuelan-cryptocurrency-in-the-us/>

Ref#15 <https://thehackernews.com/2018/05/facebook-cryptocurrency-hacking.html>

<https://www.entrepreneur.com/article/306420>

Etherium.com and Ethdocs.org

Stellar.org

Ripple.com

Block Chain Revolution, Don Tapscott

Coinmarketcap.com

Building Blocks of Commercial Crypto-Technologies Solutions

WallStreetJournal.com

Paymnts.com