People's Democratic Republic of Algeria
Ministry of higher education
University of Abdelhamid Ibn Badis Mostaganem
Faculty of exact and computer sciences
Department of computer science

2017/2018

MASTER'S THESIS

Blockchain Technology for Secure Storage and Transfer of Electronic Health Records

Prepared by :

ATTOU Aymen

Supervised by :

DR.Chahinez Bentaouza

Abstract

The goal of this study is to identify the current applications of blockchain and we want to bring the idea of the blockchain solutions to the healthcare industry.

Patient’s medical data on a decentralized secure Proof ledger is the key for personal ownership, interoperability and is a lifetime history of care.

Data is encrypted and managed by the consensus and can only accessed by the owner. By today’s standards, the blockchain is more private, liquid, costs less to administer and provides a real-time lifesaving flow of medical and health data. Basing ourselves on the blockchain technology that over the past two decades, the Internet has revolutionized many aspects of business and society... Yet the basic mechanics of how people and organizations execute transactions… have not been updated for the 21st century. Blockchain could bring to those processes the openness and efficiency we have come to expect in the Internet Era ; blockchain is a distributed database that is currently most known for being the technology used for storing transaction information of digital currencies such as the Bitcoin. Through a literature review and interviews with domain experts, research and taking part of international conferences , we identified some current application areas for blockchain, that is, money transactions, decentralized data and privacy protection, and decentralized autonomous organizations (DAO). Within the area of decentralized data and privacy protection, we further identified the two sub-areas of smart contracts and secure identities. In addition, we identified some possible application areas by conducting a second literature review. That helped us do identify all existing solutions weaknesses and possible improvements to this subject so we could introduce some new research concepts.

The contribution of this study can be used for further studies through each of the above application areas in order to identify possible advantages and disadvantages.

Keywords: Blockchain, Bitcoin, EHR, Decentralized privacy, Data protection, Smart contract, Distributed systems, Health industry, Electronic medical records, Decentralized record management system, Proof of work.

Acknowledgement

First and foremost, I want to thank those who have been involved in this work in different ways:

My explicit gratitude goes to my supervisor, Dr. Chahinez Bentaouza, for convincing me not to choose a safe topic, but to take the challenge of a very new and hot topic, with more potential but also more uncertainties. Thank you also for motivating me to apply for cooperation with ISDRS2018; it made both the working processes more interesting and the results more valuable. My fruitful discussions with her qualified feedback have been of high value.

I am grateful to Mostaganem University and the Department of Computer science for supporting me to finish my Master's thesis. And to accomplish all my higher education in the best conditions. especially the dean Houari Benmekki of the faculty who get us involved in many extra curriculum activities and open source projects and also Madam Temdi Samira the head of the international office for her help during my mobility in Italy, I also want to thank my Professor Henni Fouad for being a great professor that gave me a very strong bases in Algorithms, computer architecture and programming, and for assisting me during all this period. Without forgetting also a big thanks to my friends and fellow students for feedback and discussions, encouragement and proof-reading especially Bouali-youcef zakaria and Bekaddour Mohammed Nadir.

Big Thanks to those at MDSLab in Italy, who have been part of this Research, special thanks to all professors for showing their interest and inviting me to conferences for a productive workshop which was the basis for the case study.

Finally, I want to take this opportunity to express my gratitude to my parents, who supported me throughout the five years of studying by believing in me, leaving me the freedom to go my own way, and last but not least giving me economic support so that I was able to focus on studying and extracurricular engagement.

Thank you all, your support is very much appreciated!

Summary

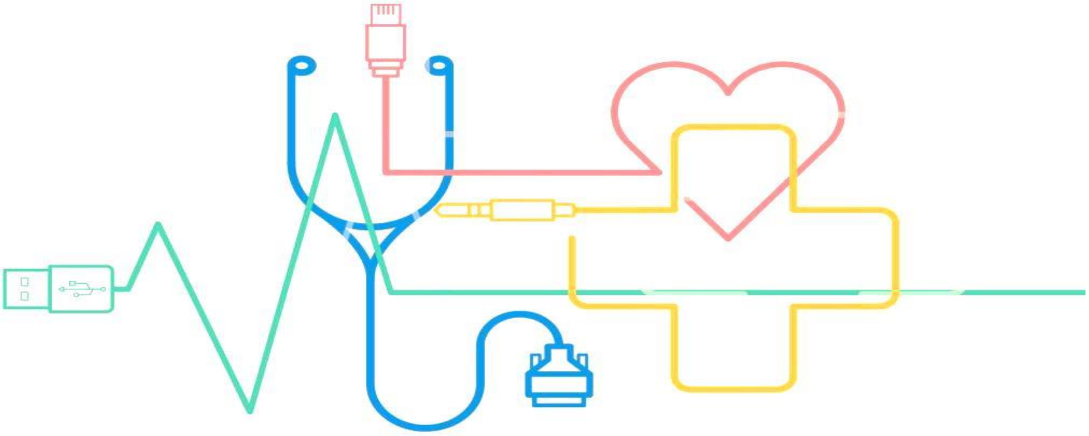


Table of Figures

Table of Tables

Table of Abbreviations and definitions

BTC	**Bitcoin**
EHR	**Electronic health record**
EMR	**Electronic Medical record**
Public (Buterin, 2015a)	**“a blockchain that anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the consensus process”**
Private (Buterin, 2015a)	**“A blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent.”**
Consortium (Buterin, 2015a)	**“a blockchain where the consensus process is controlled by a preselected set of nodes. The right to read the blockchain may be public, or restricted to the participants.”**
Public(BitFury Group,2015)	**“a blockchain, in which there are no restrictions on reading blockchain data (which still may be encrypted) and submitting transactions for inclusion into the block- chain.”**
Private(BitFury Group,2015)	**“a blockchain, in which direct access to blockchain data and submitting transactions is limited to a predefined list of entities.”**
Permissioned(BitFury Group,2015)	**“a blockchain, in which transaction processing is performed by a predefined list of subjects with known identities.”**
Permissionless(BitFury Group,2015)	**“a blockchain, in which there are no restrictions on identities of transaction processors (i.e., users that are eligible to create blocks of transactions).”**
Permissionless(Walport,2016)	**“A ledger that allows anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies.”**
Permissioned(Walport,2016)	**“May have one or many owners. The ledger’s integrity is checked by a limited consensus process. This is carried out by trusted actors.”**
Distributed Ledger(Walport,2016)	**“Are a type of database that is spread across multiple sites, countries or institutions, and is typically public.”**
Shared Ledger (Walport,2016)	**“to any database and application that is shared by an industry or private consortium, or that is open to the public. spectrum of possible ledger or database designs that are permissioned at some level.”**

Introduction

People use the term ‘blockchain technology’ to mean different things, and it can be confusing. Sometimes they are talking about The Bitcoin Blockchain, sometimes it’s The Ethereum Blockchain, sometimes it’s other virtual currencies or digital tokens, sometimes it’s smart contracts. Most of the time though, they are talking about distributed ledgers, i.e. a list of transactions that is replicated across a number of computers, rather than being stored on a central server.

The common themes seem to be a **data store** which:

- Usually contains **financial transactions**
- Is replicated across **a number of systems** in almost **real-time**
- Usually exists over a **peer-to-peer** network
- Uses **cryptography** and **digital signatures** to prove identity, authenticity and enforce read/write access rights
- Can be **written** by certain participants
- Can be **read** by certain participants, maybe a wider audience, and
- Has mechanisms to make it **hard to change historical records**, or at least make it easy to detect when someone is trying to do so

We see “blockchain technology” as a collection of technologies, a bit like a bag of Lego. From the bag, you can take out different bricks and put them together in different ways to create different results.

Blockchain has shown its usefulness when recording events like transactions. This usefulness could be extended to medical records, which often suffer from inaccuracy and discrepancies. Healthcare professionals are responsible for ensuring that sensitive medical records are accurate, complete, and only available to authorized individuals. All of this can prove to be difficult when healthcare providers all have different systems for storing information. For example, prescription records are one aspect of medical records that could be positively impacted by blockchain. Just imagine if a patient’s prescription information was left vulnerable to manipulation by hackers. Simply put, the more quality and secure that health information is, the better the quality and care.

Research questions

Supply chains lack transparency due to their complexity and fragmentation. Blockchain technology is increasingly expected to revolutionize businesses and promises to create trustworthy transparency. This study aimed to investigate the potentials of blockchain technology for supply chain transparency beyond the growing glorification.

The purposes are captured within the following four research questions:

1- What are the current application areas of the blockchain?
2- What is the lack of the current electronic health records?
3- What can the block chain technology provide to the health industry?
4- How can we integrate block chain into the health industry?

Limitations

The blockchain technology began with the Bitcoin crypto currency [1] in 2008. It is an issue that this new and young technology just began being used for different areas and it is still in testing stages for many application areas such as banking [2]. The limitation is that there are not many academic works in this manner being done.

Target

This research provided a starting point for further research, as it provided a strong basis to start from. Most important future research could focus on a further (quantitative) refinement of Environments with highly institutionalized values, to present Electronic health records with clear criteria or factors (even EHR tools or frameworks) on when to use blockchain technology. Also, a further comparison of our core category to Smart contracts and Electronic medical records literature could further improve the conceptualization of blockchain technology in the scientific literature. Finally, the formalization of our substantive theory on blockchain technology consequences is paramount to further develop understanding of blockchain technology from an economic perspective.

In the first chapter, we will explore the block chain technology and then we will find to gather a projection of the consensus and this technologies characteristic into the medical health records finally we will reach details about possible prototypes and implementations of this concept that is a research proposal itself.

I. BlockChain TECHNOLOGY

With a blockchain, many people can write entries into a record of information, and a community of users can control how the record of information is amended and updated.

I.1) What is blockchain?

Blockchain is an information storage and transmission technology that is transparent, secure, and operates without a central control body (Blockchain France definition).

By extension, a blockchain is a database that contains the history of all the exchanges between its users since its creation. This database is secure and distributed: it is shared by its various users, without intermediaries, which allows each one to check the validity of the channel.

There are public blockchains, open to all, and private blockchains, whose access and use are limited to a number of actors.

A public blockchain can therefore be assimilated to a public, anonymous and unfalsifiable public accounting book. As the mathematician Jean-Paul Delahaye writes, we must imagine "a very large notebook that everyone can read freely and free of charge, on which everyone can write, but which is impossible to erase and indestructible [1].

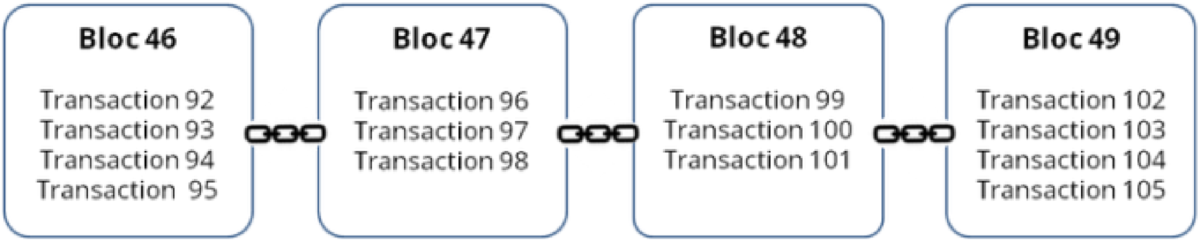


Figure I.1 : Chain blocks modelling [1]

This why we found it a very exciting time for health care and information technology (IT)[1]. Due to improvements in genetic research and the advancement of precision medicine, health care is witnessing an innovative approach to disease prevention and treatment that incorporates an individual patient's genetic makeup, lifestyle and environment. Simultaneously, IT advancement has produced large databases of health information, provided tools to track health data and engaged individuals more in their own health care. Combining these advancements in health care and information technology would foster transformative change in the field of health IT[2].

I.2) How it works?

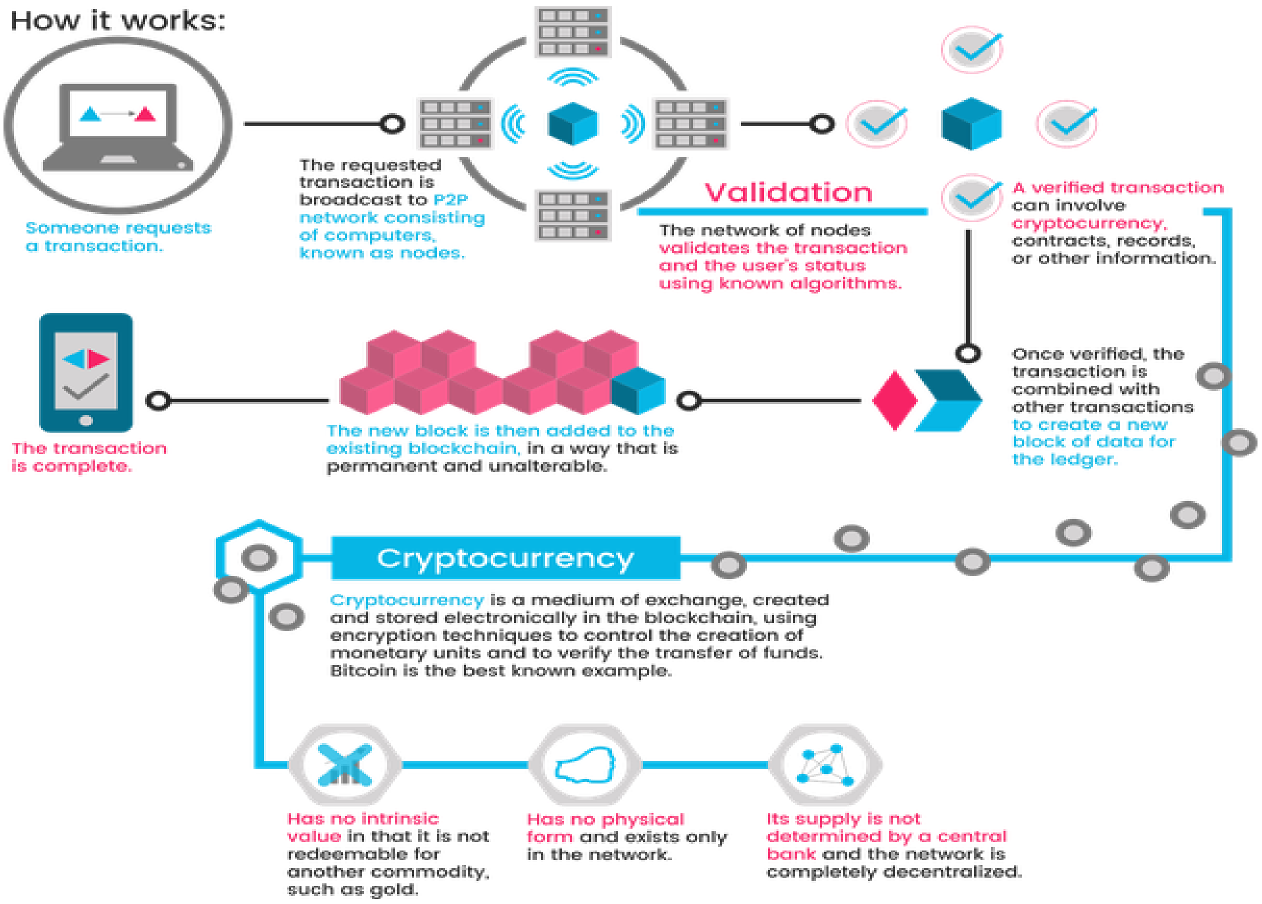

How it works:
Someone requests a transaction.
The requested transaction is broadcast to P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.
Cryptocurrency
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.
Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.

Figure I.2 : blockchain process [2]

Use Case:

- ✓ Applications for the transfer of assets (monetary use, but not only: securities, votes, shares, bonds, etc.)
- ✓ Applications of the blockchain as a register: this ensures better traceability of products and assets.
- ✓ Smart contracts: these are stand-alone programs that automatically execute the terms and conditions of a contract without requiring human intervention once started.

Implementation of the concept:

the first logical step is to decide the block structure. To keep things as simple as possible we include only the most necessary[2].

I.3) Private vs public

There is a big difference in what technologies you need, depending on whether you allow *anyone* to write to your blockchain, or known, vetted participants. Bitcoin allows *anyone* to write to its ledger[2].

Public blockchains. Ledgers can be 'public' in two senses:

- Anyone, without permission granted by another authority, can **write** data
- Anyone, without permission granted by another authority, can **read** data

Usually, when people talk about *public* blockchains, they mean anyone-can-write.

Because bitcoin is designed as a 'anyone-can-write' blockchain, where participants aren't vetted and can add to the ledger without needing approval, it needs ways of arbitrating discrepancies (there is no 'boss' to decide), and defence mechanisms against attacks (anyone can misbehave with relative impunity, if there is a financial incentive to do so). These create cost and complexity to running this blockchain[3].

Private Blockchains. Conversely, a 'private' blockchain network is where the participants are known and trusted: for example, an industry group, or a group of companies owned by an umbrella company. Many of the mechanisms aren't needed – or rather they are replaced with legal contracts – "You'll behave because you've signed this piece of paper." This changes the technical decisions as to which bricks are used to build the solution[3].

	Permissionless	**Permissioned**
Public	- No restrictions on who can read data - No restrictions on who can submit transactions or program - No Restrictions on who can take part in the consensus mechanism	- No restrictions on who can read data - No restrictions on who can submit transactions or programs - Restrictions on who can take part in the consensus mechanism
Private	- Restrictions on who can read data - Restrictions on who can submit transactions or programs - No Restrictions on who can take part in the consensus process	- Restrictions on who can read data - Restrictions on who can submit transactions or programs - Restrictions on who can take part in the consensus mechanism

table I.1 : permissionless vs permissioned

I.4) Blockchain in other words

- DATA STORAGE

A blockchain is just a file. A blockchain by itself is just a data structure. That is, how the data is logically put together and stored. Other data structures are databases (rows, columns, and tables), text files, comma separated values (csv), images, lists, and so on. You can think of a blockchain competing most closely with a database [3].

Blocks in a chain = pages in a book

for analogy, a book is a chain of pages. Each page in a book contains:

The text: for example the story

information about itself: at the top of the page there is usually the title of the book and sometimes the chapter number or title; at the bottom is usually the page number which tells you where you are in the book. This ‘data about data’ is called meta-data.

Similarly in a blockchain block, each block has:

the contents of the block, for example in bitcoin is it the bitcoin transactions, and the miner incentive reward (currently 25 BTC).

a ‘header’ which contains the data about the block. In bitcoin, the header includes some technical information about the block, a reference to the previous block, and a fingerprint (hash) of the data contained in this block, among other things. This hash is important for ordering.

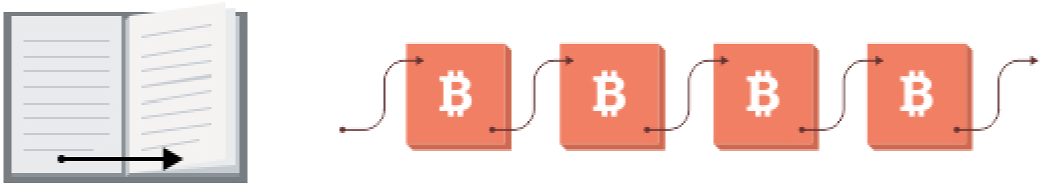


Figure I.3: Block ordering in a blockchain[4]

Block is ordered in a blockchain:

Page by page. With books, predictable page numbers make it easy to know the order of the pages [4]. If you ripped out all the pages and shuffled them, it would be easy to put them back into the correct order where the story makes sense.

Block by block. With blockchains, each block references the previous block, not by 'block number', but by the block's fingerprint, which is cleverer than a page number because the fingerprint itself is determined by the contents of the block [5].

- **Internal consistency:**

By using a fingerprint instead of a timestamp or a numerical sequence, you also get a nice way of validating the data. In any blockchain, you can generate the block fingerprints yourself by using some algorithms. If the fingerprints are consistent with the data, and the fingerprints join up in a chain, then you can be sure that the blockchain is internally consistent. If anyone wants to meddle with any of the data, they have to regenerate all the fingerprints from that point forwards and the blockchain will look different[6].

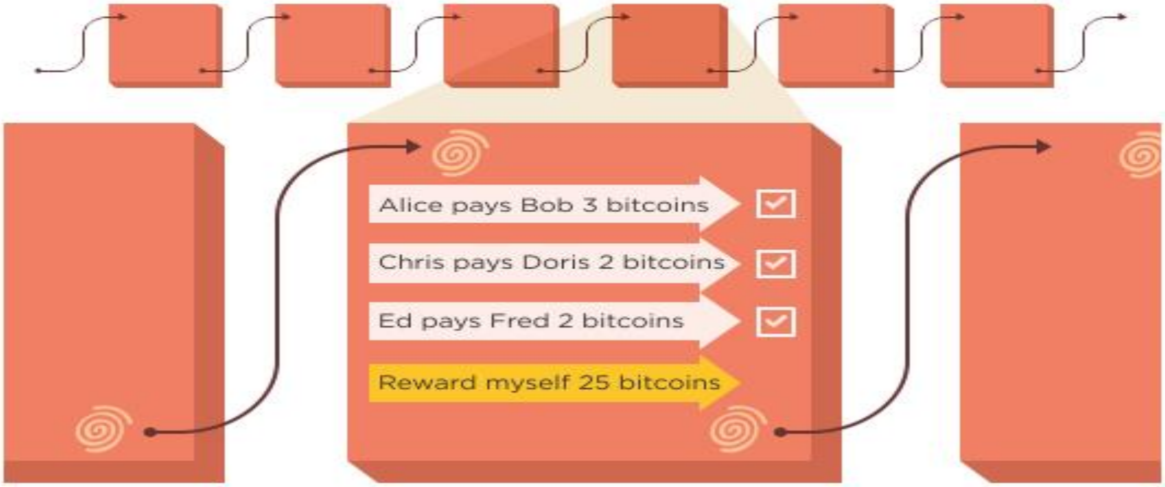

Alice pays Bob 3 bitcoins
Chris pays Doris 2 bitcoins
Ed pays Fred 2 bitcoins
Reward myself 25 bitcoins

Figure I.4 : DATA DISTRIBUTION [4]

Data distribution
Peer to peer is one way of distributing data in a network. Another way is client-server. You may have heard of peer-to-peer file sharing on the BitTorrent network where files are shared between users, without a central server controlling the data. This is why BitTorrent has remained resilient as a network.

Client-server
In the office environment, often data is held on servers, and wherever you log in, you can access the data. The server holds 100% of the data, and the clients trust that the data is definitive. [6] Most of the internet is client-server where the website is held on the server, and you are the client when you access it. This is very efficient, and a traditional model in computing[6].

Peer-to-peer

In peer-to-peer models, it's more like a gossip network where each peer has 100% of the data (or as close to it as possible), and updates are shared around. Peer-to-peer is in some ways less efficient than client-server, as data is replicated many times; once per machine and each change or addition to the data creates a lot of noisy gossip [6]. However, each peer is more independent, and can continue operating to some extent if it loses connectivity to the rest of the network. Also peer-to-peer networks are more robust, as there is no central server that can be controlled, so closing down peer-to-peer networks are harder [7].

A common conflict is when multiple miners create blocks at roughly the same time. Because blocks take time to be shared across the network, which one should count as the legit block?

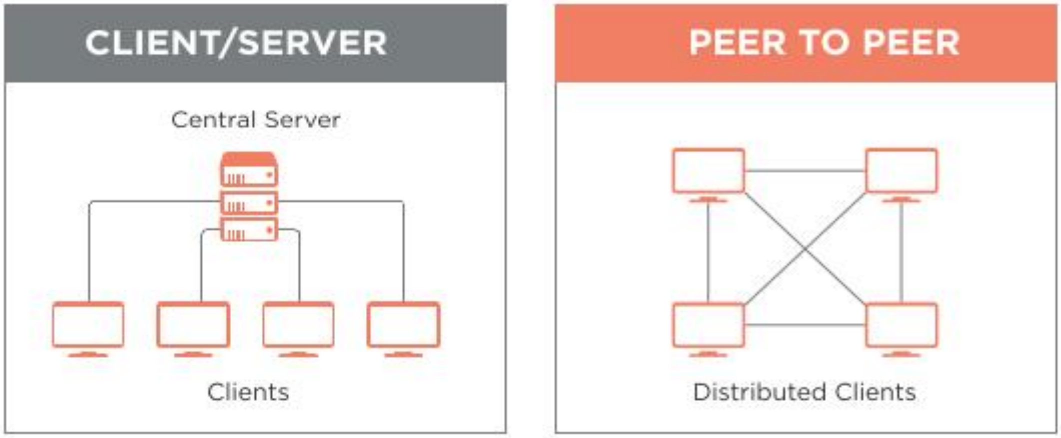


Figure I.5: Client/server vs peer to peer architecture [7]

Example. Let's say all the nodes on the network have synchronized their blockchains, and they are all on block number 80.
If three miners across the world create 'Block 81' at roughly the same time, which 'Block 81' should be considered valid? Remember that each 'Block 81' will look slightly different: They will certainly contain a different payment address for the 25 BTC block reward; and they may contain a different set transactions. Let's call them 81a, 81b, 81c.

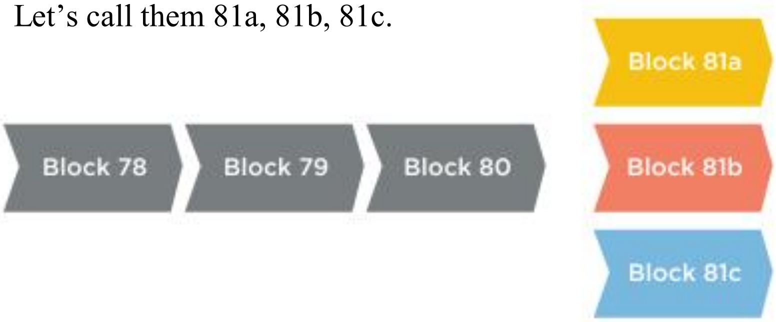
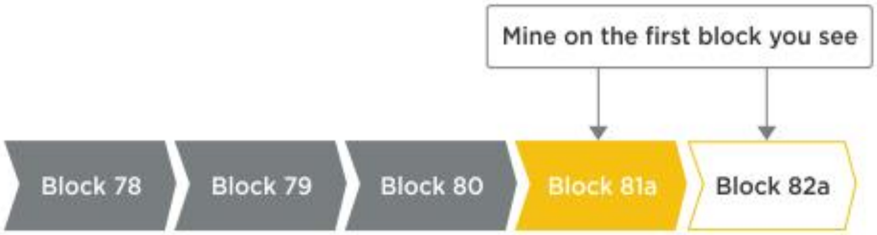


Figure I.6: blockchain synchronization positioning [8].

Longest chain rule. In bitcoin, the conflict is resolved by a rule called the “longest chain rule”.

In the example above, you would assume that the first ‘Block 81’ you see is valid. Let’s say you see 81a first. You can start building the next block on that, trying to create 82a:

Figure I.7: blockchain synchronization selection [9]



I.5) Be a part of blockchain

In the bitcoin network, theoretically anyone can download or write some software and start validating transactions and creating blocks. Simply go to https://bitcoin.org/en/download and run the “Bitcoin core” software [10].

Your computer will act as a full node which means:

- Connecting to the bitcoin network
- Downloading the blockchain
- Storing the blockchain
- Listening for transactions
- Validating transactions
- Passing on valid transactions
- Listening for blocks
- Validating blocks
- Passing on valid blocks
- Creating blocks
- ‘Mining’ the blocks

The source code to this “Bitcoin core” software is published on GitHub: https://github.com/bitcoin/bitcoin. If you are so inclined, you can check the code and compile and run it yourself instead of downloading the prepackaged software at bitcoin.org. Or you can even write your own code, so long as it conforms to protocol [10].

Permissionless

Note that you don't need to sign up, log in, or apply to join the network. We can just go ahead and join in. Compare this to the SWIFT network, where you can't just download some software and start listening to SWIFT messages. In this way, some call bitcoin 'permissionless' vs SWIFT, which would be 'permissioned' [10].

Permissionless is not the only way

you may want to use blockchain technology in a trusted, private network. You may not want to publish all the rules of what a valid transaction or block looks like. You may want to control how the network rules are changed. It is easier to control a trusted private network than an untrusted, public free-for-all like bitcoin [10].

I.6) What about security

A problem with permissionless or open networks is that they can be attacked by anyone. So there needs to be a way of making the network-as-a-whole trustworthy, even if specific actors aren't.

What can and can't miscreants do?

A dishonest miner can:

- Refuse to relay valid transactions to other nodes
- Attempt to create blocks that include or exclude specific transactions of his choosing
- Attempt to create a 'longer chain' of blocks that make previously accepted blocks become 'orphans' and not part of the main chain

He can't:

- Create bitcoins out of thin air*
- Steal bitcoins from your account
- Make payments on your behalf or pretend to be you

That's a relief.

**Well, he can, but only his version of the ledger will have this transactions. The other nodes will reject this, which is why it is important to confirm a transaction across a number of nodes.*

With transactions, the effect a dishonest miner can have is very limited. If the rest of the network is honest, they will reject any invalid transactions coming from him, and they will hear about valid transactions from other honest nodes, even if he is refusing to pass them on.

With blocks, if the miscreant has sufficient block creation power (and this is what it all hinges on), he can delay your transaction by refusing to include it in his blocks. However, your transaction will still be known by other honest nodes as an ‘unconfirmed transaction’, and they will include it in their blocks.

Worse though, is if the miscreant can create a longer chain of blocks than the rest of the network, and invoking the “longest chain rule” to kick out the shorter chains. This lets him **unwind a transaction**.

Here’s how you can do it:

- Create two payments with the same bitcoins: one to an online retailer, the other to yourself (another address you control).
- Only broadcast the payment that pays the retailer.
- When the payment gets added in an honest block, the retailer sends you goods
- Secretly create a longer chain of blocks which excludes the payment to the retailer, and includes the payment to yourself .
- Publish the longest chain. If the other nodes are playing by the “longest chain rule” rule, then they will ignore the honest block with the retailer payment, and continue to build on your longer chain. The honest block is said to be ‘orphaned’ and does not exist to all intents and purposes.
- The original payment to the retailer will be deemed invalid by the honest nodes because those bitcoins have already been spent (in your longer chain).

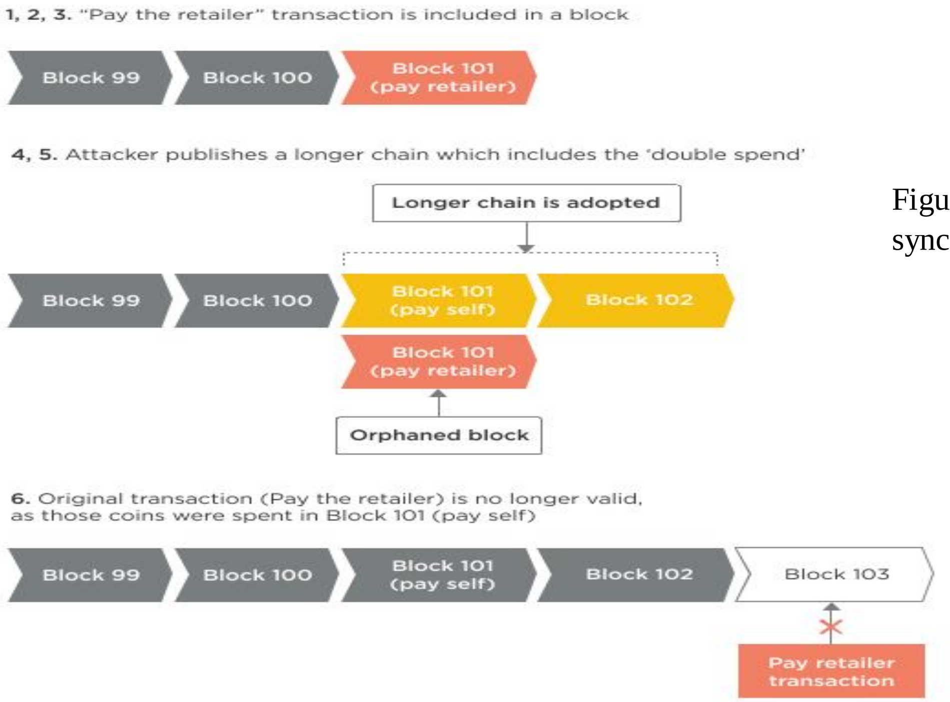

1, 2, 3. "Pay the retailer" transaction is included in a block
Block 99
Block 100
Block 101 (pay retailer)
4, 5. Attacker publishes a longer chain which includes the 'double spend'
Longer chain is adopted
Block 99
Block 100
Block 101 (pay self)
Block 102
Block 101 (pay retailer)
Orphaned block
6. Original transaction (Pay the retailer) is no longer valid, as those coins were spent in Block 101 (pay self)
Block 99
Block 100
Block 101 (pay self)
Block 102
Block 103
Pay retailer transaction

Figure I.8: blockchain synchronization process [8]

I.7) Key management

Each participant in a blockchain possesses one or more private keys, which they use to digitally sign transactions relating to the addresses they own. The security of these private keys is paramount – if a user's private key is compromised, any other user on the blockchain can forge transactions from that user. This can include spending that user's assets, writing stream items in their name, or changing other users' permissions on their behalf [11].

By default, private keys are stored in MultiChain's built-in wallet, a regular disk file on the computer where each MultiChain node is running. Although this wallet can be encrypted on disk, its contents can still be read if the computer is sufficiently compromised. MultiChain therefore allows private keys to be stored separately from the node, e.g. in another computer or hardware security module. This external private key can be randomly generated by MultiChain using the createkeypairs API command, or by an external bitcoin-compatible software library.

By using the importaddress API command, MultiChain can track the activity of any address without needing its private key. MultiChain can also be used to build an *unsigned* transaction for imported addresses using the createrawsendfrom API.

An unsigned transaction can be signed in one of two ways. The simplest method is to use MultiChain's signrawtransaction API command, passing in the private key(s) as a parameter, then passing the result to sendrawtransaction for broadcast. While this method briefly exposes the private key to MultiChain, it will not be stored on the server's disk.

A more complex but safer method is to sign the transaction completely outside of MultiChain, only using sendrawtransaction to broadcast the signed transaction. This requires an external software library or hardware device that is able to unpack the raw transaction and generate and add the signature(s) to its input(s). MultiChain uses bitcoin's transaction structure and cryptography, so any bitcoin-compatible library or device should be fine, so long as it does not choke on per-output and per-transaction metadata.

In this part, we will focus on the simplest method, since it does not require any additional software or hardware. The part requires one MultiChain node running version 1.0 alpha 28 or later, which should have at least one address with admin, issue and create permissions. If you don't yet have this, follow the instructions in section 1 of the Getting Started guide and then run multichain-cli chain1 to enter interactive mode.

- ✓ Creating the private key and address

Let’s begin by asking MultiChain to generate a new private key and corresponding address, without storing either in the node’s wallet:

```
createkeypairs
```

Copy and paste the address shown: 1...

Copy and paste the privkey shown: V...

Now let’s import the address into the node, without its private key:

```
importaddress 1... '' false
```

The false at the end saves time by not scanning the blockchain for activity relating to this address, because we know it hasn’t been used before.

At this point, let’s look for another address that we can use for receiving assets later in this tutorial. Run both of these commands:

```
listpermissions receive
listaddresses
```

An address is suitable if it appears in the output of the both commands.

Enter the address here: 1...

You should also see the imported address 1... listed in the output from listaddresses together with "ismine" : false.

- ✓ Issuing an asset to the address

Let’s go back to the imported address, grant it some permissions and issue a new asset to it:

```
grant 1... receive,send
issue 1... asset0 50000 0.001
```

Now we can check that the address has receive the new asset units:

```
getaddressbalances 1... 0
```

The 50000 units of asset0 shown be shown. Note that if we had not added the address using importaddress, we would not be able to query its balance in this way.

- ✓ Sending from the address

Now we'll send some of the newly issued asset from the imported address to another one. First:

createrawsendfrom 1... '{"1...":{"asset0":2000}}'

The response should contain a hexadecimal blob containing the raw unsigned transaction, which should be copied to the clipboard. We'll now sign the transaction using the external private key:

signrawtransaction [paste-hex-blob] '[]' '["V..."]'

The response should contain a complete field with value true, along with a larger hexadecimal blob in the hex field. This means that the transaction has been signed and is ready for broadcasting to the blockchain. Copy the new hexadecimal blob, and run:

sendrawtransaction [paste-bigger-hex-blob]

The response should contain the 64-character hexadecimal txid of the sent transaction. Now let's check that the 2000 units of asset0 have been successfully transferred:

getaddressbalances 1... 0
getaddressbalances 1... 0

- ✓ Publishing from the address

First let's create a new stream which we will use in the tutorial:

create stream stream0 true

Now let's prepare to publish something to this stream from the imported address:

createrawsendfrom 1... '{}'
'[{"for":"stream0","key":"key0","data":"457874657726e616c2069732073616665737374"}]'

The response should contain a hexadecimal blob containing the raw unsigned transaction, which should be copied to the clipboard. Now sign the transaction using the external private key: signrawtransaction [paste-hex-blob] '[]' '["V..."]'

The response should contain a complete field containing true, along with a larger blob in the hex field, containing the signed transaction. Copy the new blob, and run: sendrawtransaction [paste-bigger-hex-blob]

The response should contain the txid of the sent transaction. Finally let's check that the item was published successfully:

subscribe stream0
liststreamitems stream0

You should see one stream item, with 1... shown in the list of publishers.

- ✓ Where to go from here

Well done! You have now learned how to send assets and publish to a stream using an address whose private key is held outside of the node’s wallet. As mentioned in the introduction, instead of passing the private key to signrawtransaction, a bitcoin-compatible software library or hardware could be used to sign the transaction without ever revealing the private key to MultiChain itself.

A similar technique can be used to perform any other action for an address with an external private key – issuing or reissuing assets, creating streams, and granting/revoking permissions for other addresses. In each case, examples of the appropriate createrawsendfrom parameters can be found on the raw transactions page. Remove the final parameter send from the createrawsendfrom commands in those examples, then complete the process using signrawtransaction (or external signing) and sendrawtransaction as above.

The block chain is a **shared public ledger** on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.

I.8) Examples of properties and quotes in the open coding phase:

This section presents three examples of quotes and properties, to further clarify the use of this technology.

- ❖ Effect in Financial Sector: Cost savings
- Oliver Wyman

“Many clients (particularly on the buy side) will expect to accrue the most benefit, from the reduction in costs of capital markets dealing and securities servicing. Retail and wholesale investors may transact more among themselves, now with guaranteed execution on open markets.”

- World federation of exchanges

“Broadly speaking, respondents highlighted the cost savings (for the responding entity and the industry more broadly), efficiency enhancement and risk reduction as their main reasons for investigating the application of DLT to the use cases which are set out above. “

- IBM

“The cost effectiveness of such an infrastructure would also be critical to underpin a future ‘internet of things’, he adds. “With the number of devices connected to the internet exploding and they all becoming potential users of banking services, this technology may enable us to offer services at much lower cost,” he says.

“Real distributed ownership enabling machine to machine interactions – that is going to be really transformational,” agrees Julio Faura, Head of R&D, Banco Santander. “A use case for this could be payments in the context of the internet of things.” “

- ❖ Function in Financial Sector: Verify Transactions
- Credit Suisse

“The blockchain is increasingly recognized as the most significant technical innovation of bitcoin. Google search data reflects this trend and we have noted a rapid recent increase in our clients’ interest in blockchain's disruptive potential, particularly its impact on the payments space. Most simply, the blockchain protocol is a cryptographically secure system of messaging and recording in a shared database. Working in tandem, these systems enable the secure record, verification and confirmation of transactions without the need for a central counterparty to administer the system.”

- Cognizant

“The lure of blockchain was its method of verifying and tracking transactions. Instead of a trusted third-party or a central bank, it relies on consensus among a peer-to-peer network of computers based on complex algorithms.”

- Kynetix

“With a centralised ledger that publicly records the movement of every asset, along with proof of ownership and the authenticity of assets protected by a coded secure cryptographic framework and with confirmations of new trades identified by a unique crypto stamp, there is a significant reduction in manual processes.

- ❖ Hype issues
- Credit Suisse

“On the streets of Davos this year there are only three discussions being held. One: robots are going to take over our jobs. Two: blockchain is amazeballs and three: FinTech is like blockchain amazeballs, but with even more possibilities to control and mould the behaviours of the common man.”

- Bloomberg

“Part of the answer is that the blockchain vogue has a certain universality right now, at least among financial- technology types, that makes it an appealing pitch across markets. "We need to find a way to reduce processing time in syndicated loan markets" is a pretty niche pitch, perhaps appealing to the back-office guy who handles syndicated loans. "We want to use the blockchain to trade syndicated loans" might get you a higher-level audience, perhaps with the chief technology officer or the head of loan trading. And "we want to use the blockchain to trade syndicated loans and Treasury repos and private company shares and whatever else you've got" could get you in front of the CEO."

- de Volkskrant (translated from Dutch)

"The internet sector is shocked by the theft of 50 million dollars at "The DAO", an online investment fund without staff, managers or direction. The DAO uses a technology called blockchain. The theft heavily undermines one of biggest tech hypes of this moment. The most well know application of blockchain technology is currently bitcoin, a virtual coin that enables transactions that is not traceable or forgeable."

- ZDnet

"I haven't seen anything as hyped in such a short period of time as the blockchain ... The answer to every question seems to be 'blockchain'," said Peter Williams, chief edge officer at Deloitte's Centre for the Edge. "I expect that at the next Miss World, 'What do you want to do?' 'I want to solve world peace by using a blockchain, and end poverty and world hunger as well," he told the APIdays conference in Melbourne on Wednesday. Williams said we have an "irrational exuberance" for blockchain, the distributed ledger at the heart of Bitcoin and other cryptocurrencies. He's right. Just follow the Twitter account @bitcoin_txt for some of the more ludicrous comments from its fans. But as I've written previously, Bitcoin is an ideology, and it's unlikely to ever be workable for everyday transactions."

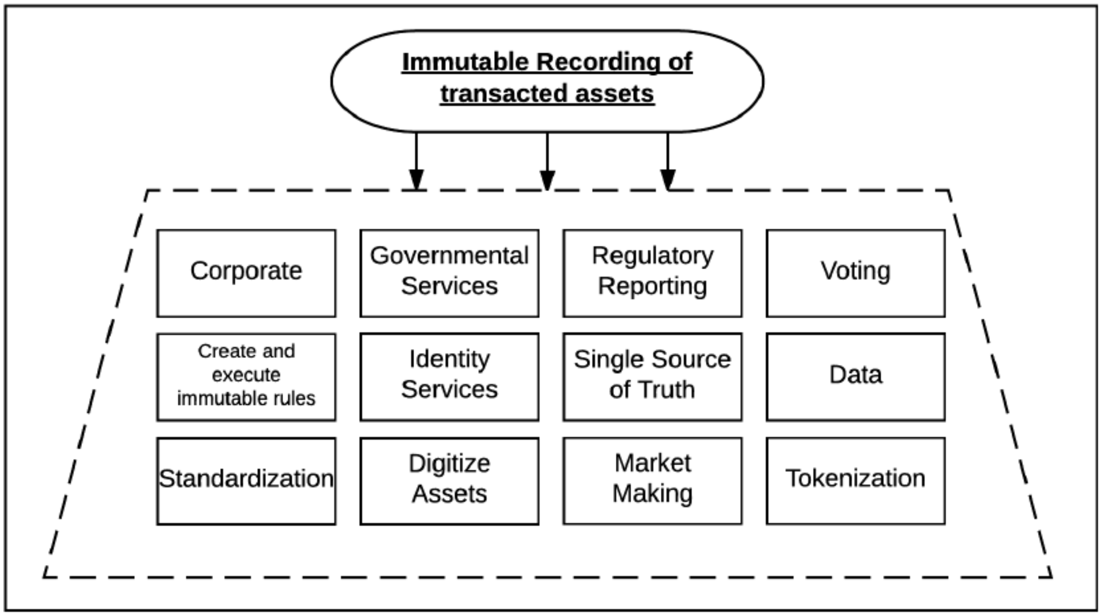


Figure I.9 Overview of the dimensions in sensitizing concept Functions [10]

Block chain can have a much wider use than a simple payment method, including various industries. So, how does blockchain actually work in the healthcare industry?

II. How blockchain can revolutionize healthcare & medical records

II.1) Introduction

The cryptocurrency market has seen many different initial coin offerings launched over the last year. Many of these new market players have presented the industry with disruptive applications of blockchain technology that fulfill a specific purpose and today I will share a project in the area of Medical health records.

Medical Blockchain plans to introduce blockchain technology to the electronic health records (EHR) industry. The blockchain securely stores health records and maintains a single version of the truth. Different medical organizations and individuals—like doctors, hospitals, labs, and insurers—can request permission to access a patient's record of the blockchain. Patients have more control over who sees their data, while healthcare providers can provide better patient care based on more accurate data and can provide a new foundation and structure for health information management by making electronic medical records more efficient, without intermediaries and empowering patients to be the owners of their own records [14].

II.2) Background

The Electronic Health Record (EHR) is a digital version of a patient's medical history maintained by a healthcare provider over the course of their visits. The record includes patient information on demographics, diagnosis, vital signs, past medical history, progress over time, lab tests and more [14].Some major advantages offered by an EHR system include accurate and up-to-date patient information, reduced healthcare cost in long term, quick access to patient related data, reduced medical errors, increased patient participation and improved efficiency of healthcare providers [15].

II.3) Electronic Health Record (EHR) Market

The global market for electronic health record (EHR) features a largely fragmented vendor landscape, with the presence of a large number of small and large players and the top five companies cumulatively accounting for a nearly 44% of the overall market in 2016. [16] Hospitals remain leading users of Electronic Health Records and the most prominent buyers as 65% of the hospitals across the globe have installed some form of EHR in 2015 compared to

54% in 2014. The segment is expected to remain the top end-use sector of the global EHR market.

Europe and Asia Pacific are also among the leading contributors of revenue to the global market and are expected to remain high-growth regions over the forecast period as well. These countries are expected to offer immense potential for EHR market as the continually growing economy of these nations will encourage healthcare providers to adopt technically advanced EHR systems [16].

Globally Government funding encouraging the meaningful use of certified EHR technology across healthcare facilities, increasing pressure for healthcare cost containment and rising demand for improved quality of healthcare services are among the major factors driving the growth of the EHR market in the North American market. Factors such as rapid technological advancement with data access through smartphones need for improved efficiency and quality of service delivery to sustain in the intensively competitive healthcare industry, and increasing disposable income are also expected to fuel the growth of the market [17]. And nowadays it is way more challenging than ever and we have to take the proper actions for it

II.4) Problem

The biggest challenge that is being faced by health care systems throughout the world is how to share medical data with known and unknown stakeholders for various purposes while ensuring data integrity and protection patient privacy. Although data standards are better than ever, each electronic health record (EHR) stores data using different workflows, so it is not obvious who recorded what, and when and hence creating a trusted environment for decision-making is a challenge for the medical fraternity. The growing focus on care coordination and EHR access across the care continuum has raised questions about how to ensure that multiple providers can view, edit, and share patient data while still maintaining an authoritative and up-to-date record of diagnoses, medications, and services rendered [18].

The EHR problem is not merely a problem of data sharing logistics. Every solution that deserves serious consideration in a national healthcare system needs to put patient privacy and informational freedom of choice first in its list of priorities. In US for almost a decade, hospitals have been waiting for EHRs to usher in a shiny new era of standardization and high-quality health care[19]. But while federal laws and incentive programs have made health care data more accessible, the vast majority of hospital systems still can’t easily (or safely) share their data. Solutions should be sought in which patients themselves control whom to divulge their identity, where to remain pseudonymous, and which pieces of data to share [18].

II.5) Opportunities

The inherently sensitive nature of health data, along with the perennial challenges of interoperability, patient record matching, and health information exchange, have created opportunities for a blockchain approach. The information presented by EHR on the distributed ledger of a permissioned Blockchain would be perfectly reconciled community-wide, with the assured integrity from the point of data generation to the point of use, without manual human intervention. The Blockchain solution for healthcare industry drastically reduces the time required to access patient's information, enhances system interoperability and improve data quality [19].

The use of blockchain also enables a reduction in overhead costs, particularly for development and maintenance of legacy health record systems. Successful deployment of blockchain for health records allows data transition between related parties in an efficient, consensus-based, seamless manner [19].

Once a blockchain is deployed to manage EHRs, it becomes the unified and common backbone for digital health. Expanding on the consequences of this development on the future of specialized backend systems, the implication of using this backbone is that each hospital or care provider no longer needs a specific version of databases or software to access patient data. The other advantage is that the development cycle for health data software is simplified significantly

Instead of relying on a designated intermediary for information exchange, such as a state-designated HIE or a private network established between local hospitals, the decentralized nature of the blockchain would allow any approved participants to join an exchange community, without the need to build data exchange pipes between certain organizations.

As an example of the growing interest of Governments and organizations around the world for EHRs in Blockchain, in January 2017, the Food and Drug Administration announced a research partnership with IBM Watson to find ways to safely share data from EHRs, clinical trials, genetic sequencing, and even mobile wearables using the blockchain approach. Blockchain trusted verification of electronic health can open new avenues of using intelligent agents for anonymous data reporting to track population statistics and trends [20].

II.6) Blockchain & Electronic Health Record (EHR)

Blockchain helps in providing a universal set of tools for cryptographic assurance of data integrity, standardized auditing, and formalized contracts for data access. The end result would be perfectly reconciled community-wide information about you, with guaranteed integrity from the point of data generation to the point of use, without manual human intervention. Blockchain could enable a comprehensive, interoperable and secure EHR data exchange in which health consumers are the ultimate owners of their EHRs. These transactions and records are created by different nodes on the network, such as a provider or a consumer uploading health data [20].

Blockchain ensures information on the chain is verified by requiring users to provide a signature and time-stamp with a private key to access the data. Therefore, the logic built into blockchain allows consumers to have the best of both worlds, providing access to doctors when they need it, while simultaneously protecting data from unauthorized users. The use of multiple digital signatures via PKI and cryptographic hashes ensures health metadata and EHR hashes travel the network securely and are accessible only to those parties with the correct public keys to access them. The blockchains use of digital signatures to create a unique patient identifier ensures all records on the chain bearing that identifier are linked to create a comprehensive EHR for that patient across his/her providers and payers. The health metadata blockchain avoids the scalability challenges that placing data-intensive EHR records in their vast numbers directly on the blockchain may impose on the technology [20].

The health metadata blockchain and EHR systems together comprise a holistic solution that enables secure exchange of EHR data and overcome incompatibilities among systems at the provider level[3]. With the EHR metadata blockchain, every provider, patient, payer, health system, record, medical device, wearable, etc. can be a part of the network. This fact, along with the immutable quality of the blockchain public ledger, ensures no one can alter the providers EHR record after the fact. The unique digital signatures carried by all stakeholders, data and transactions in a blockchain will streamline the process of creating aggregated and accurate research data sets by preventing information fragmentation and enabling correct merging of records. Blockchain technology can track and timestamp each access of and addition to an EHR, providing an immutable audit trail while ensuring the most recent version of the record is always used [20].

II.7) Medical Blockchain Platform

Medical BC is a blockchain for electronic health records. Medical BC will enable different healthcare agents such as doctors, hospitals, laboratories, pharmacists and insurers to request permission to access and interact with medical records. Each interaction is auditable, transparent, and secure, and will be recorded as a transaction in Medical BC’s distributed ledger [21].

It is built on the permission based Hyperledger Fabric architecture which allows varying access levels; patients control who can view their records, how much they see and for what length of time. The blockchain is currently in development. Medical BC is working with Coinsilium, NHS, Wings, and Hyperledger to bring the platform to life [21].

Medical BC aims to offer the following core benefits to patients and healthcare providers: Data can only be accessed by the patient’s private key; even if the database is hacked, the patient’s data will be unreadable (it’s all encrypted) Patients have full control over accessing their healthcare data; patients will control who sees their data and what they see Instantaneous transfer of medical data, where every member of the distributed network of the health care blockchain would have the same data for the patient; there’s a reduced risk of errors, and better patient care [22].

II.8) Features

The implementation of blockchain in health records offers all of the following features:

Enhanced Privacy and Access Control where the users can setup access permissions and give certain providers permission to write data to their blockchain. Real-time & Secure Doctor to Patient Communication where Patients can share their records, get second opinions, and communicate online with medical professionals through a secure channel. Robust Licensing of Health Records by Patients where patients can choose to license their electronic health records to different parties—say, pharmaceutical companies—for research.

Blockchain is thus the decentralized ledger of transactions happening across peer networks. Through this technology, there is no need of a central certifying authority to conform the transactions, including fund transfers, selling trades, managing vital information and so on. This is all done seamlessly with increased transparency and accurate tracking methods that leads to a greater level of cost reduction.

As explained earlier, one of the industries that benefits greatly through Blockchain technology is healthcare because patient information is shared across multiple providers with absolutely no risk of security or privacy breaches. The technology allows for documenting the transactions in decentralized ledgers, bringing in transparency and saving on other crucial resources like time and cost [23].

Utilization of this technology in this manner will engage millions of individuals, health care entities, medical researchers, health care provides to share vast amounts of data released to every aspect of life with guaranteed privacy protection and security. This event could lead to precision medicine and advancement of medical research to pave the way for improved health and timely prevention of diseases [23].

II.9) Process Flow

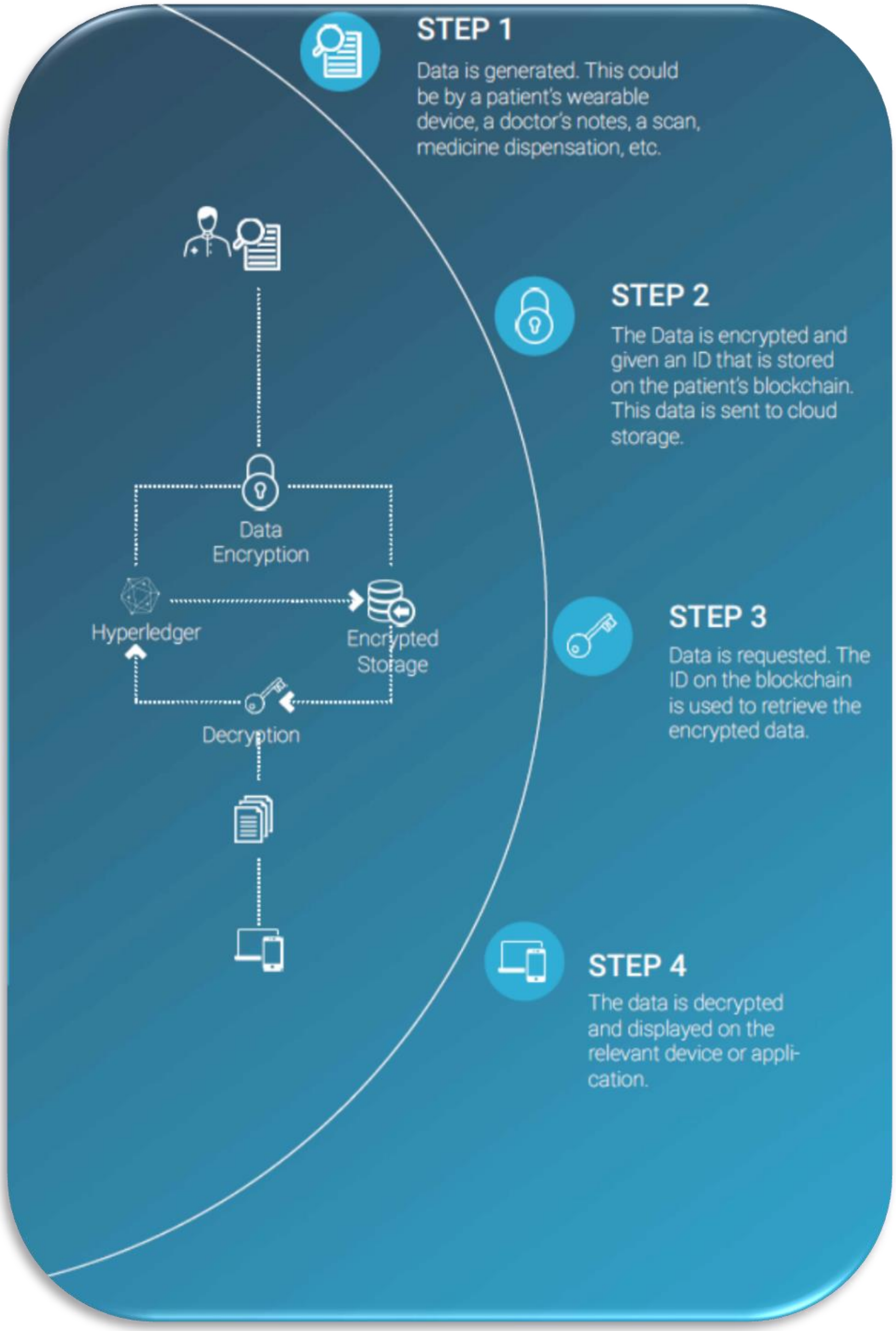

STEP 1
Data is generated. This could be by a patient's wearable device, a doctor's notes, a scan, medicine dispensation, etc.
STEP 2
The Data is encrypted and given an ID that is stored on the patient's blockchain. This data is sent to cloud storage.
STEP 3
Data is requested. The ID on the blockchain is used to retrieve the encrypted data.
STEP 4
The data is decrypted and displayed on the relevant device or application.
Data Encryption
Hyperledger
Encrypted Storage
Decryption

Figure II.1 Process flow

The basic process used in a Medical BC transaction and data entry is given below.

II.10) Final Thoughts

Health records on Blockchain is building the future of healthcare on Blockchain where there are also other Blockchain companies vying to get a pie of the Medical industry. The blockchain era has already begun. Taking into account the fast progress in the development of new and more efficient healthcare record systems, wearable devices, and medical examination systems implementing artificial intelligence, cryptography will become an important part of the way hospitals work. There are, however, a few improvements still needed in order for seamless blockchain adoption across the entire medical industry. According to Hyperledger's survey, 42.9% of healthcare organizations suppose that the interoperability of electronic health records will help for faster blockchain implementation; with 28.6% of respondents ready to use this technology in care settings today.

There is no doubt that the blockchain revolution has made significant changes in the healthcare industry. Here are some ways in which it answers the challenges that the industry faced before the technology became so popular:

- Fragmented Data

a. Computer networks aid in accurate patient data through decentralized storage
b. Data can be shared across networks and nodes
c. Decentralized source of internet
d. Timely Access to Patient Data

- Distributed ledger system facilitates distributed, secure access to patient health data

a. Updates to patient's shared data done in real time
b. System Interoperability

- Decentralized Internet and computer networks across boundaries

a. High-level authenticity
b. Data Security

- Digital transaction security ensured; this protects patient identity

a. Patient Generated Data

- Holistic patient data collected through data from wearable IoT

b. Access and Data Inconsistency

- Select healthcare companies enjoy consistent and rule-based method to access and analyze patient data through Smart Contracts.

a) Cost Effectiveness

- System turns highly efficient through real-time processing and reduced transaction costs

a) No third-party applications, so no time-lag in accessing data

III. Build application

A vexing problem facing health care systems throughout the world is how to share more medical data with more stakeholders for more purposes, all while ensuring data integrity and protecting patient privacy.

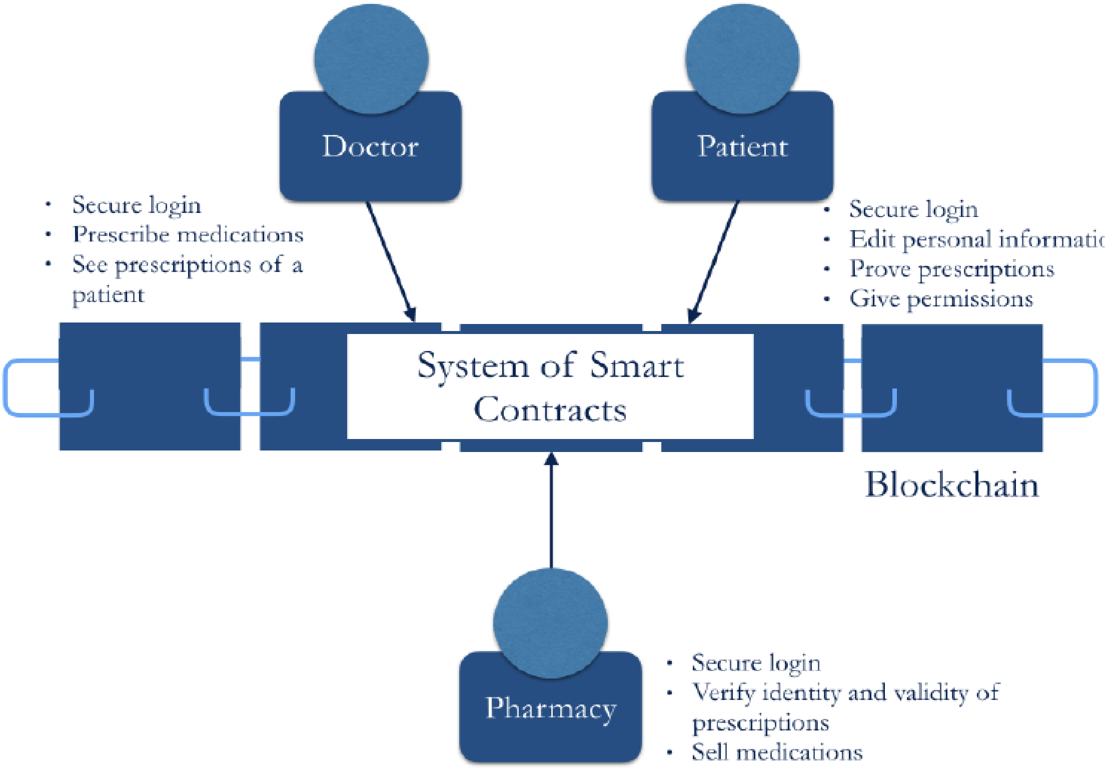
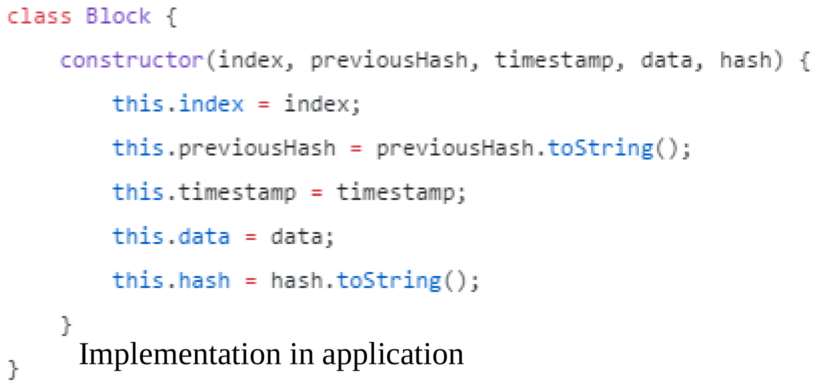


Figure III.1 General architecture

III.1) Building steps

Step 1=> block Structure:

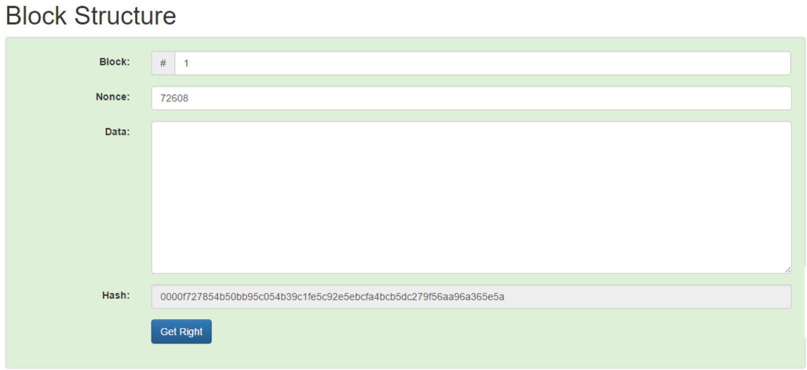
Transaction data is permanently recorded in files called **blocks**. They can be thought of as the individual pages of a city recorder's record book (where changes to title to real estate are recorded) or a stock transaction ledger. Blocks are organized into a linear sequence over time (also known as the block chain). Each block contains, among other things, a record of some or all recent transactions, and a reference to the block that came immediately before it. It also contains an answer to a difficult-to-solve mathematical puzzle - the answer to which is unique to each block. New blocks cannot be submitted to the network without the correct answer - the process of "mining" is essentially the process of competing to be the next to find the answer that "solves" the current block.



```
class Block {
    constructor(index, previousHash, timestamp, data, hash) {
        this.index = index;
        this.previousHash = previousHash.toString();
        this.timestamp = timestamp;
        this.data = data;
        this.hash = hash.toString();
    }
}
```

Figure III.2 block Structure implementation

Implementation in application



Block: # 1

Nonce: 72608

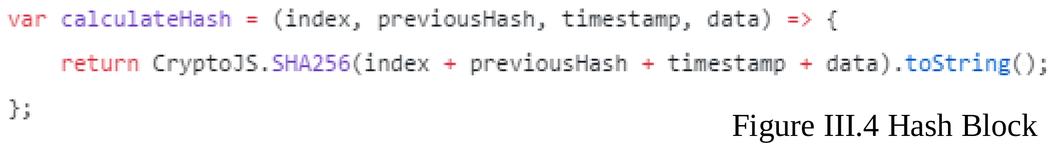
Data:

Hash: 0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a

Figure III.3 block Structure

Step 2 =>Hash Block:

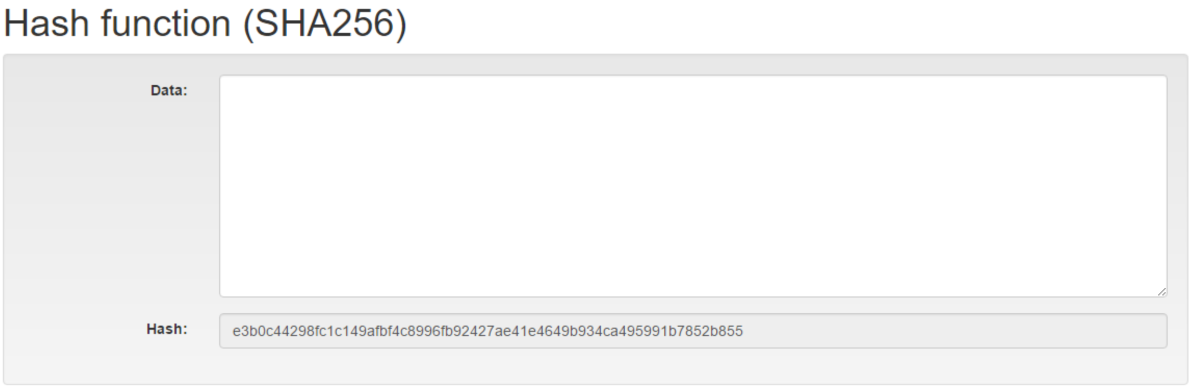
The block needs to be hashed to keep the integrity of the data: The algorithm to link the blocks to each other is a cryptographic hash (of its small intimate name SHA256). It will mix the incoming data in order to output a number. The complication comes from the fact that this mixture is irreversible: it is impossible to start from the arrival number to go back to the arrival data without making a lot of random assumptions. This is exactly what miners do: insert many output numbers into this function until the input digit matches certain criteria. After this random aspect, the minors can add a block of the waiting pool to the last block of the chain. Each node of the network, called node, represents a computer connected via its wallet, which has a complete copy of the blockchain.



```
var calculateHash = (index, previousHash, timestamp, data) => {
    return CryptoJS.SHA256(index + previousHash + timestamp + data).toString();
};
```

Figure III.4 Hash Block

SHA-2 (Secure Hash Algorithm) is a family of hash functions that have been designed by the US National Security Agency (NSA), modeled on the SHA-1 and SHA-0 functions, Of the MD4 function of Ron Rivest (which gave parallel MD5). As described by the National Institute of Standards and Technology (NIST), it includes the functions SHA-256 and SHA-512 whose algorithms are similar but operate on different word sizes (32 bits for SHA-256 and 64 bits For SHA-512), SHA-224 and SHA-384 which are essentially versions of the previous ones whose output is truncated, and more recently SHA-512/256 and SHA-512/224 which are truncated versions of SHA-512. The last suffix indicates the number of bits of the hash.



Hash function (SHA256)

Data:

Hash: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Figure III.5 Hash Block implementation

Step 3=> Coherence of blocks:

To generate a block we must know the hash of the previous block and create the rest of the required content.

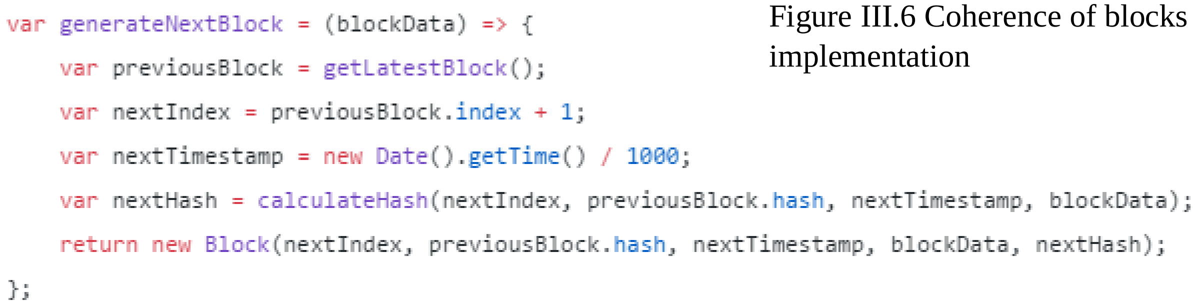
The chain links together all the updates in our ledger. It's useful to use Bitcoin as an analogy - while its unpermissioned nature means there are fundamental differences to the ledgers we are looking at, it remains the most widely used blockchain implementations.

A series of Bitcoin transactions are collected together into a block. This block is then linked to the last block in the chain, itself becomes the new last block in the chain. This link validates 2 important properties:

- The content of the new block. If the content changes, the link will show it as invalid.
- The previous block. If the previous block is changed, the link will show it as invalid.

Honest generators only build onto a block (by referencing it in blocks they create) if it is the latest block in the longest valid chain. "Length" is calculated as the total combined difficulty of that chain, not number of blocks, though this distinction is only important in the context of a few potential attacks. A chain is valid if all of the blocks and transactions within it are valid, and only if it starts with the genesis block.

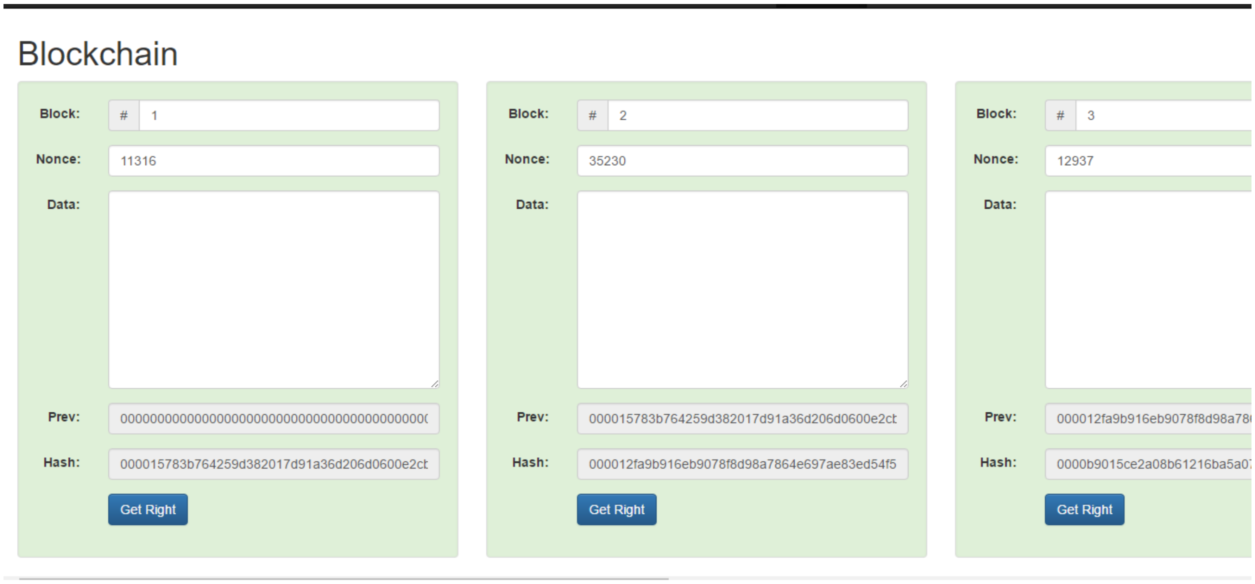
And this is the code to generate blocks:



```
var generateNextBlock = (blockData) => {
    var previousBlock = getLatestBlock();
    var nextIndex = previousBlock.index + 1;
    var nextTimestamp = new Date().getTime() / 1000;
    var nextHash = calculateHash(nextIndex, previousBlock.hash, nextTimestamp, blockData);
    return new Block(nextIndex, previousBlock.hash, nextTimestamp, blockData, nextHash);
};
```

Figure III.6 Coherence of blocks implementation

So with this piece of code we developed for the blockchain:



Blockchain

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000(
Hash: 000015783b764259d382017d91a36d206d0600e2cb

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cb
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a78
Hash: 0000b9015ce2a08b61216ba5a0

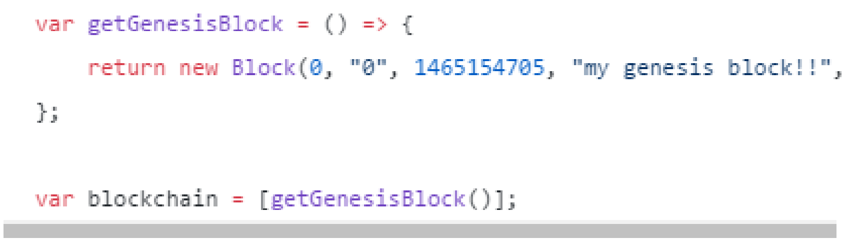
As we see in picture above every block contain the hash of the previous block to get linked each other.

Figure III.7 Coherence of blocks

Step 4=> Storing Blocks:

The blockchain is stored, distributed, on every machine in the Bitcoin network being used to mine Bitcoin.

This network is self-regulating and peer-to-peer. There is majority rule, meaning that if one node on the network no longer agrees with the other nodes (on, say, what the hash of the last block was), it is kicked out of the network and will have to "resync" its data to be in agreement with the network.



```
var getGenesisBlock = () => {
    return new Block(0, "0", 1465154705, "my genesis block!!", "816534932c2b7154836da6afc3676
};

var blockchain = [getGenesisBlock()];
```

Figure III.8 Storing Blocks implementation

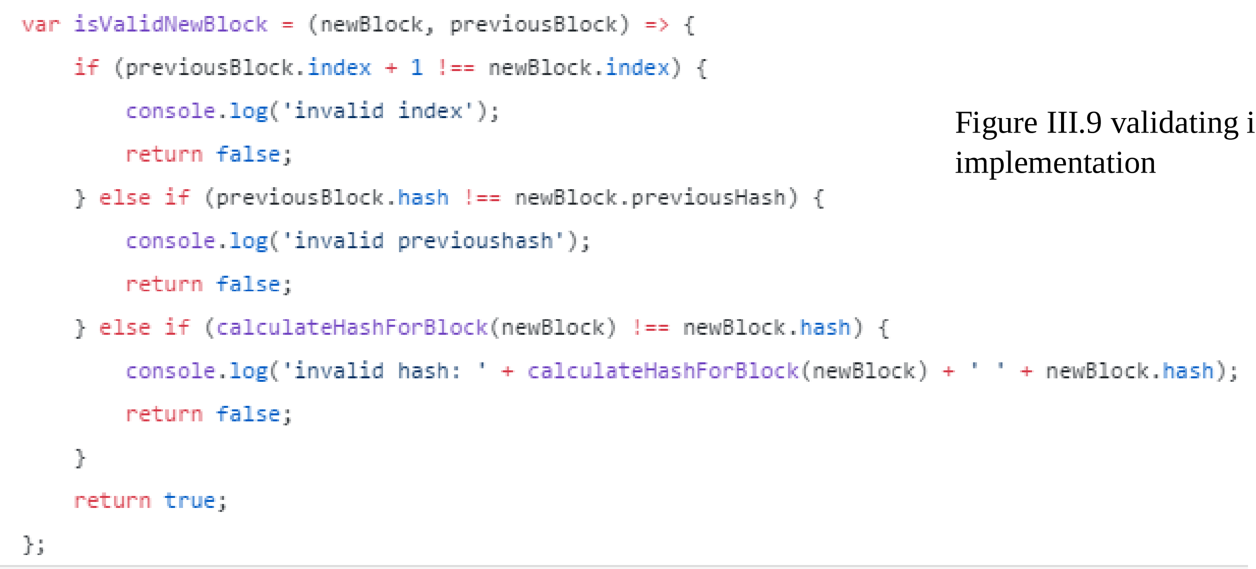
Step 5=> validating integrity:

The blockchain Data Integrity service is data-centric and provides customers with the ability to detect tampering of digital assets and find compromised data. Every data asset can be signed and verified when data is being ported. This is consistent with most regulatory compliance requirements that require data integrity.

Blockchain Data Integrity service provides a chronological record of the time the data was signed, the identity of who signed the data and assurance that the data has not been changed after being signed. This can provide an auditable trail of the chain of custody.

Independent verification of the integrity of data is possible using the media published publication code and the signature to prove the integrity of the data. The lifecycle integrity of data can be monitored by continuously verifying the data in near real time and generating alerts in the event of a failure.

The end of the cycle is that your security partner sends the hash from the blockchain back to you, where it is compared to the newest hash of your data. The whole cycle could take less than a second.

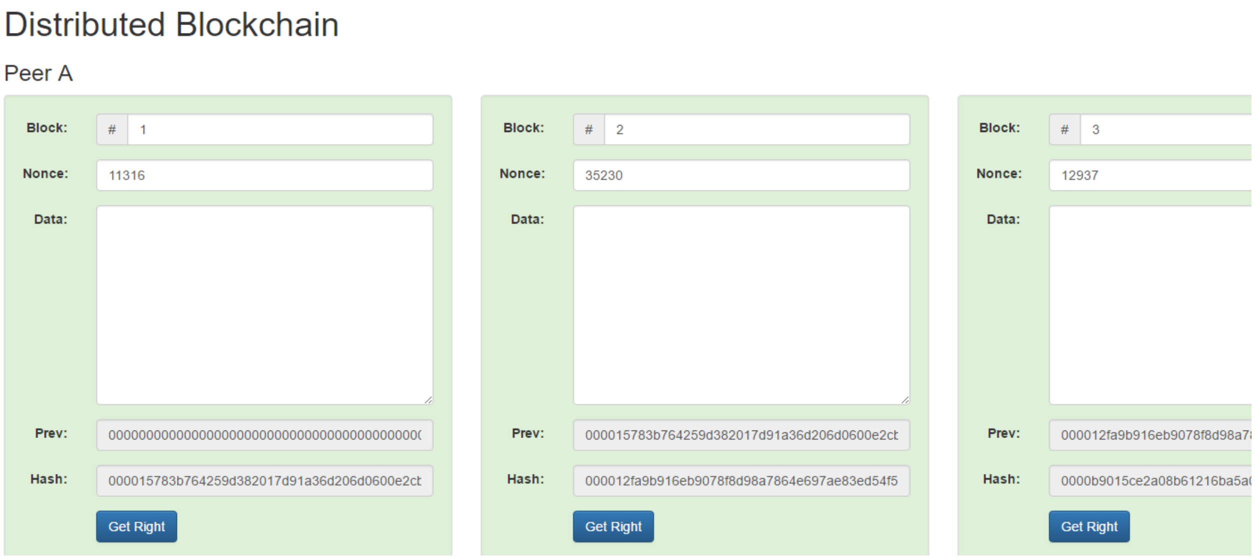


```
var isValidNewBlock = (newBlock, previousBlock) => {
    if (previousBlock.index + 1 !== newBlock.index) {
        console.log('invalid index');
        return false;
    } else if (previousBlock.hash !== newBlock.previousHash) {
        console.log('invalid previoushash');
        return false;
    } else if (calculateHashForBlock(newBlock) !== newBlock.hash) {
        console.log('invalid hash: ' + calculateHashForBlock(newBlock) + ' ' + newBlock.hash);
        return false;
    }
    return true;
};
```

Figure III.9 validating integrity implementation

For example, for blockchain we realize a small application of bitcoin using blockchain technology we used first all the step above to form a blockchain and we made it distributed on 3 peer like the picture below will explain :

Peer A



Distributed Blockchain

Peer A

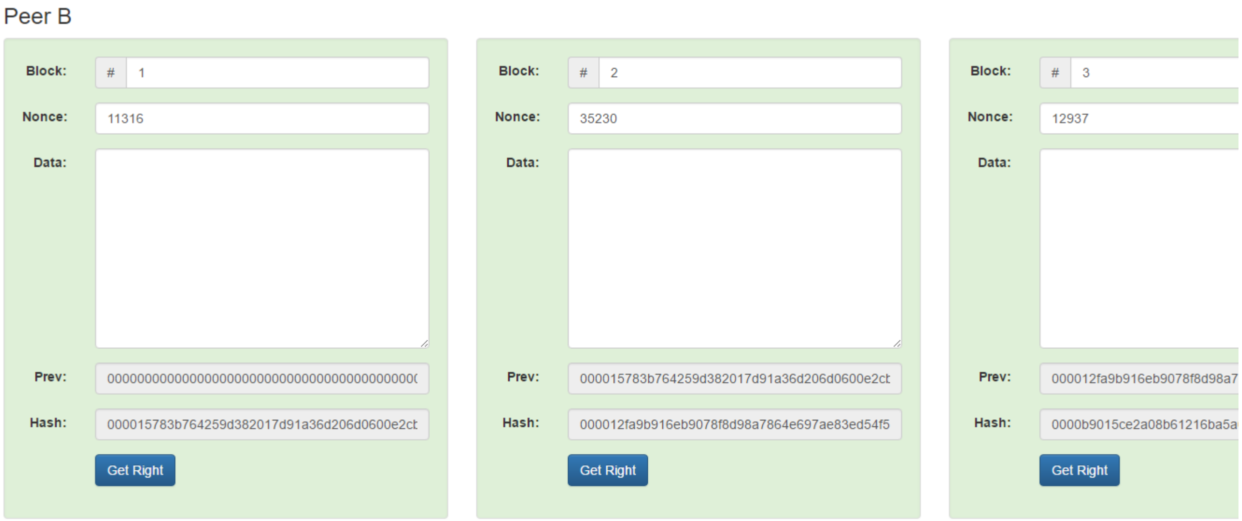
Block: # 1
Nonce: 11316
Data:
Prev: 000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2c

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2c
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7
Hash: 0000b9015ce2a08b61216ba5a

Peer B

Figure III.10 validating integrity view



Peer B

Block: # 1
Nonce: 11316
Data:
Prev: 000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2c

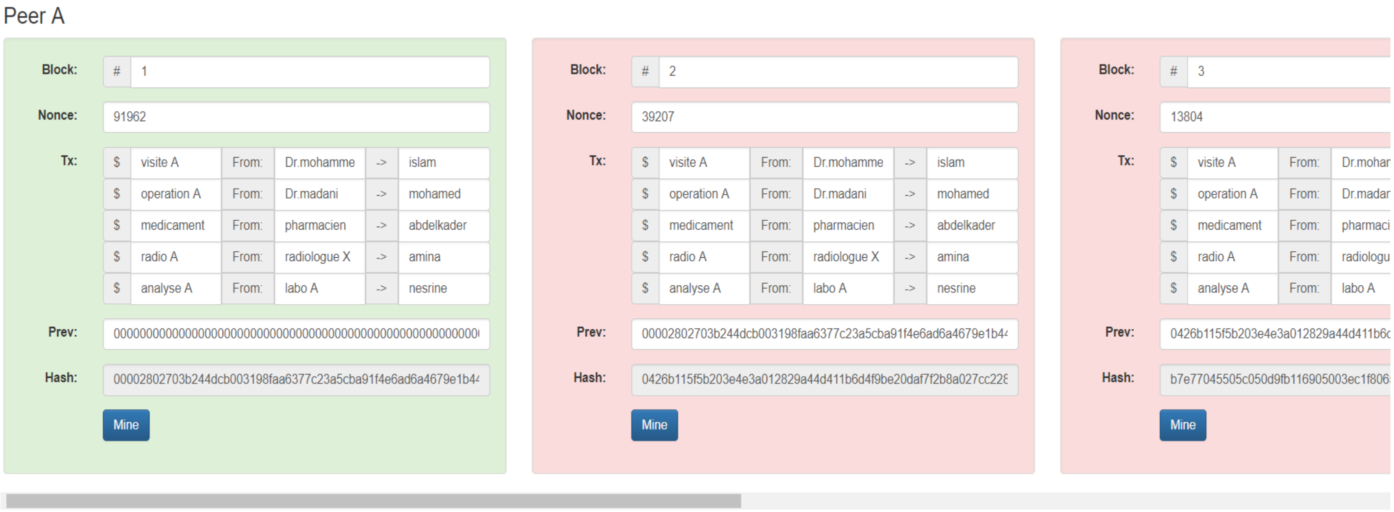
Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2c
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7
Hash: 0000b9015ce2a08b61216ba5a

Simply put, a blockchain is a peer-to-peer networks that timestamps records by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. On the other hand, a distributed ledger is a peer-to-peer network that uses a defined consensus mechanism to prevent modification of an ordered series of time-stamped records. All blockchains are distributed ledgers, but not all distributed ledgers are blockchains.

So the application in bitcoin gives us this form:

Figure III.11 invalidation of integrity view



Peer A

Block:	#	1				
Nonce:	91962					
Tx:	$	visite A	From:	Dr.mohamme	->	islam
	$	operation A	From:	Dr.madani	->	mohamed
	$	medicament	From:	pharmacien	->	abdelkader
	$	radio A	From:	radiologue X	->	amina
	$	analyse A	From:	labo A	->	nesrine
Prev:	0000000000000000000000000000000000000000000000000000000					
Hash:	00002802703b244dcb003198faa6377c23a5cba91f4e6ad6a4679e1b4					

Block:	#	2				
Nonce:	39207					
Tx:	$	visite A	From:	Dr.mohamme	->	islam
	$	operation A	From:	Dr.madani	->	mohamed
	$	medicament	From:	pharmacien	->	abdelkader
	$	radio A	From:	radiologue X	->	amina
	$	analyse A	From:	labo A	->	nesrine
Prev:	00002802703b244dcb003198faa6377c23a5cba91f4e6ad6a4679e1b4					
Hash:	0426b115f5b203e4e3a012829a44d411b6d4f9be20daf7f2b8a027cc22					

Block:	#	3		
Nonce:	13804			
Tx:	$	visite A	From:	Dr.mohar
	$	operation A	From:	Dr.madar
	$	medicament	From:	pharmaci
	$	radio A	From:	radiologu
	$	analyse A	From:	labo A
Prev:	0426b115f5b203e4e3a012829a44d411b6c			
Hash:	b7e77045505c050d9fb116905003ec1f806			

Like we see in the picture above every block forming the blockchain contain some transaction that show the amount, the sender and the receiver and all these transactions are stored in a form of blocks that form also a blockchain w this block chain is distributed.

The blockchain cloud is a thin cloud if compared to a traditional cloud computing infrastructure, therefore it is more ideally suited for running a new breed of thin programs, specifically known as “smart contracts”, and they are business logic that executes on the blockchain’s Virtual Machinery (VM) [21].

Not surprisingly, the “virtual machine” naming borrows from the traditional cloud computing nomenclature, and it is really this virtual network of decentralized computers that are bound together by the commonalities of a given blockchain’s consensus rules, i.e. to execute the logic represented in the software code.

Therefore, the blockchain cloud has a form of micro-value pricing that parallels the traditional cloud computing stack, but via a new layer. It’s not a physical unbundling of the cloud rather, it’s a new layering of cryptography-based transaction validation and state transition recordings on a parallel, but thinner cloud.

But let’s not get carried away with the cloud computing analogy. The blockchain infrastructure resembles a layer of cloud computing infrastructure, but it doesn’t allow us to replace it. Blockchain VM’s may be too expensive if we are to literally compare their functionality to a typical cloud service such as Amazon Web Services or Digital Ocean, but they will be useful for certain decentralized applications. As a side note, we could also see a future where client nodes can talk to each other directly in scenarios where blockchains are too expensive or slow.

There is a challenging part to run applications on this new infrastructure: we need to do some work. That work comes in the form of adhering to a new paradigm of decentralized apps that follows a web3 architecture to run specifically on the blockchain [22].

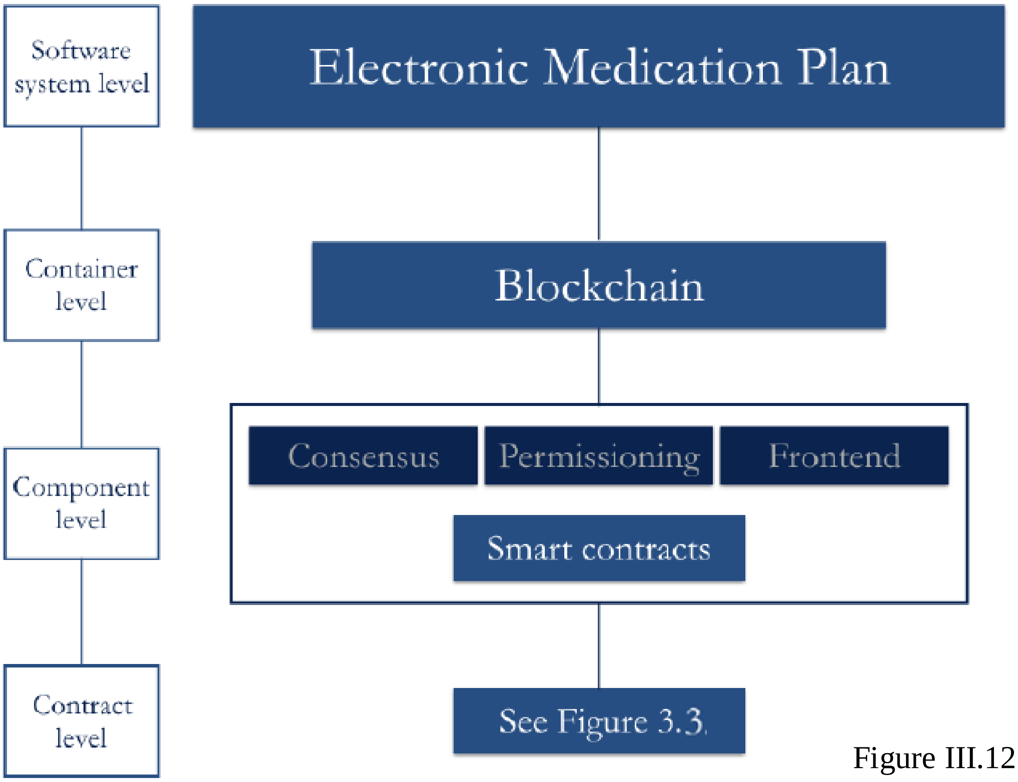


Figure III.12 : infrastructure of blockchain

III.2) New SaaS?

So, it looks like blockchain technology is just like other software technology, but is it going to sit in the realm of Information Technology departments? The answer is Yes and No. Yes, there will be some applications that will require the involvement of IT and large software teams in order to produce some end-user, back-end, intra- or inter-company applications.

But a more disrupting facet is that business users will also be able to run their own smart contracts, P2P apps, and other Dapps on open blockchains without seeking permission from IT, in the same way that SaaS was a Trojan horse that enabled employees to sign-up for services on their own without disturbing the company infrastructures (until it was time to perform some integrations).

This new form of SaaS will be possible because a new infrastructure layer can emerge by being supported on a peer to peer and shared cost basis. And it is very possible that the costs of this new computing infrastructure will be as cheap as Internet access today, on a relative per-user basis. If that's the case, this opens-up the application possibilities even further [22].

The thin cloud represents freedom and flexibility for users and developers. It will allow anyone to create their own business logic for ownership, commerce, contractual law, transaction formats and state transition functions without worrying about setting-up an infrastructure.

We must fully embrace the thin cloud as an outcome of the blockchains' infrastructures, and we must innovate with creative applications that run on it.

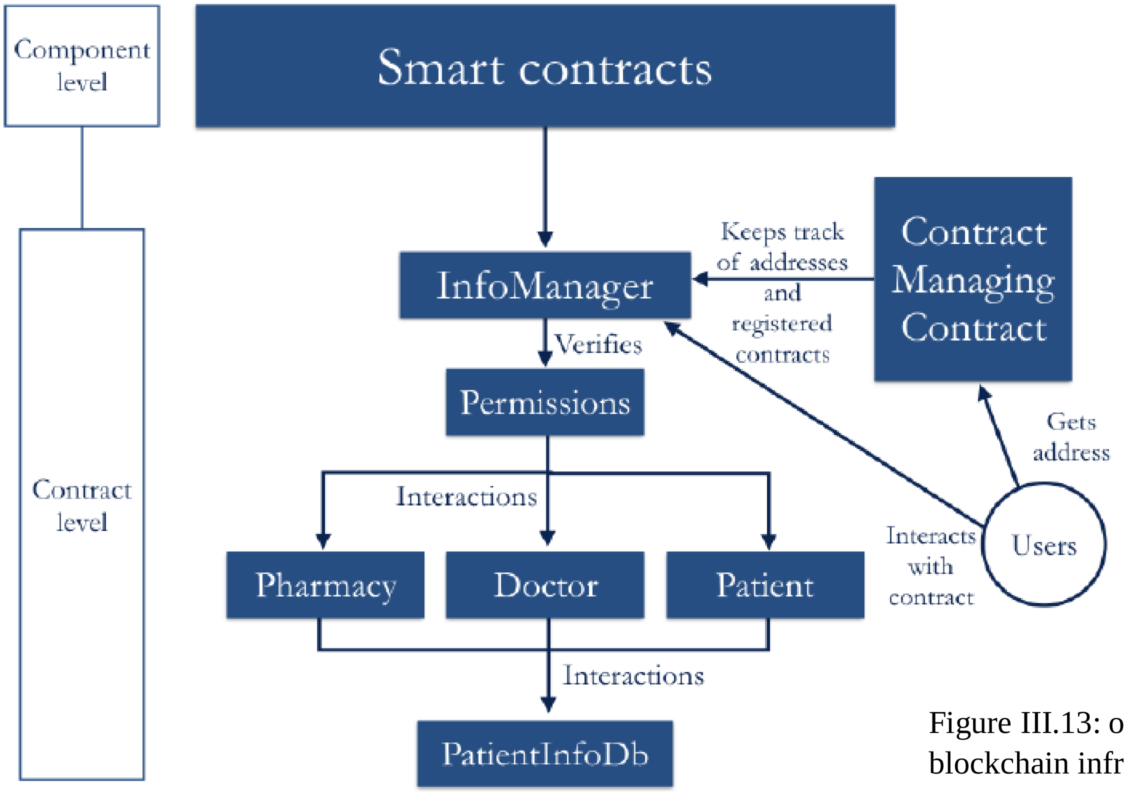


Figure III.13: over view of blockchain infrastructure

III.3) Digital Platforms and Boundary Resources

Digital platforms are shifting the boundaries of industry ecosystems, transforming how value is created and captured, as well as changing job descriptions and the trust relationships between different parties in the economy. Making predetermined boundary resources available to anyone willing to participate is a key strategy in platform innovation management.

The term "digital platforms" refers to IT systems via which different parties can do business that adds value to the whole ecosystem. The parties may be users or suppliers of the platform or inter-organizational interest groups such as application developers or advertisers. Typically the different parties create, provide and maintain complementary products and services to the various distribution channels and markets, while adhering to the jointly agreed upon rules and user experiences. [23] The platforms commit and attract different parties with the financial benefits generated by the network. The effect of digital platforms on agreements and technological compatibility is best showcased by boundary resources. Boundary resources refer to contractual and other co-operative regulations as well as software tools and interfaces which act as an open interface between the digital platform company and any other third party. It is characteristic for these digital boundary resources to be openly available and free (or almost free) to any third party on the internet, which allows a heterogeneous population of users to participate in the development and maintenance of various commodities in different platforms and system architectures [24].

Boundary resources can be understood as the opposite of barriers to entry. The use of boundary resources is aimed at lowering the often large development and commercialization costs related to new innovations, therefore helping to create wider network effects than seen previously [23].

Digital platform owners mostly benefit from sharing boundary resources with third parties by capitalizing on split revenue business models

III.4) Blockchain Technology as an Enabler of Decentralized Platforms

One way to perceive blockchain technology is to look at it as a potential enabler for next generation digital platforms and their boundary resources, e.g. smart contracts. Typically, digital platforms have been understood as company-specific internal platforms or platforms controlled by a certain central operator, but not as decentralized systems maintained together by a multitude of equal parties Then again, smart contracts can be utilized in all the three different situations [25].

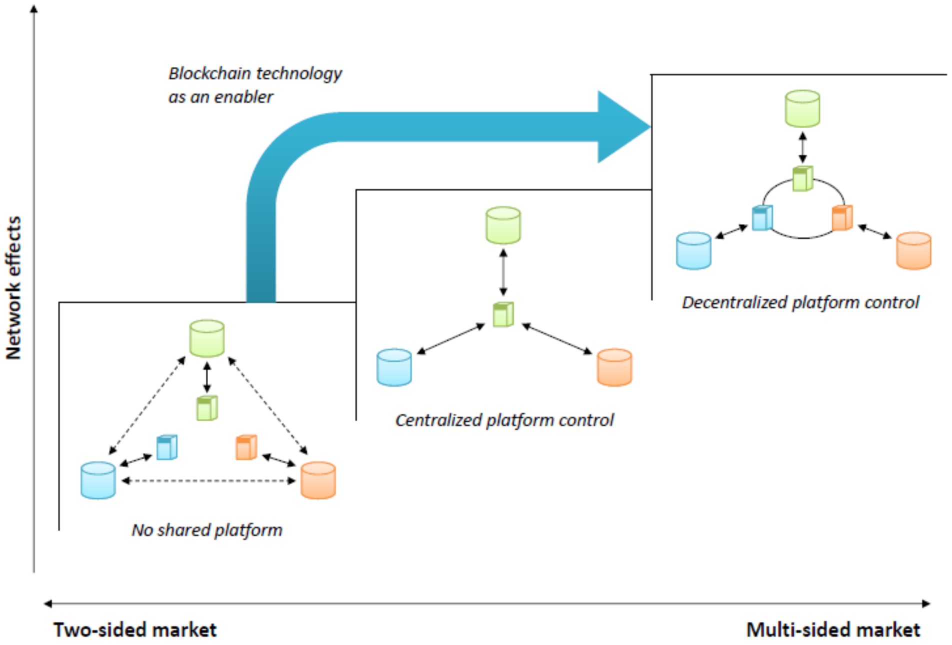


Figure III.14: from centralized platform control towards a decentralized consensus [25]

III.5) Contracts vs Smart Contracts?

- Contract Law and the Interpretation of Smart Contracts

Contracts are a key legal instrument for private operators as they execute changes in their legal relations or try to prepare for future turns of events [3]. Contracts also enable organized collaborative activity and are often used to carry out economic activity. The definition of the term "contract" contains a number of different meanings. First of all, the term may refer to the conclusion of the agreement itself, therefore describing the parties' commitment to the contract. Secondly, it may refer to the contents of the agreement, therefore determining the parties' rights and obligations in relation to one another. Thirdly, it may refer to the actual document in which the terms of the contract have been specified. Contract law is traditionally non-mandatory, in other words the parties can disregard certain rules of presumption by implementing their own terms. The principle of freedom of contract is the premise from which Finnish contract law starts. For a number of reasons, however, freedom of contract is restricted by certain mandatory rules regarding the content of agreements.

The main principle is nonetheless that parties can exercise full freedom in deciding whether to enter into a contract, with whom the contract will be concluded, and how and with what terms the contract is to be concluded. The right to decide on the dissolution of a contract has also been considered an important, yet separate, part of freedom of contract. In addition to the principle of freedom of contract, the legal system also acknowledges the principle of pacta sunt servanda [25]. That is, agreements must be kept in Various sanction mechanisms also make it necessary to abide by the contracts one has entered into, since the other party has the opportunity to claim damages or enforce the contract by help of the authorities. Based on case law alone we are able to conclude that the principle of pacta sunt servanda is a prevailing reality in our legal system without which society would not function properly. In this publication, we will address contracts as individual agreements with the main purpose of organizing economic legal relations and which have been concluded between rational and equal private parties. Due to practical reasons, our presentation of contract law will be limited to a rather general level, focusing on the mechanisms leading to the conclusion of a contract. Our goal of this publication is to analyze through doctrinal research and as straightforwardly as possible those aspects of contract law which are relevant to the interpretation of smart contracts. This perspective leaves out several significant legal themes which we are not able to explore in this publication. Since there has been little research on smart contracts, this type of approach is necessary in order to define them and assess them in a legal context [27].

- Smart Contracts

A fully established definition of smart contracts has yet to be formed, and the official legal status of smart contracts is not perfectly clear. In this publication, smart contracts are defined as digital programs, based on the blockchain consensus architecture, which will self-execute when the terms of the agreement are met, and due to their decentralized structure are also self-enforcing and tamper-proof. As this article focuses on the utilization of computer programming in order to create contracts, the definition of smart contracts is restricted to programs which have similar qualities to contracts and are also meant to replace, or add to, traditional contracts [3].

Diverging from contracts concluded in form of action, speech or writing, a smart contract is characteristically a computer program built on code. Some smart contracts, however, contain similar logic and characteristics that can be likened to those of conventional contracts, at least from a theoretical viewpoint. In addition to traditional contract terms and conditions listed in the agreement, smart contracts are capable of actions such as collecting data from outside resources and processing it according to the terms specified in the contract, as well as adopting concrete solutions based on the results of this procedure. There is indeed reason to note that the term "smart contracts" is also commonly used in connection with many other programs in the blockchain and not only those resembling a formal agreement [27].

According to Nick Szabo, creator of the concept behind smart contracts, the most primitive type of smart contract is the vending machine in which transactions are based on simple automation.

The vending machine, with its automated mechanisms, accepts the coins, returns the change and finally hands over the sold item. The vending machine therefore completes the transaction on its own when the necessary prerequisites are met, that is, a sufficient amount of money has been handed over to the machine. Anyone in possession of a sufficient amount of coins and with the desire to purchase an item is capable of becoming a contracting party in this type of transaction. Additionally, since the items for sale are situated within the vending machine, it is capable of protecting the contract from unauthorized changes [28].

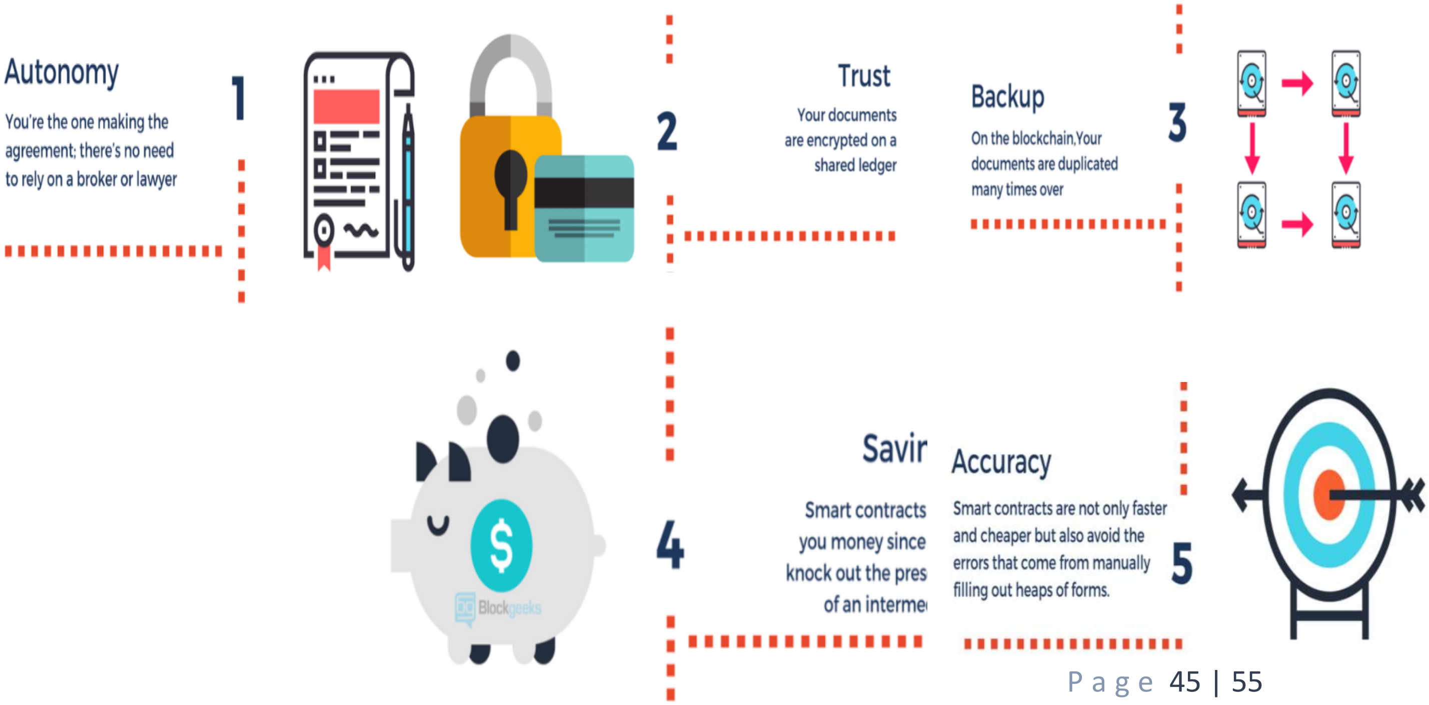
Smart contracts further develop the concept of the vending machine, as they can be applied to all digitally manageable assets of value. Szabo defines smart contracts as computerized transaction protocols that execute the terms of a contract. The purpose of a smart contract is to execute the general terms of a contract and limit the amount of exceptions and other errors.

This simultaneously removes the need for third parties responsible for checking the accuracy of the process. Szabo's theory states that smart contracts diminish the number of frauds and other malicious phenomena while lowering transaction costs as contract terms are automatically implemented.

The blockchain that the cryptocurrency Bitcoin is based on was for long the only functioning large-scale blockchain system. Due to technical restrictions caused by the programming language, the decentralized performance of applications other than cryptocurrency had its challenges in the Bitcoin blockchain. In 2013, programmer Vitalik Buterin published an article describing a new type of blockchain-based platform called Ethereum. Ethereum was launched in 2015. As a significant advancement from Bitcoin, Ethereum finally offered a real opportunity for the decentralized performance of programs within the blockchain. These programs, which according to Buterin are cryptographic "boxes" containing value that only unlock where certain conditions are met, can also be called smart contracts66. Buterin later presented a definition in which smart contracts are described as automated mechanisms with at least two (contracting) parties. In addition, one or more of the parties must provide an asset or assets to be managed by the smart contract. After this, the assets are re-distributed between the parties according to the plan presented in the contract, so that the execution of the transaction is based on data that was not yet available when the contract itself was concluded [29].

In a smart contract based on blockchain technology the terms of the contract are thus formulated in programming language [3], after which the smart contract is usually transferred to a blockchain in which it self-executes automatically without the assistance of the contracting parties when pre-defined conditions are met. In addition, it is capable of preventing unauthorized changes of its internal logic. A party cannot therefore intentionally prevent the execution of a smart contract or unlawfully alter its content. from a more technical point of view, smart contracts are autonomous programs situated in a certain address in the blockchain, which can be rerun infinitely and can also be programmed to contain a wide array of business-model logics. Once the event specified in the contract takes place and the transaction containing data arrives to the address of the smart contract, the distributed virtual machine of the blockchain executes the programming code [3].

Our traditional understanding of contracts rarely covers contract-like programs. If a traditional contract were to be created in code, this would require the contract to be arranged and presented as a process depicting interdependency: “if X, then Y, otherwise Z”. Since the way in which traditional contracts are worded can often result in ambiguity, this new use of formulas can in at least some cases reduce the need for interpretation. This kind of development can at best lead to significant reductions in the costs caused by drafting contracts and overseeing their execution, Smart contracts are thus automatic programs built on code which have been placed in a blockchain to perform certain processes. They begin to show contract-like characteristics once digital (or other) assets have been transferred to them for management and are transferred again or redistributed once certain conditions are met. In this phase, another party may join the smart contract and can initiate automatic execution by meeting certain preconditions. This could mean an action such as transferring a predetermined sum of cryptocurrency to the smart contract. It must be noted, however, that the aforementioned course of events is only a presumption, and the smart contract can also remain at a stage where it functions purely as a re-router built to transfer data or, for instance, the contents of one crypto-wallet to another [3].


Autonomy
You're the one making the agreement; there's no need to rely on a broker or lawyer
1
2
Trust
Your documents are encrypted on a shared ledger
Backup
On the blockchain,Your documents are duplicated many times over
3
Blockgeeks
4
Savir
Smart contracts you money since knock out the pres of an interme
Accuracy
Smart contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms.
5

The legal status of such smart contracts can indeed be questioned with good reason, at least from the perspective of contract law. As a term, “smart contracts” can at times be misleading, for there are several types of smart contracts in existence. From a contract law perspective, therefore, their interpretation would seem to require case-by-case evaluation.

III.6) Blockchain Model for Health Care

Any blockchain for health care would need to be public and would also need to include technological solutions for three key elements: scalability, access security and data privacy.

a. **Scalability**

A distributed blockchain that contains health records, documents or images would have data storage implications and data throughput limitations. If modeled after the Bitcoin blockchain, every member of the distributed network of the health care blockchain would have a copy of every health record for every individual in the U.S. and this would not be practical from a data storage perspective. Because health data is dynamic and expansive, replicating all health records to every member in the network would be bandwidth intensive, wasteful on network resources and pose data throughput concerns. For health care to realize benefits from blockchain, the blockchain would need to function as an access-control manager for health records and data [30].

The information contained in our proposed health blockchain would be an index, a list of all the user’s health records and health data. The index is similar to a card catalog in a library. The card catalog contains metadata about the book and a location where the book can be found. The health blockchain would work the same way. Transactions in the blocks would contain a user’s unique identifier, an encrypted linked to the health record and a timestamp for when the transaction was created. To improve data access efficiency, the transaction would contain the type of data contained in the health record and any other metadata that would facilitate frequently used queries (the metadata could be added as tags). The health blockchain would contain a complete indexed history of all medical data, including formal medical records as well as health data from mobile applications and wearable sensors, and would follow an individual user throughout his life. All medical data would be stored off blockchain in a data repository called a data lake. Data lakes are highly scalable and can store a wide variety of data, from images to documents to keyvalue stores. Data lakes would be valuable tools for health research and would be used for a variety of analysis including mining for factors that impact outcomes, determining optimal treatment options based on genetic markers and identifying elements that influence preventative medicine. Data lakes support interactive queries, text mining, text analytics and machine learning. All information stored in the data lake would be encrypted and digitally signed to ensure privacy and authenticity of the information [29].

When a health care provider creates a medical record (prescription, lab test, pathology result, MRI) a digital signature would be created to verify authenticity of the document or image. The health data would be encrypted and sent to the data lake for storage. Every time information is saved to the data lake a pointer to the health record is registered in the blockchain along with the user's unique identifier. The patient is notified that health data was added to his blockchain. In the same fashion a patient would be able to add health data with digital signatures and encryption from mobile applications and wearable sensors [29].

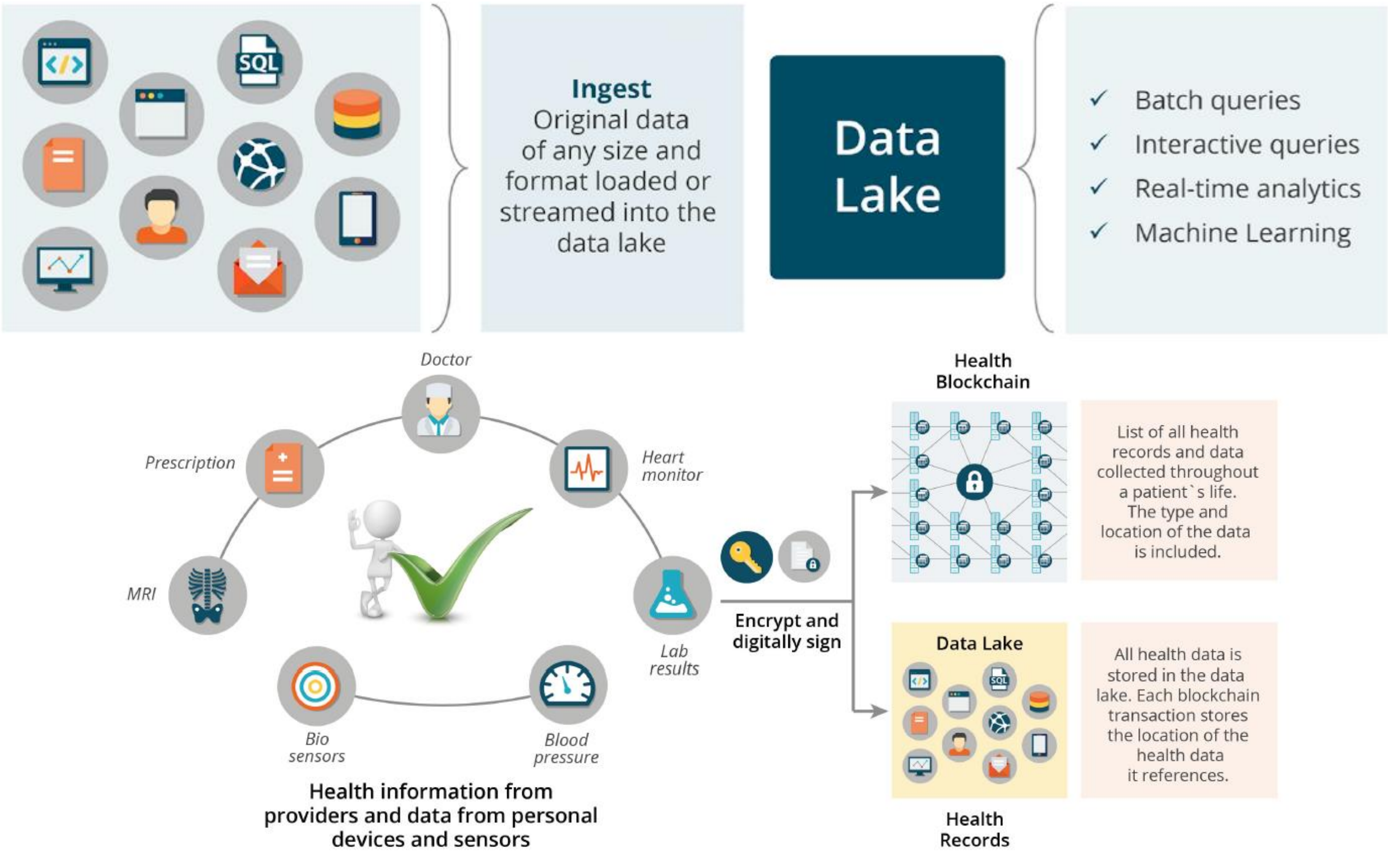

SQL
Ingest
Original data of any size and format loaded or streamed into the data lake
Data Lake
✓ Batch queries
✓ Interactive queries
✓ Real-time analytics
✓ Machine Learning
Doctor
Prescription
Heart monitor
MRI
Lab results
Bio sensors
Blood pressure
Health information from providers and data from personal devices and sensors
Encrypt and digitally sign
Health Blockchain
List of all health records and data collected throughout a patient`s life. The type and location of the data is included.
Data Lake
All health data is stored in the data lake. Each blockchain transaction stores the location of the health data it references.
Health Records

Figure III.15 functional architecture

b. Access Security and Data Privacy

The user would have full access to his data and control over how his data would be shared [30]. The user would assign a set of access permissions and designate who can query and write data to his blockchain. A mobile dashboard application would allow the user to see who has permission to access his blockchain. The user would also be able to view an audit log of who accessed his blockchain, including when and what data was accessed. The same dashboard would allow the user to give and revoke access permissions to any individual who has a unique identifier. Access control permissions would be flexible and would handle more than “all-or-nothing” permissions. The user would setup specific, detailed transactions about who has access, the allotted time frame for access and the particular types of data that can be accessed. At any given time the user may alter the set of permissions. Access control policies would also be securely stored on a blockchain and only the user would be allowed to change them. This provides an environment of transparency and allows the user to make all decisions about what data is collected and how the data can be shared. After a health care provider is granted access to a user’s health information, he queries the blockchain for the user’s data and utilizes the digital signature to authenticate the data. The health care provider could utilize a customized best-of-breed application to analyze the health data [31].

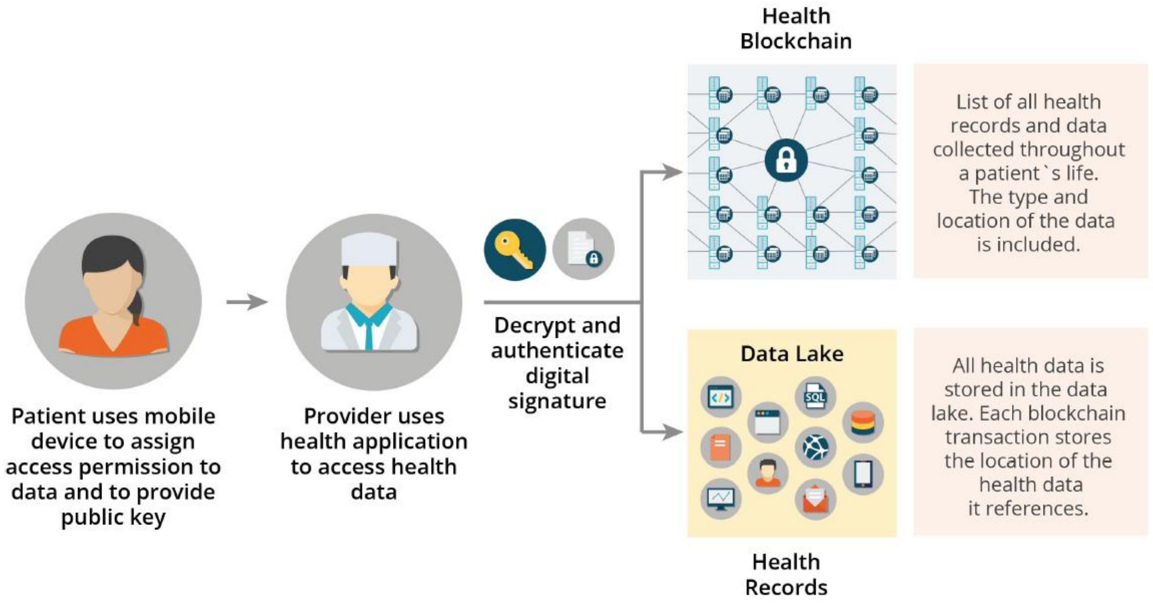

Health Blockchain
List of all health records and data collected throughout a patient`s life. The type and location of the data is included.
Patient uses mobile device to assign access permission to data and to provide public key
Provider uses health application to access health data
Decrypt and authenticate digital signature
Data Lake
All health data is stored in the data lake. Each blockchain transaction stores the location of the health data it references.
SQL
Health Records

Figure III.16 transaction architecture

Identity authentication would follow the best practices established by financial institutions and regulators. Ideally, biometric identity systems would be utilized as they offer enhanced security over password and token (smartcard) based methods for identity authentication. Given this model, the user has a singular control over his data and the power to grant access to specific health care providers and/or health care entities for communication and collaboration in disease treatment and prevention. The decentralized nature of the blockchain combined with digitally signed transactions ensure that an adversary cannot pose as the user or corrupt the network as that would imply the adversary forged a digital signature or gained control over the majority of the network's resources. Similarly, an adversary would not be able to learn anything from the shared public ledger as only hashed pointers and encrypted information would be contained within the transactions [32].

III.7) Technical Advantages of a Health Care Blockchain

Blockchain technology offers many advantages for health care IT[34]. Blockchain is based on opensource software, commodity hardware, and Open API's. These components facilitate faster and easier interoperability between systems and can efficiently scale to handle larger volumes of data and more blockchain users. The architecture has built-in fault tolerance and disaster recovery, and the data encryption and cryptography technologies are widely used and accepted as industry standards. The health blockchain would be developed as open-source software. Open-source software is peer-reviewed software developed by skillful experts. It is reliable and robust under fast changing conditions that cannot be matched by closed, proprietary software. Open-source solutions also drive innovations in the applications market. Health providers and individuals would benefit from the wide range of application choices and could select options that matched their specific requirements and needs. Blockchain would run on widely used and reliable commodity hardware. Commodity hardware provides the greatest amount of useful computation at low cost. The hardware is based on open standards and manufactured by multiple vendors. It is the most cost effective and efficient architecture for health and genomic research. Excess blockchain hardware capacity could be shared with health researchers and facilitate faster discovery of new drugs and treatments [35].

Blockchain technology also addresses the interoperability challenges within the health IT ecosystem. Health IT systems would use Open API's to integrate and exchange data with the health blockchain. Open API's are based on industry best practices. They are easy to work with and would eliminate the need for development of complex point-to-point data integrations between the different systems. Blockchain would allow patients, the health care community and researchers to access one shared data source to obtain timely, accurate and comprehensive patient health data.

Blockchain data structures combined with data lakes can support a wide variety of health data sources including data from patients' mobile applications, wearable sensors, EMR's, documents and images. The data structures are flexible, extendable and would be able to accommodate the unforeseen data that will be available in the future. Data from cheap mobile devices and wearable sensors is growing at an exponential rate. Distributed architectures based on commodity hardware provide cost efficient high scalability [36].

As more health data is added to the blockchain cost efficient commodity hardware can be easily added to handle the increased load. Another advantage of blockchains distributed architecture is built-in fault tolerance and disaster recovery. Data is distributed across many servers in many different locations. There is no single point of failure and it is unlikely a disaster would impact all locations at the same time. Blockchain works with standard algorithms and protocols for cryptography and data encryption. These technologies have been heavily analyzed and accepted as secure and are widely used across all industries and many government agencies [37].

III.8) Health Care Advantages of Health Care Blockchain

Blockchain technology offers many advantages to medical researchers, health care providers, care givers and individuals. Creation of a single storage location for all health data, tracking personalized data in real-time and the security to set data access permissions at a granular level would serve research as well as personalized medicine.

Health researchers require broad and comprehensive data sets in order to advance the understanding of disease accelerate biomedical discovery, fast track the development of drugs and design customized individual treatment plans based on patient genetics, lifecycle and environment. The shared data environment provided by Blockchain would deliver a broad diverse data set by including patients from different ethnic and socio-economic backgrounds and from various geographical environments. As blockchain collects health data across a patient's lifetime, it offers data ideal for longitudinal studies [36].

A health care blockchain would expand the acquisition of health data to include data from populations of people who are currently under-served by the medical community or who do not typically participate in research. The shared data environment provided by Blockchain makes it easier to engage "hard-to-reach" populations and develop results more representative of the general public [37].

Blockchain data structures would work well for gathering data from wearable sensors and mobile applications and, thus, would contribute significant information on the risks versus the benefits of treatments as well as patient reported outcomes. Furthermore, combining health data from mobile applications and wearable sensors with data from traditional EMR's and genomics will offer medical researchers increased capabilities to classify individuals into subpopulations that respond well to a specific treatment or who are more susceptible to a particular disease. Daily, personalized health data will likely engage a patient more in his own health care and improve patient compliance. Moreover, the ability for physicians to obtain more frequent data (i.e., daily blood pressures or blood sugar levels versus only when a patient appears for an appointment) would improve individualized care with specialized treatment plans based on outcomes/treatment efficacy [38].

Blockchain would ensure continuous availability and access to real-time data. Real-time access to data would improve clinical care coordination and improve clinical care in emergency medical situations. Real-time data would also allow researchers and public health resources to rapidly detect, isolate and drive change for environmental conditions that impact public health. For example, epidemics could be detected earlier and contained [38].

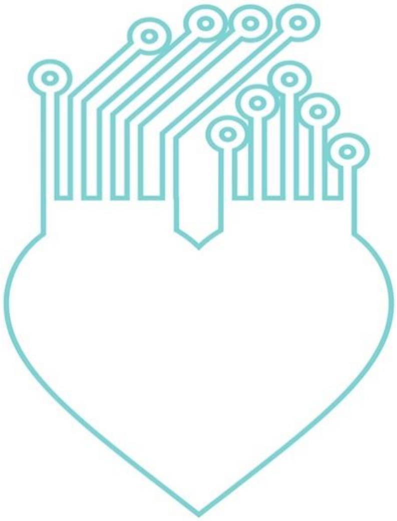
The real-time availability of mobile application and wearable sensor data from the blockchain would facilitate continuous, 24 hour-a-day monitoring of high risk patients and drive the innovation of "smart" applications that would notify care givers and health providers if a patient reached a critical threshold for action. Care teams could reach out to the patient and coordinate treatment options for early intervention [39].

A health care blockchain would likely promote the development of a new breed of "smart" applications for health providers that would mean the latest medical research and develop personalized treatment paths. The health provider and patient would have access to the same information and would be able to engage in a collaborative, educated discussion about the best-case treatment options based on research rather than intuition [39].

Conclusion

Blockchain technology has huge potential to disrupt a wide range of industries, ranging from data management, security and healthcare as we introduced in this thesis, but Medical block chain is still an early prototype, not ready for wide scale deployment any time soon. But government health technologists see its promise. Because it provides ways to safely share data from EHRs, clinical trials, genetic sequencing, and even mobile wearables using the blockchain approach. The technology is still in its infancy when it comes to health care applications, but in a recent poll of health care executives, those polls intend to implement some sort of blockchain solutions by the end of this year.

The purpose of this Master's thesis is to explore blockchain technology and smart contracts as a way of building privacy-sensitive applications. The main focus is on a medication plan containing prescriptions, built on a blockchain system of smart contracts. This is an example use case, but the results can be transferred to other ones where sensitive data is being shared and a proof of validity or authentication is needed. First the problem is presented, why medication plans are in need of digitization and why blockchain technology is a fitting technology for implementing such an application. Then blockchain technology is explained, since it is a very new and relatively unfamiliar IT construct. Thereafter, a design is proposed for solving the problem. A system of smart contracts was built to prove how such an application can be built and suggested guidelines for how a blockchain system should be designed to fulfil the requirements that were defined. Finally, a discussion is held regarding the applicability of different blockchain designs to the problem of privacy-handling applications.



References

Books:

[1]. Deutsch, M. (1973). *The resolution of conflict: Constructive and destructive processes*: Yale University Press.

[2]. Dwivedi, Y. K. (2009). *Handbook of research on contemporary theoretical models in information systems*: IGI Global.

[3]. Walport, M. (2016). Distributed Ledger Technology: Beyond Blockchain. *UK Government Office for Science, Tech. Rep, 19*.

[4]. Williamson, O. E. (1975). *Markets and hierarchies : analysis and antitrust implications : a study in the economics of internal organization*. New York: The Free Press.

[5]. Williamson, O. E. (1998). Transaction cost economics: How it works; where it is headed. *Economist, 146*(1), 23-58.

[6]. Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. *Available at SSRN 2580664*.

[7]. Book : Blockchain: Blueprint for a New Economy

[8]. Allen, D. W. (2017). Discovering and developing the blockchain cryptoeconomy. *Available at SSRN 2815255.*

[9]. Baran, P. (1964). On distributed communications networks. *IEEE transactions on Communications Systems, 12*(1), 1-9.

[10]. Cearley, D. W., Walker, M. J., & Burke, B. (2016). Top 10 Strategic Technology Trends for 2017. Stamford: Gartner.

[11]. Chuen, D. L. K. (2015). *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. London: Academic Press. CIO. (2016).

Web documents:

[12]. Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System, http://www.bitcoin.org Retrieved from (01-04-2018).

[13]. 20. Kelly J., REUTERS, http://uk.reuters.com/article/uk-banking-tradingblockchainidUKKCN0UY28W Retrieved from (02-06-2018).

[14]. Blockchain and smart coontracts (international conference - Italy)

[15]. CIO [Security]. (2016). Is blockchain good for security? Retrieved from (01-06-2018): http://www.cio.com/article/3050995/security/is-the-blockchain-good-for-security.html

[16]. Cognizant. (2016). Blockchain in Banking: A Measured Approach. Retrieved from (01-02-2018): https://www.cognizant.com/whitepapers/Blockchain-in-Banking-A-Measured-Approachcodex1809.pdf

[17]. Coindesk. (2016). Understanding The DAO Attack. Retrieved from (01-02-2018): http://www.coindesk.com/understanding-dao-hack-journalists/

[18]. Coinmarketcap. (2016). Crypto-Currency Market Capitalizations. Retrieved from (15-03-2018): https://coinmarketcap.com/

[19]. Coinmarketcap. (2017). ZCash Charts. Retrieved from (01-02-2018): http://coinmarketcap.com/currencies/zcash/

[20]. Deloitte [Banking]. (2016). Blockchain in Banking. Retrieved from (01-02-2018): https://www2.deloitte.com/uk/en/pages/innovation/articles/blockchain.html

[21]. Deloitte [Insurance]. (2016). Blockchain in Insurance. Retrieved from (01-02-2018): https://www2.deloitte.com/uk/en/pages/innovation/articles/blockchain.html

[22]. Deloitte [Main]. (2016). Blockchain: Enigma Paradox Opportunity. Retrieved from (01-02-2018): https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-ukblockchain-full-report.pdf

[23]. Deloitte [Public]. (2016). Blockchain in Public sector. Retrieved from (01-09-2016): https://www2.deloitte.com/uk/en/pages/innovation/articles/blockchain.html

[24]. Forbes [LessonsEth]. (2016). A Painful Lesson For The Ethereum Community. Retrieved from (01-02-2018): http://www.forbes.com/sites/francescoppola/2016/07/21/a-painful-lesson-for-theethereum-community/print/

[25]. rauenfelder, M. (2016). Bitcoin is the Sewer Rat of Currencies. Retrieved from (05-02-2018): https://medium.com/institute-for-the-future/bitcoin-is-the-sewer-rat-of-curranciesb89819cdf036

[26]. ZDNet. (2016). Let's quit the magic blockchain talk. Retrieved from (23-05-2018): http://www.zdnet.com/article/lets-quit-the-blockchain-magic-talk

[27]. Conférence Big Bang Blockchain (France)

[28]. https://www.block-md.com/

[29]. https://www.ibm.com/blogs/blockchain/category/blockchain-in-healthcare/

[30]. Actors. (n.d.). Oxford English dictionary online. Retrieved from (10-05-2018): https://en.oxforddictionaries.com/definition/actors

[31]. AD. (2016). Blockchain gaat de wereld veranderen. Retrieved from (22-05-2018): http://www.ad.nl/nieuws/blockchain-gaat-de-wereld-veranderen~a4697f98/

[32]. Berkeley. (2015). BlockChain Technology:Beyond Bitcoin. Retrieved from (01-02-2018): scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

[33]. BitFury Group. (2015). Public versus Private Blockchains Part 1: Permissioned Blockchains [Whitepaper] Retrieved from (12-03-2018): http://bitfury.com/content/5-white-papersresearch/public-vs-private-pt1-1.pdf

[34]. BitNation. (2016). Bitnation Whitepaper. Retrieved from (07-02-2018): https://docs.google.com/document/d/1ZiIZrmI79HPNbfJ1AXwcgoe8TKMoUMatDf7YfO5LZw/ edit

[35]. Ascribe. (2015). Towards An Ownership Layer for the Internet. Retrieved from (01-09-2016): https://bravenewcoin.com/assets/Whitepapers/ascribe-whitepaper-20150624.pdf

[36]. BlockchainHealth. (2016). Blockchainhealth. Retrieved from (21-04-2018): https://blockchainhealth.co/

[37]. Blockchains: Hype or Reality. Retrieved from (17-03-2018): http://www.cio.com/article/3058266/security/blockchain-technology-hype-or-reality.html

[38]. Blockverify. (2016). Blockverify. Retrieved from (01-09-2016): http://blockverify.io/

[39]. Buterin, V. (2013). A Next-Generation Smart Contract and Decentralized Application Platform [White paper]. Retrieved from (01-04-2018): https://github.com/ethereum/wiki/wiki/White-Paper

[40]. A full liste of the referances you will find it here : https://mega.nz/#!dM8lmKIC!MpFxp2kcaYMjY9wAajl8ECMNUS5e6rJVJfI768z7kCM