“We must recognize internet access as a basic right, and we must work to make sure all young people can connect to a web that gives them the power to shape their world.”

— Tim Berners-Lee

PROVISIONAL SOFTWARE PATENT No.US63/294,483
Licence Granted: 05 January 2022

INVENTION TITLE: Blockchain and Distributed Ledger Technology software, Web3, Str.Domain ecosystem, creating a new web platform with different protocols than www, encrypted and decentralised.

The ecosystem on which Sourceless is based on, will not permit the execution of any malware or computer viruses; based on blockchain characteristics proof, blockchain identity will not permit any type of bad intentions on the Internet, and the digital identity will be white labeled by KYC and AML and will not permit identity theft, thus the information will be protected by blockchain and DLT, Peer-2-Peer in networking with 256-bit encryption from Web 2.0 to Web 3.0;

If web or www allows the existence and execution of malware, expensive hosting or too many resources are running without a purpose, the hosting will be distributed in the whole network, improving hosting armament and carbon reduction by almost 40%; We are having a 90% hosting use and also a bulletproof security web, since everything is public and identity stays proved for all users in the ecosystem. ABSTRACT Blockchain and Distributed Ledger Technology software, Web3, Str.Domain ecosystem, creating a new web platform with different protocols than www, encrypted and decentralised is disclosed.

We are having a 90% hosting use, we are having a bulletproof security web, since everything it's public and identity proved for all users in the ecosystem.

ABSTRACT

Blockchain and Distributed Ledger Technology software, Web3, Str.Domain ecosystem, creating a new web platform with different protocols than www, encrypted and decentralised is disclosed. We are having a 90% hosting use, we are having a bulletproof security web, since everything it's public and identity proved for all users in the ecosystem.

SourceLess Blockchain ISO 20022

ISO 20022 is a globally accepted messaging standardization approach (methodology, process, repository) to be used by all financial standards initiatives as a common platform for the development of messages. It was introduced in 2005 by the International Organization for Standardization to help financial institutions streamline their communication infrastructure by using the same language for all financial communications.

Today, ISO 20022 is used by payment systems in over 70 countries. It is estimated to be the defacto standard for high-value payment systems of all reserve currencies, supporting 80% of global volumes and 87% of value of all global transitions in the coming years. This common language is now an emerging global and open standard for payments data, and is the expected future standard of fintech innovation and competition. ISO 20022 utilizes richer, higher quality data than other standards, driving improved payment outcomes that can easily adapt and are not controlled by a single interest. According to SWIFT, the benefits of ISO 20022 specifically include:

- Better data - ISO 20022 enables richer, better structured, and more granular data for payments messages
- Higher quality payments - higher quality data means more transparency and more remittance information for customers, which means better customer service
- Improved analytics - less manual intervention is required, compliance processes are more accurate, and fraud prevention measures are improved
- A foundation for end-to-end automation - with a single standard for all business domains and processes, new services are more easily created, and straight-through processing is enhanced
- Uses modern technology - ISO 20022 uses XML (Extensible Markup Language) technology, which defines rules for encoding documents in a format that’s readable by both humans and machines. This allows for fast and single integration of systems, even if a financial institution is running a legacy platform.

- Worldwide adoption - ISO 20022 is already becoming more pervasive, almost 200 market infrastructure initiatives are implementing the standard or are considering adopting it.

Payment clearers and central banks are migrating payment messages to the new format on a phased basis over the next 3 years. When the phased migration is complete MT format messages will no longer be used for payment processing.

ISO 20022 messages are intended to be used in five business areas:

- Payments
- Securities
- Trade Services
- Cards
- Foreign exchange

Dates to migrate payment processing to the new format have been communicated by country clearing organizations. However, the other four business areas timelines have not been announced yet.

According to ISO20022.org, the first focus of ISO 20022 is on international (cross-border) financial communication between financial institutions, their clients and the domestic or international 'market infrastructures'.

ISO 20022 messages replace message types developed under an older standard, ISO 15022. These older message types are used by the SWIFT electronic payments network. These have been ubiquitous for 40 years. The new ISO 20022 message types are known as SWIFT MX messages.

The Bank of England cites the following advantages of ISO 20022 messages over the older ISO 15022 messages:

- Flexibility – adapts to changes more easily
- Harmonization – over 70 countries have adopted
- Compliance and regulation – richer data aids transparency of transactions

- Resilience – interoperability allows rerouting
- Enriched data – better and more complete reference information
- Competition and innovation – fuelled by flexibility
- Straight-through processing – better data leads to less intervention
- Analytics – improved decision making based on better data

The older ISO 15022 messages that are being replaced by ISO 20022 are used by SWIFT members including banks, money brokers and security broker dealers, clearing systems, corporates, non-bank financial institutions and others.

There are also service provider outside of SWIFT who have adopted MT-like messages for the services they provide. They are likely to feel pressure to support ISO 20022 style messages, in which case their customers may also have to make the switch.

The switch to ISO 20022 is already underway. Some settlement systems and clearing houses in South American countries began supporting the new messages as early as 2007. Some of the most important financial services providers in Europe and the United States will make the change in 2021 and 2022.

If you are sending or receiving SWIFT MT messages then you will have to adapt your workflows to the new style of messaging. These changes are likely to impact not only the payments process, but in the future will also impact reconciliations, confirmations, cash management, liquidity management and other business functions.

Because support for the older style of messages is likely to wane quickly, doing nothing is probably not a viable strategy. You may be able to outsource transformations between the older messages and the new ISO 20022 messages, but this is likely to be acceptable only as an interim measure. Most organizations will find that they need to adapt their systems to the new messaging standard.

Disclaimer

This paper - *SourceLess Blockchain Whitepaper* – is made strictly for informational purpose. SourceLess Blockchain does not guarantee the accuracy of the conclusions reached after being studied.

SourceLess Blockchain does not provide, express or imply any warranties and is not limited to:

1. Warranties of commercial exchanges suitable to a particular purpose, agreement, usage or balance of trade;
2. The document's details may contain errors of interpretation;
3. Fulfilments of legal rights of third parties;

SourceLess Blockchain assumes no liability for any form of usage, exchange or reliance damages even if one is informed about the possibility of such damages.

SourceLess Blockchain must not be chargeable by any means to any entity for damages, losses, costs or expenses of any kind whether direct or indirect, consequential, compensatory, incidental, actual, commendable or special for using or referring to this document (whitepaper), or to any part of its content, including without limitations any loss of business, income, profits, data, goodwill or other intangible losses.

This document is not approved by any governmental authority. *SourceLess Blockchain Whitepaper* is only available on *SourceLess.io* website and must not be shared, reproduced or transmitted to any other entity or published, partly or entirely, for any purpose without prior written consent of SourceLess Inc. In addition, the document must not be transmitted to any country or territory in which its circulation or content is prohibited or restricted.

Every single entity (legal or not) in possession of this document (whitepaper) must inform him/herself, comply with relevant, legal and regulatory restrictions to which one may be subjected and seek all necessary professional advice to it.

Provisional Software Patent No.US63/294,483
ISO 20022 Compliant

INTRODUCTION

INTRODUCTION

From the start of human evolving point until nowadays there have been several revolutionary moments. Since the discovery of the wheel, all the way to the combustion engine, written press or Internet foundation, the world has been in a continuous change and expansion.

In order to get to its current form, the Internet, which appeared in 1977 in the form of a small number of interconnected computers, carrying a small amount of data, has encountered drastic changes. Currently, the amount of data which can be transferred is limited only by the capacity of the system storage.

For interconnection, there is no need of wires and communication has advanced therefore and has become a necessity to everyday life. However, even if this evolution opened up new opportunities, several problems have also increased, such as: human trust has reached a critical level, being obvious in any filed and the vulnerability of intrusion has expanded considerably.

In fewer words, the Internet resembles the blockchain way of function, exchanging value instead of information.

Blockchain technology was created to solve the problem of doubt and in order to achieve data transfer in a safe and controlled way, without the need for a centralized authority to coordinate it.

The infrastructure of this technology was set in 1991, when Scott Scornetta and Stuart Haber considered developing for the first time a cryptographically secured block system. The project was supposed to grow the following year when, together with Dave Bayer, they integrated the Merkel-type trees into the existing technology, optimization that improved the functionality of blockchain, making it possible to store and send information between several blocks of data.

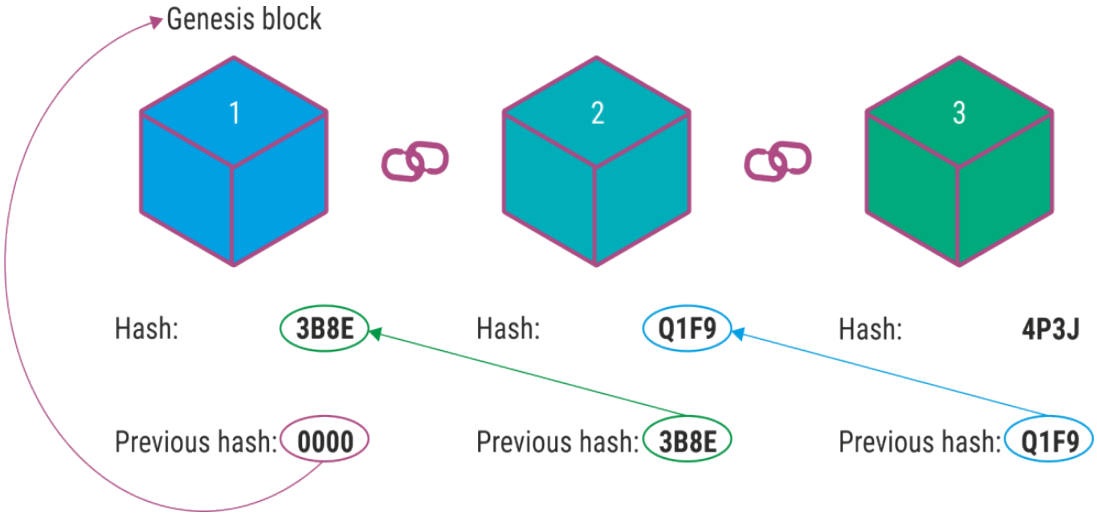
A blockchain is a thriving list of records/data, called blocks, which are linked together and secured with the help of cryptography. Identical to data structure, a blockchain is a simple chained list, in which the links between elements are connected to each other. This way, each block contains a link to a previous block, a timestamp and the transaction data.

By design, blockchains are resistant to data alteration. A blockchain is a transparent and distributed ledger, in which can be recorded transactions between two members in an efficient, testable and permanent way.

In order to be used as a distributed ledger, a blockchain has to be managed by a peer-to-peer collective network that follows a validating new blocks protocol. Once recorded, the data from any block can no longer be modified retroactively without altering the blocks following the previous one, a measure that requires the majority participants in the network's consent.

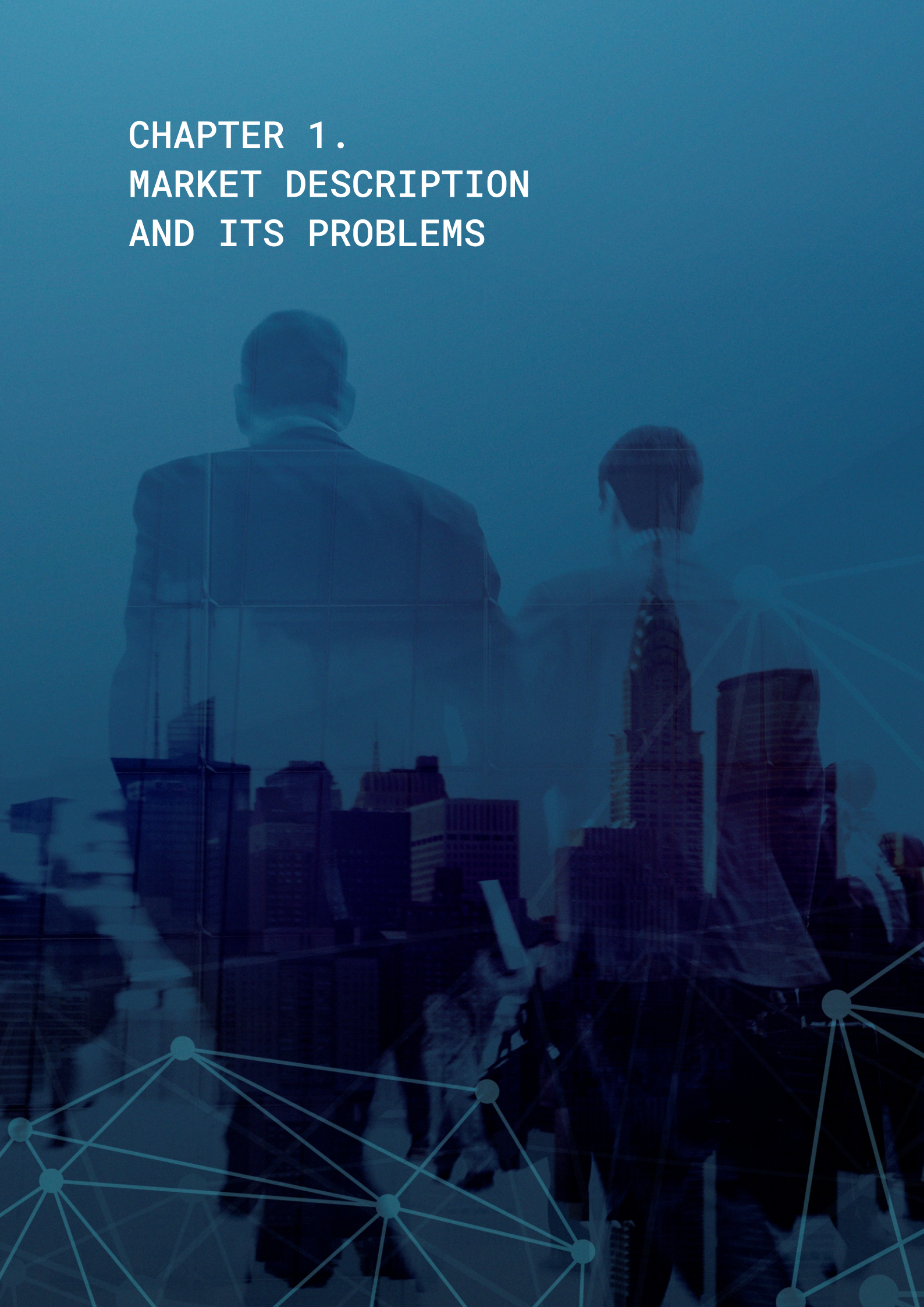
Blockchains are secured by construction and remain an example of a distributed computing system with high tolerance to attackers or uncooperative computers. Therefore, the issue of decentralized consent has been solved using blockchain technology.

This makes blockchain technology suitable for recording events, medical history as well as other management activities: identity management, transaction processing, documentation origins, commercial route of food products tracking or voting systems.



Provisional Software Patent No.US63/294,483
ISO 20022 Compliant

CHAPTER 1.
MARKET DESCRIPTION AND ITS PROBLEMS



CHAPTER 1. MARKET DESCRIPTION AND ITS PROBLEMS

World Wide Web (current www)

In order to get to its current form, the Internet, which appeared in 1977 in the form of a small number of interconnected computers, carrying a small amount of data, has encountered drastic changes.

Currently, the amount of data which can be transferred is limited only by the capacity of the system storage. For interconnection, there is no need of wires and communication has advanced therefore and has become a necessity to everyday life. However, even if this evolution opened up new opportunities, several problems have also increased, such as: human trust has reached a critical level, being obvious in any filed and the vulnerability of intrusion has expended considerably.

Hosting Issues

Slow loading speed or recurring downtime

For a site to get more traffic, it is necessary to have a considerably faster navigation. Low speed and downtime are some of the biggest website hosting issues, as slow performance will steal site traffic, SEO rankings and conversions. The time of breakdown is the most problematic issue. During that time, not only is your site down, but the web is unavailable and the business opportunities along with your reputation are fading.

Lack of security

Everyone wants their site data safe. When your provider (the only one who can help you with hosting process problems) is not available, it can be really inconvenient. When it comes to hosting types, a shared one is probably the least secured, due to low level of privacy.

There are a lot of web hosting companies which cannot protect your data against hacking or identity theft and they often offer a false sense of security in order to take over the hosting facilities.

Slow or unresolved customer support

At some point, you may need to call customer support. They must respond quickly and solve the problems which have appeared. Otherwise, you could get stuck in your work or have a really long delay.

Excessive cost of a web hosting and its limitations

You might find it surprising how some companies can afford giving free hosting services, while others charge a fortune. Many web hosting service providers do not unveil the limitations of web hosting services in advance. For this reason, customers fail to understand the scope of the service offered by the web hosting company.

ERRORS RELATED TO IP ADDRESSES

Failed connections to local files or shares

Sharing issues are probably the most difficult network issues to be solved, due to the number of components in need of a correct configuration.

Most commonly, sharing problems arise due to conflict between mixed security environments. Even different versions of the same operating system sometimes use slightly different security models, which can make workstations interconnectivity difficult to getting solved.

Slow internet performance

Slow performance appears because of congestion or sometimes, poor quality connections which have corroded or even deteriorated. Congestion may not be directly related to bandwidth reduction since a single overloaded port on a switch router can reduce drastically network performance. This can appear especially with leased lines, where a dedicated bandwidth is expected, but the speed tests indicate that the network does not reach its nominal potential.

WWW/HTTP domains

Tim Berners Lee made the following statement: “I would like to see people enrolled in a cheap data plan by default. I would like them to get it for free.”

The current internet doesn’t give you ownership of your domain and just allows you to rent it for a while. This means that it can offer you these data but with regulations and a lot of conditioning, fact that leads to other expenses and technical and logistical problems: IP, hosting etc. Current domains can be transporters of viruses which a computer is not able to exterminate.

Security

In a centralized system with a common server and a commonly known network architecture we can observe different types of vulnerabilities, based on a very defined attack point, to which is added the human factor. In these conditions, those vulnerabilities can persist and also cause damage. In recent years, individuals and institutions (public or private) which had used centralized systems, also faced ransomware attacks.

The vulnerability of networks can manifest on 2 levels:

- The possibility of modifying or destroying information, i.e., attacking its physical integrity;
- The possibility of unauthorized use of information, i.e., its leakage from the settled web of users;

Threats to the security of a computer network can have the following origins: human made or natural disasters, equipment failures, human operating or manipulating errors, or fraud. Several computer security studies estimate that half of the costs involved in solving these incidents are due to wilfully destructive actions, a quarter to accidental disasters and another quarter to human mistakes. Analysing the wilfully threats, we can distinguish two main categories: passive attacks and active attacks.

Passive attacks – are those attacks in which the intruder notices the information he is passing by through the "channel", without interfering with the flow of messages. As a result, only traffic analysis is performed by reading the identity of the communicating parts and learning the length and frequency of these messages from the channel, even if the content is unintelligible.

Passive attacks have the following common characteristics:

- Do not cause damage (no data are2333323 deleted or changed);
- Violates privacy rules;
- The main scope is "listening" to the data exchanged throughout the network;
- Can interfere in a variety of methods, such as surveillance of telephone or radio links, exploitation of the electromagnetic radiation emitted or routing of data through additional but less protected nodes;

Active attacks – are those attacks in which the intruder engages either in stealing messages or in modifying, resuming or inserting false messages. This means that he can delete, delay or modify messages, insert false or old messages or change the order of messages either in a certain direction or in both directions of a logical channel. These attacks are extremely worrying, as they change the state of the computer systems, data or communication systems.

These are the following types of active threats:

Identity theft – is the attack in which one entity claims to be another entity; For example, one user can try to substitute himself for another, or one service can claim to be another service with the intention of storing confidential data (credit card number, passwords or encryption algorithm key). Identity theft is usually accompanied by another active threat, such as replacing or modifying messages.

Replay – this attack occurs when a message or a part of it is repeated with the intention of producing an unauthorized effect; For example, one can reuse the authentication information of a previous message: in bank accounts, the resumption of data units involves duplication and/or other false changes in the account value.

Modifying messages – this form of attack causes the message data to be altered by modifying it, inserting something false or deleting it. It can be used for example to change the recipient of a loan. Another use may be the change of the recipient/sender field of an email.

Denial of service – this attack occurs when an entity fails to perform its own function or when certain actions prevent another entity from performing its own function;

Service repudiation – occurs when an entity refuses to recognize an executed service. It is obvious that in electronic funds transfer apps, the repudiation of the service by both the sender and the recipient must be avoided at all costs.

When it comes to active attacks, some programs created with a destructive purpose and, which sometimes essentially affect the security of computers are also enrolled. There is technology which can be used to present the different possibilities of attacking a system.

This vocabulary is well popularized by “stories” about “hackers”. Attacks generally involve either reading unauthorized information or destroying (partially or totally)

data or computers, the most serious aspect being the potential possibility of infestation through the network or even copies of floppy disks.

Among these destructive programs we mention the following:

Viruses – are programs inserted into applications which are multiplying on their own in other programs in the resident memory space or disks; Then, either they completely saturate the memory/disk space and lock the system or, after a finite number of multiplications, they become active and enter into a destructive phase.

Software bomb - is a procedure or part of code included in a "normal" application, which is activated by a predefined event; The author of the bomb announces the event, leaving it to “explode";

Worms - have similar effects to the ones of bombs and viruses. The main difference is that they don't reside in fixed locations and don't duplicate themselves; they move around all the time, making them difficult to be detected. The most famous example is The Internet Worm, which removed a part of the internet from its function in November 1988.

Traps – are special accesses to the system, which are normally reserved for remote loading procedures, maintenance or for developers of some applications. However, they allow access to the system, circumventing the usual identification procedures;

Trojan Horse - is an application that has a very well-known use function and that, in a hidden way, also fulfills another function: it does not create copies.

For example, a hacker can replace the code of a normal 'login' control program through another code, which does the same, but additionally copies to a file the name and password that the user types in the authentication process. Subsequently, using this file, the hacker will very easily penetrate the system.

BLOCKCHAINS

Most blockchains are designed as a decentralized database which functions as a distributed digital ledger. These blockchain records store up data in blocks, which are organized in a chronological sequence and are linked by cryptographic evidence.

The creation of blockchain technology has brought many advantages to a variety of industries, ensuring increased security in environment with trust problems. However, its decentralized nature also brings in some disadvantages. For example, compared to traditional centralized database, blockchains have limited efficiency and require increased storage capacity.

Blockchain is not a distributed computing system

Blockchain is a network which relies on nodes to function properly. The quality of the nodes determines the quality of the blockchain.

For example, the Bitcoin blockchain is powerful and incentivizes nodes to participate in the network. However, the same cannot be true for a blockchain network that does not stimulate nodes, meaning that it is not a distributed computing system in which the network depends on the involvement and participation of nodes.

In comparison, a distributed computing system works to ensure that transactions are verified, that they are registered and also that there is a transaction history for each transaction. Each of these actions are similar to those of the blockchain, but there still exists a lack of synergy, mutual assistance and parallel to each of them.

Clearly, blockchain could be a distributed network, but it lacks the features which make a distributed stem so beneficial for ordinary users or corporations.

The problem of scalability

Blockchains are not scalable like their counterpart centralized system. If you have used Bitcoin network before, you would know that transactions are completed depending on the congestion of the network. This issue is closely related to the scalability problem of blockchain policy. However, there has been a growing shift in the wat blockchains technology works.

With the correct evolution of technology, scalability options have also been integrated into the Bitcoin network. The solution would be making transactions outside the blockchain and use it only to store and access information. In addition to this, there are also new ways to solve the scalability problem, including authorized networks or the use of different architectural blockchain solutions e.g., Corda.

Comparing the speed of Bitcoin to VISA transactions, one can quickly notice the major difference: at the moment, Bitcoin can only make 4 to 6 transactions per second, compared to VISA, which can make up to 1700 transactions per second. At this speed, one day it will be able to make up to 150 million transactions per second.

To conclude, we can say that blockchain may not be well equipped for real world application yet and there is still a need for significant improvements before it can be adopted in everyday life.

Some blockchain solutions consume too much energy

Blockchain technology was introduced at the same time as Bitcoin’s. Miners are incentivized to solve complex mathematical problems because high energy consumption is exactly what makes these complex mathematical problems not ideal for the real world.

Every time the register is updated with a new transaction, the miners have to solve the problems which will arise, respectively spend a lot of energy. Although not all blockchain solutions work in the same way, there are other consensual algorithms that can still solve this problem. For example, authorized or private networks do not have these problems due to theirs limited number of nodes. Also, since there is no

need for a global approve, they can use effective methods of consent in order to reach it. If you think about the most popular blockchain network – *Bitcoin* – the problem still persists and requires solving.

To resume, authorized networks are efficient from the energy consumption point of view, while public networks can consume a lot of energy just to stay operational.

Blockchain data is immutable

Data immutability has always been one of the biggest drawbacks of blockchain functionalities. It is clear that several systems may benefit from it, including large supply chains, financial systems etc., but if you want to analyze how networks work, the first thing to do it to understand that this immutability can only be present if the network nodes are distributed correctly.

To be more specific, a blockchain network can be controlled by an entity if it owns 50% or more of the nodes, fact that is making it vulnerable. Another existing problem is that the data, once written, cannot be removed.

Privacy is one of the human rights. However, if one uses a digital platform running on blockchain technology, then no one can remove its trace from the system if they will no longer want it there. Therefore, there is no way to remove personal data without violating someone’s privacy rights.

Blockchains are sometimes inefficient

At the moment, there are several blockchain technologies in existence. If you choose the most popular ones, including the blockchain technology used by Bitcoin, you will be able to notice the inefficiency of the system, one of the most important drawbacks of blockchain.

A useful example may be the following: trying to configure the bitcoin miner on my system, I have come to realize that the registry can easily storage up to 100 GB.

This does not favor the data storage which can lead to storage problems for multiple nodes with the intention of becoming part of the network. Clearly, there needs to be a

better way to manage this because, whenever the data is updated, the nodes have to replicate it.

In addition, the size of the blockchain is increasing with multiple transactions and nodes so, if it continues to grow, the entire network will be slowed down. On the other hand, commercial blockchains need the network on which they operate to be fast and secure at the same time.

Slowly, these obstacles can be improved with the help of blockchain system solutions. Bitcoin is also trying to overcome these obstacles with the help of Lightning Network (LN).

Blockchains are not completely secure

Blockchain technology is more secure than many other platforms. However, this does not imply that it is completely safe. There are different ways in which the blockchain network can be compromised:

51% attack (sybil): in the 51% attack, if an entity can control 51% or more of the network nodes, then it can take over the control of the network. Doing so, it may modify then the data in the register and also double the expenses. This is possible only in networks where one can control the miners and the nodes.

Afterwards, the private networks are more capable of remaining protected from the 51% attack, while public networks are more vulnerable.

Double spending: there is still a problem with the current blockchain technology; to prevent duplication of spending, the blockchain network implements different consent algorithms, including proof of stake (PoS), proof-of-work etc. Double expanse is possible only in networks which are vulnerable to the 51% attack.

DdoS attack: in a DdoS attack, nodes are attacked by congesting the network and knocking it down.

Cryptographic cracking: another way in which blockchain technology is not secure is because of the cryptographic solution it is using; Quantum algorithms or calculus are more than capable of destroying cryptographic cracking.

Private keys

In order to decentralize the blockchain, it is necessary to give individuals the ability to act as their own bank. In order to access the assets or information stored by the user in the blockchain, they need a private key. This key is generated during the process of creating the wallet and it becomes the responsibility of the user to not misplace it. He also needs to make sure he doesn't share it with anyone else. If they fail to do so, their wallet integrity is in danger.

In addition, if the private key is lost, users will lose access to the wallet forever. This possibility becomes a disadvantage of blockchain.

Thus, once you lose your key and access to your wallet, no one can recover it. This is a problematic point as not all users are familiar with the current technology and have more and more chances to make mistakes. If there is a centralized authority who is dealing with this issue, then the goal of decentralization is defeated.

Coordination and implementation efforts

The start cost of implementing a blockchain technology is a fortune. Even though most blockchain solutions, including Hyperledger, are open sources, they require huge investments from organizations that are willing to pursue them.

There are costs associated with hiring developers, managing a team which surpasses different aspects of blockchain technology, licensing costs if opting for a paid blockchain solutions as well as the maintenance costs associated with the chosen option. For blockchain projects for businesses, the cost can also exceed 1 million dollars. We suggest that companies which do not trust the idea of blockchain or do not have the necessary funds or budget carefully analyze the market, as well as the advantages and disadvantages before boarding this technology train.

Maturity

Blockchain technology was born just a decade ago, being still a new technology, which needs time to reach maturity. Inspecting the market monopoly, one can notice many players trying to solve the problem of decentralization using their unique solution, among which we can name: Corda, Hyperledger, Enterprise Ethereum, Ripple etc.

All in all, it is still too early for blockchain to mature and so, companies will have even less hesitation to adopt blockchain technologies as their foundations are becoming more and more solid.

Like any other new technology, maturity is another issue blockchain has to solve and therefore, one of its disadvantages.

There is still a lot of work to be done before we see changes in the standardization of blockchain technology. At the moment, there are various options that aim to solve the essential problems but we have to work together to standardize them.

Interoperability

Another disadvantage that blockchain technology suffers from is interoperability. As we mentioned before, there are several blockchain networks, working separately, trying to solve the DLT problem in their unique way. This leads to interoperability problems, where these chains are no longer able to communicate effectively.

The problem of interoperability also persists when it comes to traditional systems or systems using blockchain technology.

Blockchain is the new prototype database, which has solved some of the problems centralized systems are dealing with, such as transactions without intermediary, the time spent on each transaction or unintentional deletion or modification of data in the blockchain.

Using the benefits of technology such as transparency, trust, multiple copying of transactions and decentralized digital ledger, blockchain technology is reliable and cannot be destroyed and the attacks mentioned above could disrupt the

functioning of the system, but not the technology on which it is based.

Technology used in blockchain is useful and versatile for our world, as it can facilitate most current systems in different industries but it is new and its implementation is too little studied in practice. Blockchain technology promises us a bright future, fraud and deception free due to the benefits of technology.

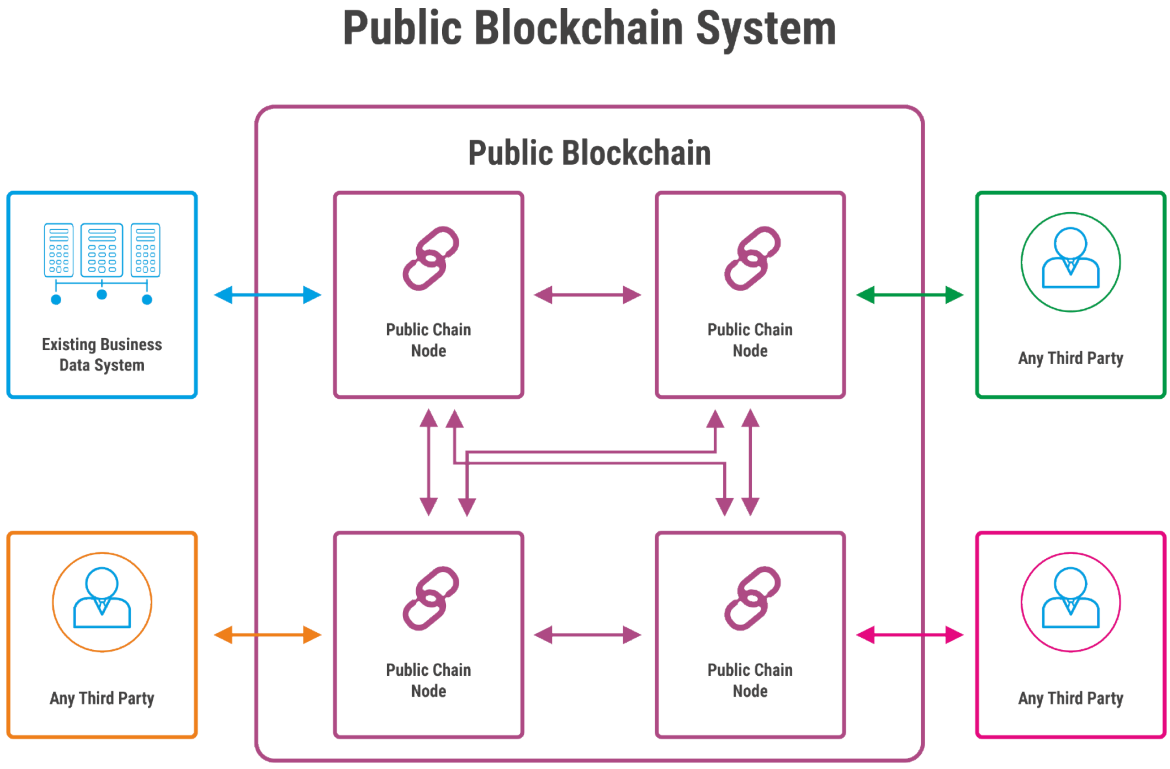
Developers need to devote more time, practical application and implementation into the already existing systems of the main industrial domains, as blockchains can help businesses, governments and honest and reliable logistics systems.

Even though blockchain technology implies a lot of challenges, the results of its use weigh more in balance. It is necessary to continue to explore the development and application of blockchain in different areas in the near future, as this new technology can help solve many difficult problems that bother the proper functioning of systems.

CHAPTER 2.
CLASSIFICATION OF BLOCKCHAINS

CHAPTER 2. CLASSIFICATION OF BLOCKCHAINS

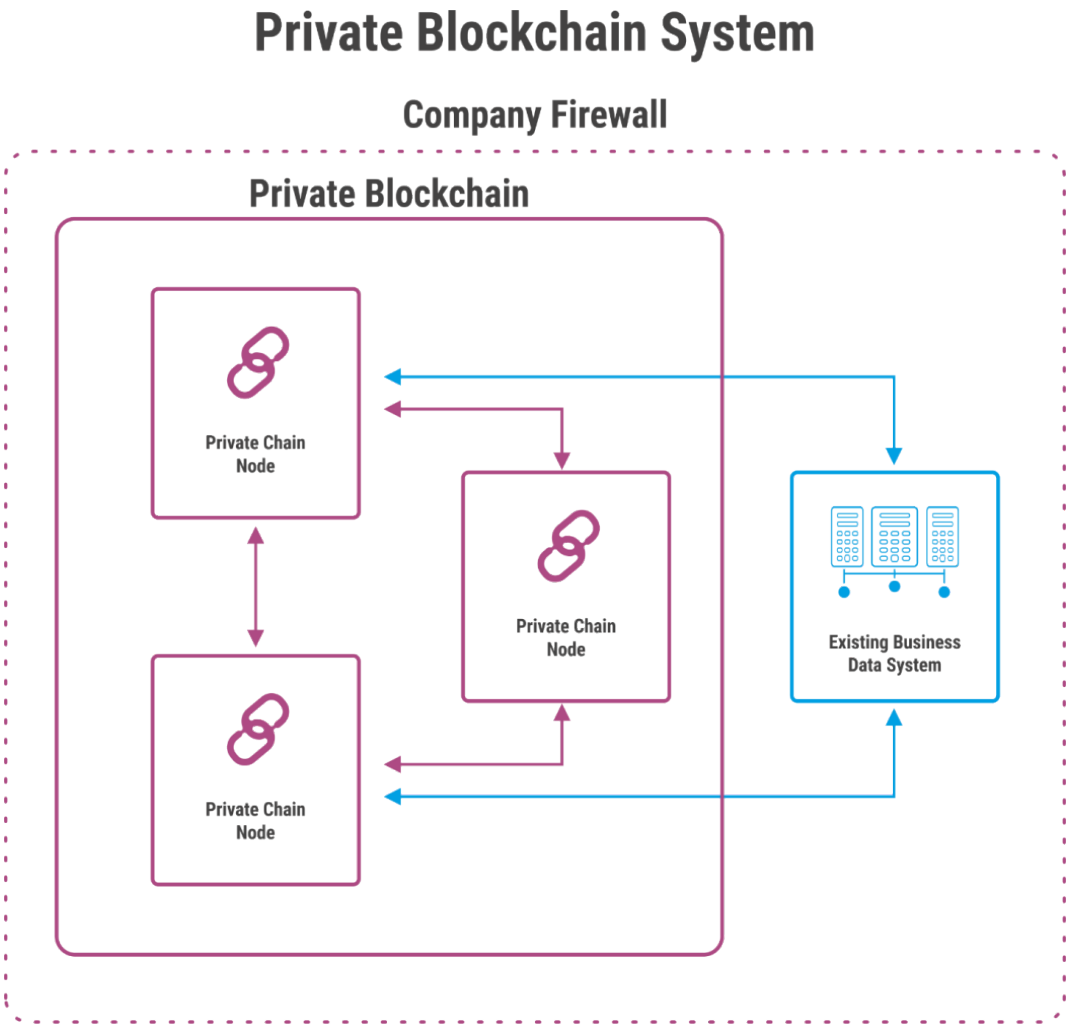
PUBLIC BLOCKCHAIN: in a public blockchain, everyone is free to join and participate at the core activities of the network. Anyone cand read, write or audit the ongoing activities from the public blockchain network, which helps maintaining its autonomous nature.



The public network operates on an incentive scheme which encourages new participants to join and maintain the agile network. Public blockchains offer a particularly valuable solution from the point of view of a truly decentralized, democratized or unreserved operation.

There are however, some downsides to a public blockchain. The first one would be the high energy consumption required to maintain the distributes public register. Other problems are: incomplete confidentiality and anonymity. This can lead to a weaker security of the participant's identity. Along genuine collaborators, participants can sometimes include fraudulent members who may be involved in malicious activities such as hacking, theft or network clogging.

PRIVATE BLOCKCHAIN: a private blockchain allows the selected entry of the verified participants; A participant can join such a private network only through an authentic invitation, after being also verified. A validation is also required to be carried out either by the network operator(s) or through a clearly defined protocol implemented by the network in cause.

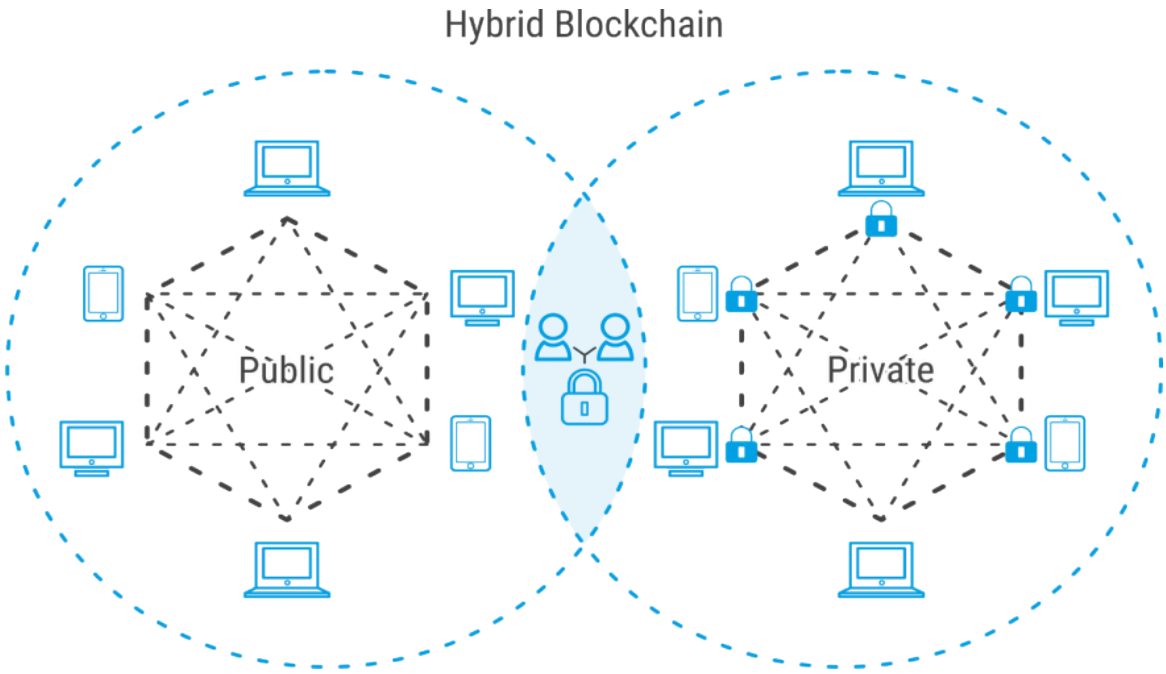


The main distinction between public and private blockchains is that the private ones control who is allowed to participate in the network, to execute the protocol, to decide mining rights and rewards and maintain the shared register. The owner or operator has the right to modify, edit or delete entries that are not needed from the blockchain.

In its truest meaning, a private blockchain is not decentralized and represents a distributed ledger, functioning like a closed, secured database along with cryptography concept foundations. From a technical point of view, not

everyone can run a complete node on the private blockchain, make transactions or validate the changes of the blockchain.

HYBRID BLOCKCHAIN: this type of blockchain is made through a mix between the private and the public blockchains and supports many customization options, such as allowing anyone to join the authorized network after proper verification of their identity and assigning selected designed permissions to perform only certain network tasks.



These type of blockchain is built in order to grant special permissions to each participant. This allows participants to be able to perform specific functions (reading, accessing and writing information in the blockchain). Companies are opting even more now for authorized blockchain hybrid networks, as they can place restrictions during network configuration and control the activities of different participants in the desired roles.

SourceLess Hybrid Blockchain is best defined as a blockchain that uses the best solutions of both public and private networks. SourceLess Hybrid Blockchain means both controlled access and freedom.

SourceLess Hybrid Blockchain architecture is distinguished by the fact that is not open to anyone, but still

offers blockchain specific functions such as integrity, transparency and security.

Considered the internet of values – WEB 3.0 is among the top disruptive technologies alongside Artificial Intelligence, Internet of Things, Augmented Reality or Robotics and is an integral part of SourceLess Blockchain.

A.R.E.S.

A.R.E.S. is a software based smart contract in the SourceLess ecosystem which will govern the entire behavior of SourceLess components. A.R.E.S. will help implement smart contracts in regular computer-based software and facilitate the governance of account tokenization.

A.R.E.S. has over 900 predefined functions and rules, influenced by Python, Java, GO (GoLang), designed to work with all workers (node).

Through A.R.E.S., anyone can create contracts for uses such as the voting process, crowdfunding, auctions and multi-signature wallets.

Due to the interoperability of the SourceLess Blockchain with other blockchains such as Solana, Ethereum, Polygon, etc., related software will be recognized and usable (e.g. Solidity, Rust, GO) in the SourceLess ecosystem.

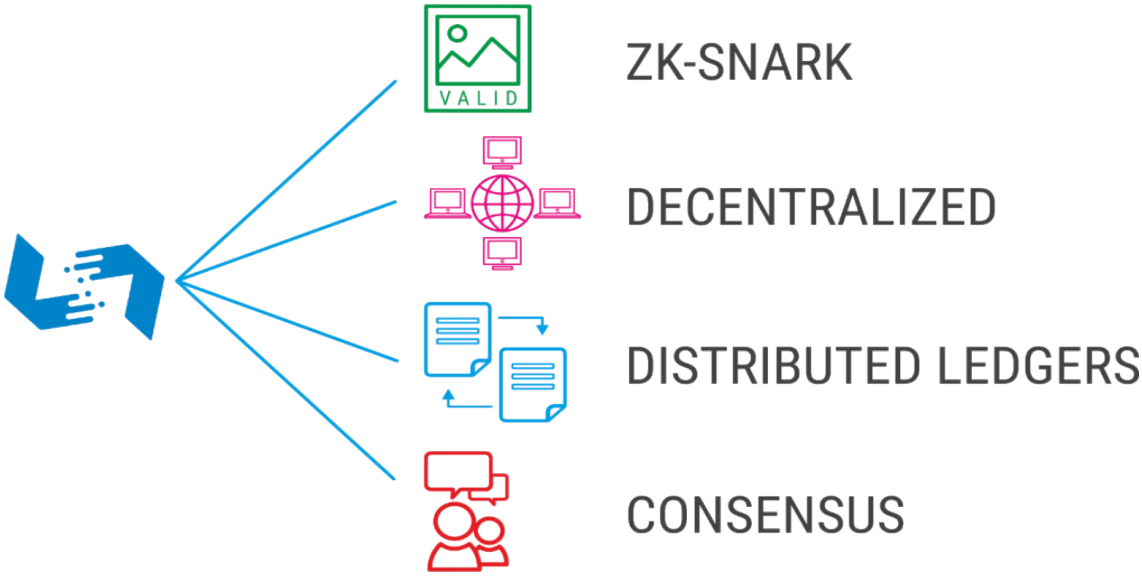
CHAPTER 3.
WRITING THE SYSTEM

CHAPTER 3. WRITING THE SYSTEM

Security and privacy

First of all, we need to make a first distinction between anonymity and confidentiality in the context of transactions of any kind, whether we are talking about financial transactions or data transactions. It is called an “anonymous” transaction when no one knows your identity and a “confidential” when the transaction and its content are unknown.

SourceLess Blockchain ensures this anonymity with the help of secure, credible and accredited companies in the fields of Know Your Customer (KYC) and Anti Money Laundering (AML). Specifically, when a user creates an account in SourceLess Blockchain, he is anonymous at the time of creating the account, but then he must provide his identity data to a third company which will KYC and AML verify him and also certify that the WNFT and the registration in the blockchain are the same as in reality.



The anonymity part only works when the transactions are written in the blockchain and does not violate the law. When a user breaks the law, the force structures can directly access the third-party company providing the KYC & AML services and clearly identify the user who committed the illegality. This

rule will coerce SourceLess Blockchain user, through the identity he is assuming and certifying, not to violate the law, fact that demonstrates that our product is considered 100% WHITE LABEL.

The security in SourceLess Blockchain is also based on +256 KB data encryption. At this moment, no one can create a fracture into a 256 KB encryption, thanks to patented and confirmed security standards IEEE STD 1363.1 and OASIS KMIP, which specify that any type of AES256 bit encryption will be based on an algorithm with the level of security appropriate to the attacks initiated by Quantum Counters.

The SourceLess Blockchain system is created to have the possibility of initiating an upgrade regarding Quantum Computers, a fairly clear component in which any type of connection with a Quantum Computer is identified and automatically removed. In the written code of SourceLess Blockchain, everything that becomes Quantum Resistant starts from the military grade encryption to the piece of code that rejects a certain number of connections with a particular node directly.

An important perspective of SourceLess consists in the importance of SNARK, not-interactive zero-knowledge proofs, which refers to the proof of the construction in which the possession of an information can be proved, without showing that information and without any interaction between the one who asks for proof and the one who checked it. ZK (Zero Knowledge) translates to information verified without making it public.

For a platform to be truly considered decentralized, it must eliminate the possibility of manipulation or control shown by centralized entities, which cannot happen without confidentiality. Recent incidents in the spectrum of security and privacy have shown the need to protect one’s identity and data has never been a higher priority. With the help of the distributed ledger technology (DLT) protocol, which allows the existence of a decentralized database, SourceLess Blockchain removes all security risks from the system, including the authority of a person/entity and distributes it to all the users in the network.

In a centralized system with a common server and a commonly known network architecture we can observe different types of vulnerabilities, based on a very defined attack point,

to which is added the human factor. In these conditions, those vulnerabilities can persist and also cause damage. In the recent years, hospitals, state institutions, public or political persons using centralized systems have faced ransomware attacks that in the first phase, in order to produce effects, must identify a clear target.

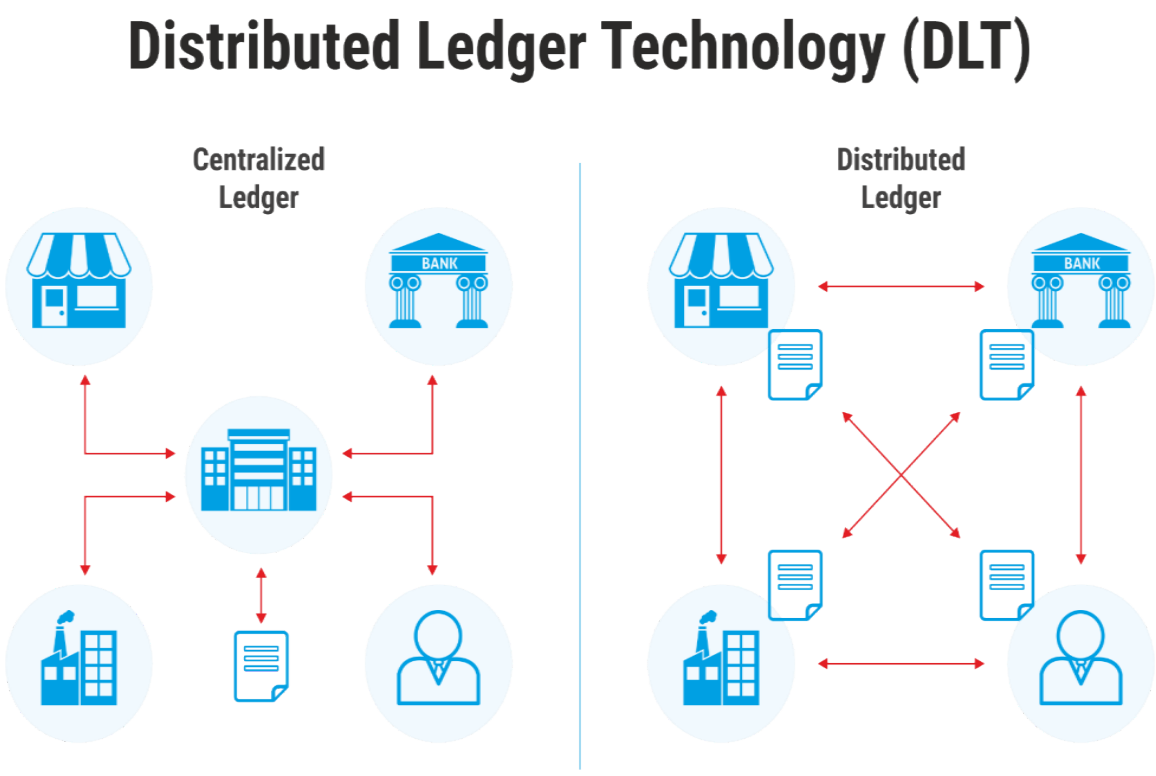
In SourceLess Blockchain it is impossible to identify the target or central point, since the database is both encrypted and then randomly distributed among the users with the help of DLT. All the copies are then stored in the network. For such an attack to be successful, this decentralized database should be attacked and corrupted at the same time. Under these circumstances, not having a central point that can be attacked and not having the possibility to attack all the nodes at once, our system becomes 100% immune by definition.

DLT has a much more substantial role than encrypting information and distributing it to the users specifically, it has the role of getting each participant to contribute automatically with some of his memory and processing power for the well function of the network and to create information in a much faster way, taking out the standard and turning it into a database more accurate, easier to maintain and valuable correct. By using DLT technology and by distributing the amount of information throughout the network, the information can be accessed faster in 90% of the cases and can be distributed among each member of the network respectively, with certain rights. The yield in the network is increasing, making our product eco-friendly and carbon free.

Also, the DLT technology together with the ZK-SNARK allow SourceLess Blockchain to minimize the number of nodes in the network, so that each device becomes a node, joining each other node from the database. In terms of efficiency, this process is becoming faster and cheaper, with no other solution more cost effective in our days.

Distributed Ledger Technology (DLT)

DLT is a digital data transaction registration system in which transactions and their details are recorded in several places at the same time. Unlike other traditional databases, distributed ledgers do not have a central repository for a well-constructed administration functionality.



In a distributed ledger (DL), each node processes and verifies each item at a time, thus generating a record of each one and creating a consent of its veracity. A distributed ledger can be used to record static data, such as a ledger, but also dynamic data, as data transactions are doing.

Blockchain is a well-known example of distributed ledger technology

DLT is specifically reflected into the technological infrastructure and protocols, allowing access, validation and simultaneous updating of the records characteristics, the distributed registers and multiple entities or location operations.

DLT uses cryptography to securely store data, cryptographic signatures and keys which allow access only to those authorized users. Also, this technology creates an immutable database, which means that information once stored, cannot be deleted and all the updates are permanently recorded for posterity.

The system architecture represents a significant change in the way information is collected and communicated by moving the record from a single, authorized location to a decentralizes system where all relevant entities can view and modify the register.

As a result, all other entities can see who is using and modifying the ledger. The transparency of DLT provides a high level of trust among the participants and it practically eliminates the possibility of fraudulent activities appearing in the register.

In essence, DLT removes the need for entities of using the register to rely on a central trust authority which controls the register or on a third-party supplier to fulfil this role.

The enthusiasm in DLT has grown significantly in the decade before Bitcoin's launch, in 2009, as a cryptocurrency powered by blockchain technology and the first to demonstrate that DLT technology not only works, but is able to scale and stay secure at the same time.

A company for example, may have different bits of data owned by each of its divisions which contribute to a centralized database only periodically.

The great process of DLT is its ability to diminish or eliminate the often time consumption and to end error prone processes needed to reconcile the different contributions to the registry, to ensure that everyone has access to the current version and that its accuracy can be trusted.

The terms DLT and Blockchain are often used together and sometimes even interchangeably. However, they are not the same. The easiest way to define them is: Blockchain is a type of DLT, but not all distributed ledger technology uses blockchain technology.

This confusion is understandable, given the grown interest in such technologies, since the advent of Bitcoin and how interchangeable the technologies in actual use can be.

Both are used to create decentralized registers using cryptography. Both create immutable records which include time stamps. Both are considered almost unattainable, can be public, making them open for anyone to use as in the case of Bitcoin, or can be made private and thus restricted to authorized users who agree to certain standards of use.

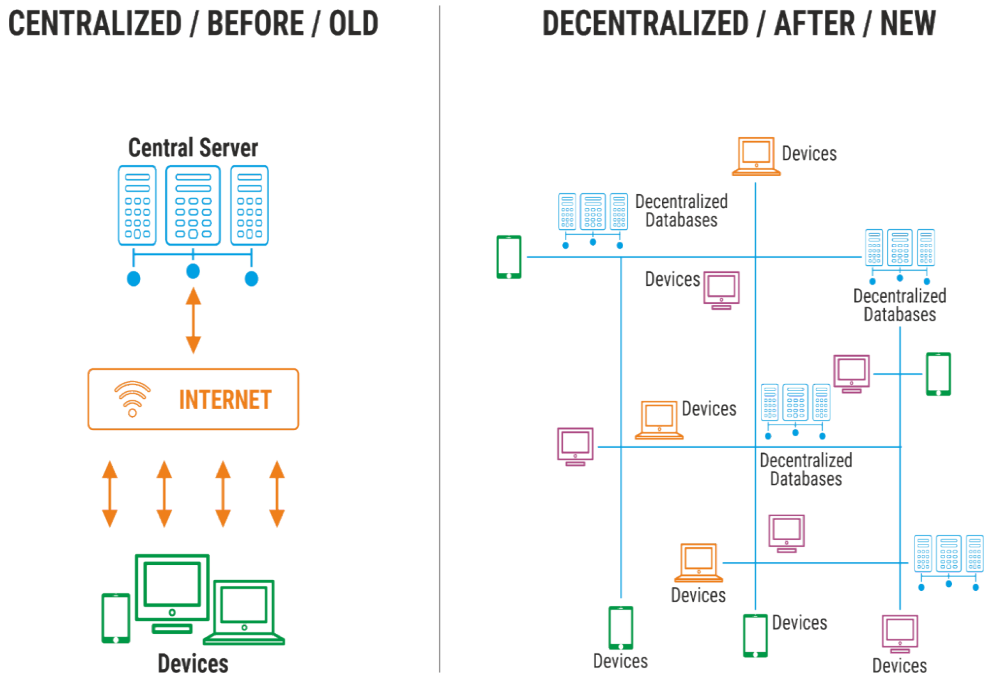
The major difference between the two is that Blockchain uses blocks of data that are chained together to create the distributed regulator, as the name describes it, while DLT also includes technologies that use other designs principles to create a distributed ledger.

To be considered a DLT, the technology does not have to structure the data into blocks.

Peer-to-Peer (P2P)

A peer-to-peer (P2P) network is a group of computers, each one acting as a node for sharing files within the group. Instead of having a central server acting as a shared drive, each computer acts as a server for the files stored on it.

When a P2P network is established over the Internet, a central server can be used to index files or to set up a distributed network where file sharing is accepted between all users on the network which store a particular file.



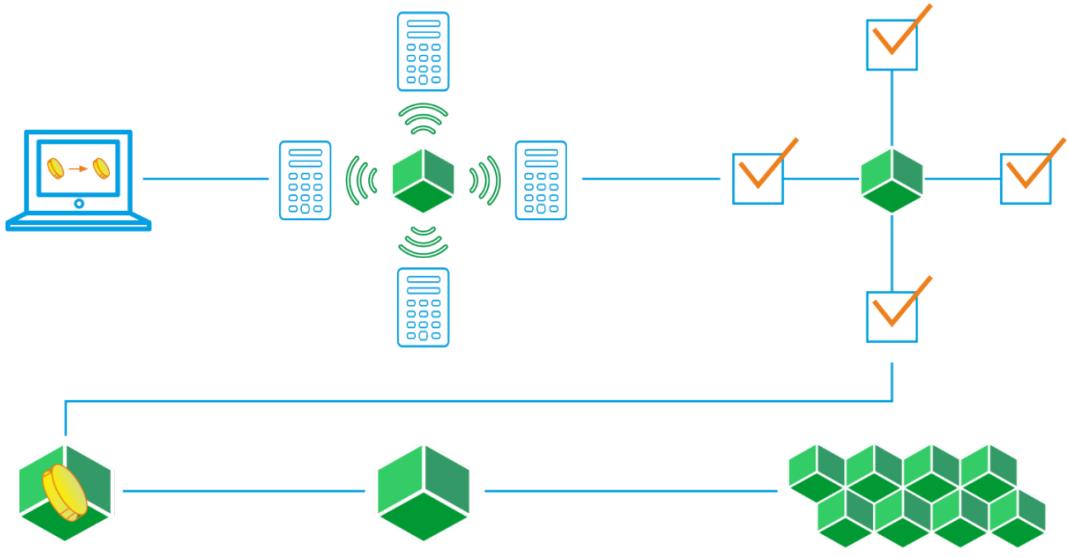
Elementary speaking, a peer-to-peer is a simple network in which each computer doubles like a node and as a server for the files it owns exclusively. These are just like a home network or an office network. However, when P2P networks are established on the internet, the size of the network and the

files available allow sharing huge amounts of data. Early P2P networks like Napster used client software and a central server and later networks like Kazaa and BitTorrent removed the central server and split their sharing tasks between multiple nodes to free up bandwidth. P2P networks are usually associated with internet piracy and illegal sharing of fact sheets.

ZK-SNAKR

ZK-SNARK is an acronym for Zero Knowledge Succinct Non-Interactive Argument of Knowledge. A ZK-SNARK is cryptographic evidence that allows one of the parts to demonstrate that it has certain information without disclosing it. This proof is possible using a secret key created before the transaction takes place.

A ZK-SNARK uses a concept knows as “zero-knowledge proof”. The idea behind this was first developed in the 1980s. Putting “zero-knowledge proof” is a situation in which each of the two parts in a transaction is able to verify each other shared information, without revealing, at the same time, what that information is.



For most other types of evidence, at least one of the two parts must have access to the information. A traditional proof of that can be compared to a password used to access an online network. The user sends the password and the network itself checks the content of the password to verify that it is correct.

To do this, the network must also have access to the content of the password.

A Zero-Knowledge Proof version of this situation would require the uses to prove to network (though mathematical evidence) that he has the correct password, without revealing the password itself. The advantages of confidentiality and security in this situation are clear: if the network does not have the password stored somewhere for verification purposes, the password cannot be stolen. The mathematical basis of ZK-SNARK is very complex however, such evidence enables one of the parts to demonstrate not only that there is a certain amount of information, but also that the part concerned is aware of that information. In SourceLess Blockchain, ZK-SNARK's bases can be checked almost instantly and the protocol does not require any interaction between the user and the verifier.

Another attribute of ZK-SNARK in SourceLess Blockchain is its ability to minimize up to below 1MB the nodes in the network, making it possible to place a node at each wallet holder.

CHAPTER 4.
PROBLEMS SOLVED BY SOURCELESS

CHAPTER 4. PROBLEMS SOLVED BY SOURCELESS

Sourceless Platform

Sourceless Platform is a Web3 platform, a software based on Sourceless Blockchain network. SOURCELESS PLATFORM is a LaunchPad by Definition – easy to use (you can create your own "ecosystem" trough Sourceless Blockchain).

The platform will give users hosting space for free.

- 1 GB for personal use,
- 10 GB for business use.

Using Sourceless Platform you can also navigate on Web2 (https://www; Apps+Software) under the protection of Sourceless Blockchain.

By using Sourceless Platform you have the possibility to integrate programs, applications and all kind of data (used as public or private) under protection of Sourceless Blockchain.

SOURCELESS PLATFORM will give free acces for user to AI software OpenAI GPT-3 and Formwelt AI.

Using the Sourceless blockchain platform, you will navigate in a 100% safe, fast and easy way.

Security using Sourceless Platform

By fully integrating companies into the platform, Sourceless solves all current cyber security problems, covering the entire area, such as:

- Application Security
- Cloud Security
- Data Security
- Identity Access Management
- Infrastructure Protection
- Integrated Risk Management
- Network Security Equipment
- Other Information Security Software
- Security Services
- Consumer Security Software

(more details in the case study area of the whitepaper)

Str.Domains (WNFT)

- WNFT is a lifetime property of a STR.domain;
- STR.domain is a unique digital identity to connect in the Sourceless Platform;
- Every owner of a STR.domain will have to complete the KYC & AML verification, before getting the full functionality of his domain;
- You can buy as many Str.Domain addresses you want, and sell them anytime you want, at any price you want, but this process is made only through Sourceless Inc. – owner of Sourceless Platform;
- Based on the KYC & AML protocols, all identities will be clear and certified, which means that the system is WHITE LABEL 100%.

Web 3.0

Web 3.0 is the next stage of web evolution that would make the internet smarter and have the ability to process information with an almost humanoid intelligence through the power of AI systems, which could run intelligent programs in order to help the users.

Tim Berners-Lee came to the conclusion that the semantic web is meant to “communicate automatically” with systems, people and devices at home. As such, content creation and decision-making processes will evolve in both humans and machines. This would allow the ability of a faster way of creating and distributing content directly to each internet consumer.

There are some fundamental differences between Web 2.0 and Web 3.0, but decentralization is among the most important one of them.

The beginning of a new era

Now that we have understood what Web 3.0 is, let’s go deeper into what Web 3.0 has to offer. Web 3.0 is mostly built on three new layers of technological information: edge

computing, decentralized data networks and artificial intelligence.

In Web 3.0, developers do not typically build or implement applications that run on a single server or store their data in a single database (usually hosted and managed by a single provider cloud).

In comparison, Web 3.0 applications either run on blockchains, decentralized networks of many peer-to-peer nodes or on “a combination of the two that form an economic crypto protocol”. These apps are often referred to as *dapps* (decentralized applications) and this term can be seen really often in web 3.0.

Benefits of Web 3.0

We are going through a revolution that will completely change our lives. Web 1.0 was all about building basic technologies and the ability to connect via internet. Web 1.0 has ahead of what Web 2.0 had to offer but it was primarily controlled by organisations and corporations in their own interest.

Web 3.0 reduces the need for human interaction, providing privacy and security to users and more power than have ever had before. The vision about Web 3.0 has changed in the last 7-8 years with the introduction of blockchain and Bitcoin. Now, the Web 3.0 focuses more on the decentralized features and the what blockchain has to offer.

Anti-monopoly and pro privacy

Web 3.0 will bring a pro privacy and anti-monopoly structure to the network and will not boost centralized platforms.

In fewer words, we will move to a completely opposite direction, where the central theme will be focused on privacy and decentralization. The middle man will not be aware of any business or obligation for this type of platform. This move will be facilitated with the help of SOURCELESS BLOCKCHAIN.

Secure network

Web 3.0 features will be more secure than its predecessors. This is possible due to two factors: the distributed nature and decentralization. Hackers or exploiters will have problems penetrating the network.

Also, if they are able to do so, each of their operations can be tracked and withdrawn from the network. Without centralization, it will become tough for hackers to take full control of an organization.

However, blockchain based platforms suffer from some form of exploitation, such as the 51% attack, but most blockchain applications and platforms can be quickly corrected for defending from these types of threats.

Data ownership

It will be easy for users to trust Web 3.0. Until now, user-generated data was stored and used by large corporations. With Web 3.0 functions, end users can expect full ownership of their data. The data transferred over the network will be fully encrypted.

Users will also be able to decide what information they want to share with corporations or advertising platforms. On the other hand, the current trend is a completely different one. With Web 3.0 functions, users can now sell their corporate data and gain from it.

Interoperability

Interoperability is one of the main features of Web 3.0. With a decentralized network, it will become easier for apps to work on different devices and platforms: TVs, smartphones and so on. It will also be easier for developers to promote Web 3.0 applications.

Provisional Software Patent No.US63/294,483
ISO 20022 Compliant

No interruption in service

Distributed systems are less prone to service interruptions. Since there is no central entity that works, it becomes difficult for an attempt to distribute service denial (DDoS) or other forms of service malfunctions to have an impact. This makes Web 3.0 a great place to share essential data and services without worrying about service interruptions.

Blockchains without permission

The idea behind Web 3.0 is to empower blockchains that they don’t need a central authority. This means that anyone can join the blockchain and participate by creating just an address. Blockchains without permission open up a new range of possibilities, including access to people discriminated for their gender, income, geography and many more. This means that there will be no restrictions whatsoever on Web 3.0.

Semantic Web

Web 3.0 will also host the properties of a semantic web. Semantic webs had improved a lot over the last years and are more complex than the latest set of technology, the one used for Web 2.0. They allow data to be shared across multiple community systems, platforms and boundaries and will act as a bridge between different data formats and platforms. By using the semantic web, we will be able to connect, share and enjoy the Internet better than ever before.

Ubiquity

Ubiquity is the result of interoperability. With Web 3.0, we can access data and information through multiple applications without being limited to a specific device, so you will not have to worry about accessing the Web 3.0. If a device has basic internet functionality and connectivity, you are able to access the Web. All in all, our lives will change completely as we will be connected through a better set of

technologies, such as artificial intelligence, blockchains and many others.

The result: a compatible human-centric computer science network which preserves privacy for the next wave of the Web. AI and machines learning algorithms have become powerful enough to create useful predictions and actions, sometimes even lifesaving. When layered over the new decentralized data structures, potential applications go far beyond targeted areas.

In Web 3.0, identity also works differently from what we are used to today. Most of the time, in Web 3.0 applications identities will be linked to the wallet address of the user interacting with the app in cause. Unlike Web 2.0 authentication methods, such as OAuth or email + password (which requires almost all the time the users to hand over sensitive and personal information), the wallet addresses are completely anonymous, unless in which the user decides to publicly expose his identity.

Generative Pre-trained Transformer 3 (GPT-3)

The GPT-3 is a self-regulating language model that uses deep learning to produce human-like text.

It's the third-generation language prediction model in the GPT-n series (and the successor to the GPT-2) created by OpenAI, a san Francisco artificial intelligence research lab. The full version of the GPT-3 has a capacity of 175 billion machine learning parameters. The GPT-3, which was introduced in May 2020 and has been in beta testing since July 2020, is making it seemlike a trend in natural language processing systems of pre-trained language representations.

GPT-3 was used to create articles, poems, stories, news and dialogues using only a small amount of text.

The GPT-3 is also used for automated conversational tasks, responding to any text that a person types on the computer with a new piece of text appropriate to the context. GPT-3 can create anything with a text structure, and not just text in a human way. It can also automatically generate text summaries and even programming code.

When a user provides text, the system detects the language and uses a preacher of text to create the most likely output.

Even without much adjustment or additional trainining, the model generates high-quality output text that feels similar to what the human mind would produce.

Whenever a large amount of text needs to be generated from a robot based on a small amount of text entered, the GPT-3 offers an excellent solution. There are many situations in which it is not practical or effective to have a human at hand to generate text or to need the automatic generation of a text that seems human.

For example, customer service centers can use GPT-3 to answer customer questions or support chatbots; sales teams can use it to connect with potential customers and marketing teams can write articles using GPT-3.

The OpenAI API can be applied to virtually any task that involves understanding or generating natural language or code. It offers a spectrum of models with different levels of depth, suitable for different tasks, as well as the ability to adjust your own custom models. These models can be used for everything from content generation to semantic re-search and classification.

The API is powered by a family of models with different capabilities and price points. The basic GPT-3 models are called Davinci, Curie, Babbage and Ada. The Codex series is a descendant of the GPT-3 that has been trained in both natural language and code.

So, whether you want to build a chat bot, whether you want to create a translation platform or even build and generate a virtual game, GPT-3 is the future of creation.

FORMWELT

FORMWELT is a coding language for language and meaning. It is a linguistic system based on the injunction of acquiring a definition. Its core consists of about 320 references: we can consider them words with concrete meaning that explain each other, without gaps.

The formwelt core is more than enough from a semantic point of view. It contains the basic concepts necessary to describe any phenomenon that one can think of.

Using the FORMWELT core you can clearly say what can be said and do what can be done, resulting in a significant description.

FORMWELT always offers exits to empirical, practical or mental experience: so that you can understand what you are saying, do what you say and see, feel, hear, taste or smell the results of your descriptions.

FORMWELT offers a language that can be spoken just like conventional language. In fact, it is based on the language we speak every day and improves it, since each user can further improve it.

FORMWELT is used in the existing languages of our world and the results of interactions based on the language programmed by FORMWELT will be better coordinated, less prone to misunderstandings and failure and more accurate and much more in line with the plans of the individuals who use it.

The core is constructed from references, each reference being represented by a fairly short string of words: a label indicating its referent, which is (mostly) constructed from labels indicating their referents. Sufficiency of the kernel means that it uses only words that are either referenced in the kernel or can be understood by the simplest and most common cognitive or practical concepts.

In short, FORMWELT is a language we can use to communicate with each other, regardless of nationality or language, and to understand each other directly without leaving room for interpretation.

Internet of Things (IoT)

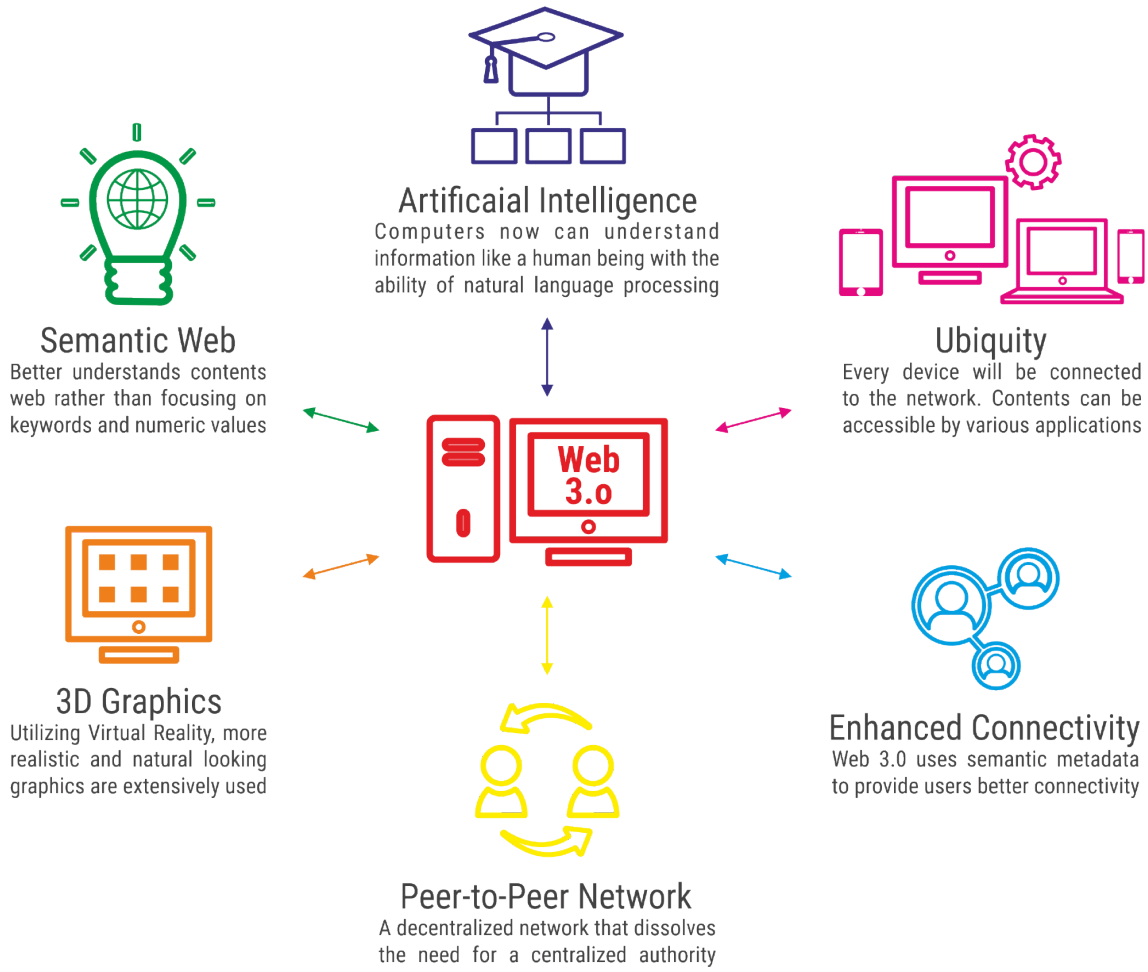
The Internet of Things (IoT) refers to the billions of objects and devices around the world that are connected to the internet, collecting and exchanging data. All personal, commercial and industrial devices are equipped with chips through which they collect and communicate various information without human intervention.

Commercially, many of these objects aim to improve what is known as Quality of Life (QoL), easing people's daily responsibilities, and industrially, interconnecting machines and appliances to further revolutionize the market.

According to a study released by the Gartner Institute (source: www.gartner.com) "more than 50% of new businesses will incorporate elements of IoT". According to the same study, utility providers and governments are and will remain the most important users of IoT technology.

The IoT segments that are growing the most during this period are the automotive industry (autonomous cars), automated services (street lighting) and healthcare providers, who use this technology mostly for monitoring chronic diseases.

The adoption of new technologies is visible across industry, in public institutions and in the everyday lives of consumers. The data generated by the devices helps companies operate more efficiently, gain insight into business processes and make real-time decisions.



By combining device connectivity with systems automation, information can be collected, analysed and, by default, a

decision can be made in response. IoT can therefore help a person accomplish a task. Moreover, IoT gives devices the opportunity to communicate not only within a private network, but also between different types of networks, creating an interconnected world.

Benefits of IoT for businesses:

Even though the benefits for business differ depending on the way of implementation, a common thread can be observed: companies have access to more data about their products and internal systems, thereby possessing a stronger ability to make changes.

For example, within the manufacturing industry, various retailers are introducing sensors into product components that transmit data on their performance. In this way, companies can identify when a component is prone to failure and replace it before it causes a real danger. Furthermore, businesses can use the data to streamline their systems and supply chains, given reliable information about their functionality.

Considered at the size of an entire supply chain or within a particular industry, the impact can be huge, noticeable in the accurate delivery of materials and the efficient management of production throughout its lifecycle.

Benefits of IoT for consumers:

New technologies come with the central promise of making our environment (homes, cars) smarter, easier to measure and manage. By developing such applications, consumers have the opportunity to optimise a lot of processes and measure their performance, schedule events and even prevent certain hazards.

But apart from the obvious benefits for large companies and users who want a smart home where things work at their performance, there are also some risks as there is a lot of sensitive information or personal data involved in these processes.

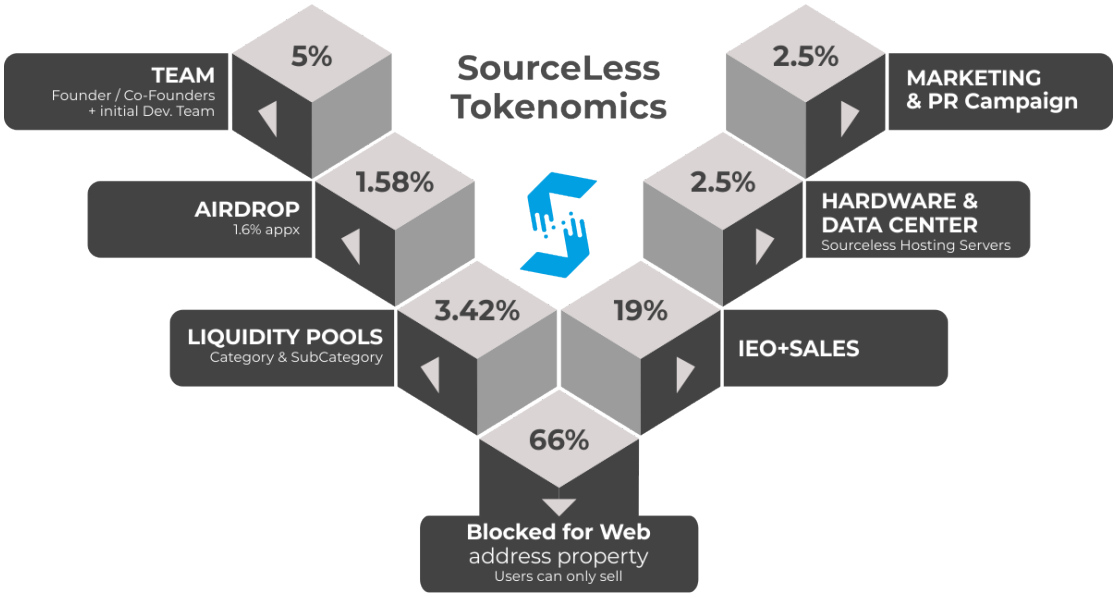
Just as having a social media account is not entirely free, as we "pay" for it with personal data that is passed on

to companies and marketing and analytics departments, so goes the IoT: the more smart objects we own, the more personal and behavioural data we send out into the void, without knowing exactly where it ends up or how it can be used.

The SourceLess Blockchain platform retains all the benefits and performance of IoT, making it a secure and encrypted environment.

CHAPTER 5.
TOKENOMICS

CHAPTER 5. TOKENOMICS



Sourceless-STR token information:

- Type: BEP-20 token, created in the Binance smart chain.
- Ticker: STR
- Total supply: 63,000,000,000 STR
- Contract: 0x30DCf96a8a0c742AA1F534FAC79e99D320c97901
- Permanent on-going supply: 21,000,000,000 STR
- Private sale price: $0.015 / $0.010 / $0.0095 / $0.009 / $0.0085 / $0.008 / $0.0075 / $0.0070.
- Public sale price: approx. $0.05

Sourceless-STR is a deflationary cryptocurrency, as it decreases market supply as time passes. This factor implies that users or the project team will participate in activities that reduce the supply of the coin on the blockchain. The way Sourceless Blockchain is going to do this is by locking in the coins (smart contract) with which the STR domains of the Sourceless platform are purchased.

One aspect worth noting is that cryptocurrencies with a limited supply are deflationary by default. They achieve this

status because as long as investors buy and hold the coin, its supply is reduced.

The Sourceless-STR cryptocurrency is a utility token, being the main currency of the Sourceless Blockchain and by which 'lifetime' ownership of a domain (of str.domain) in the Sourceless blockchain is obtained.

Practical features of a token:

- Granting (Bestowing) a right to the owner of the token, such as the right to own or use a product or the right to vote on a topic;
- Exchanging value for services provided, such as storage decentralised storage;
- Equipping (Tolling) users to enter the blockchain infrastructure or use decentralised services;
- Functioning as a way to improve the user experience, by rewarding users with tokens for certain things;
- Acting as a currency for payments on or off the blockchain, as an alternative to traditional financial payments;
- Earnings from certain things can be distributed and shared using tokens utilities;

Economic Composition

STR - Government token - 63B STR: 42B STR locked (str.domains), 2.15B STR liquidity funds locked (category and subcategory).

Str.Domains (WNFT) www.wnft.eu - value generator (42B STR - tokenomics) - WNFT is the web address (portal to the new web) which is held for life once acquired. You can buy as many Str.Domain addresses as you want and sell them whenever you want, at whatever price you want.

STR value

- 1,000 STR (~$15) locked for life per "personal" WNFT address (personal use)

- 10,000 STR (~$150) locked for life per "business" WNFT address (business use)

*personal use - e.g. STR.johndoe

*business use - e.g. STR.companyname

Examples of subdomains:

- STR.johndoe.guest1
- STR. companyname.marketingdepartment
- STR.companyname.employee1

You can also create your own token, in a very simple way, (no programming knowledge required) within the SourceLess Blockchain.

Categories and subcategories Rules + Pools

The amount paid to purchase a category or subcategory will be matched by SourceLess with the corresponding amount of STR token for liquidity (amount invested at parity with STR).

- 40 major web categories;
- Each category will have in its liquidity pool: minimum 200 ETH + 20M STR - locked liquidity;
- 40 web categories will have: a minimum of 8000 ETH + 800M STR - locked liquidity;
- 270 web sub-categories.

Each sub-category will have in its liquidity pool: 50 ETH + 5M STR - locked liquidity; 270 Web sub-categories will have: - 50 ETH + 5M STR - locked liquidity: 13,500 ETH + 1.35B STR - locked liquidity Maturity Cap -minimum 21500 ETH + 2.15B STR - locked liquidity.

SourceLess - Business Solutions - Web Categories

1. 40 categories auctioned: starting bid 200 ETH /category + STR quantity of 20M STR

The amount paid to purchase a category will be matched by SourceLess with the corresponding amount of STR token for liquidity.

Category owner benefits:

- 40% revenue for business domain address sales - worldwide.

2. 270 subcategories auctioned: starting at 50 ETH / subcategory

The amount paid to purchase a subcategory will be matched by SourceLess with the corresponding amount of STR tokens for liquidity.

Benefits to the subcategory owner:

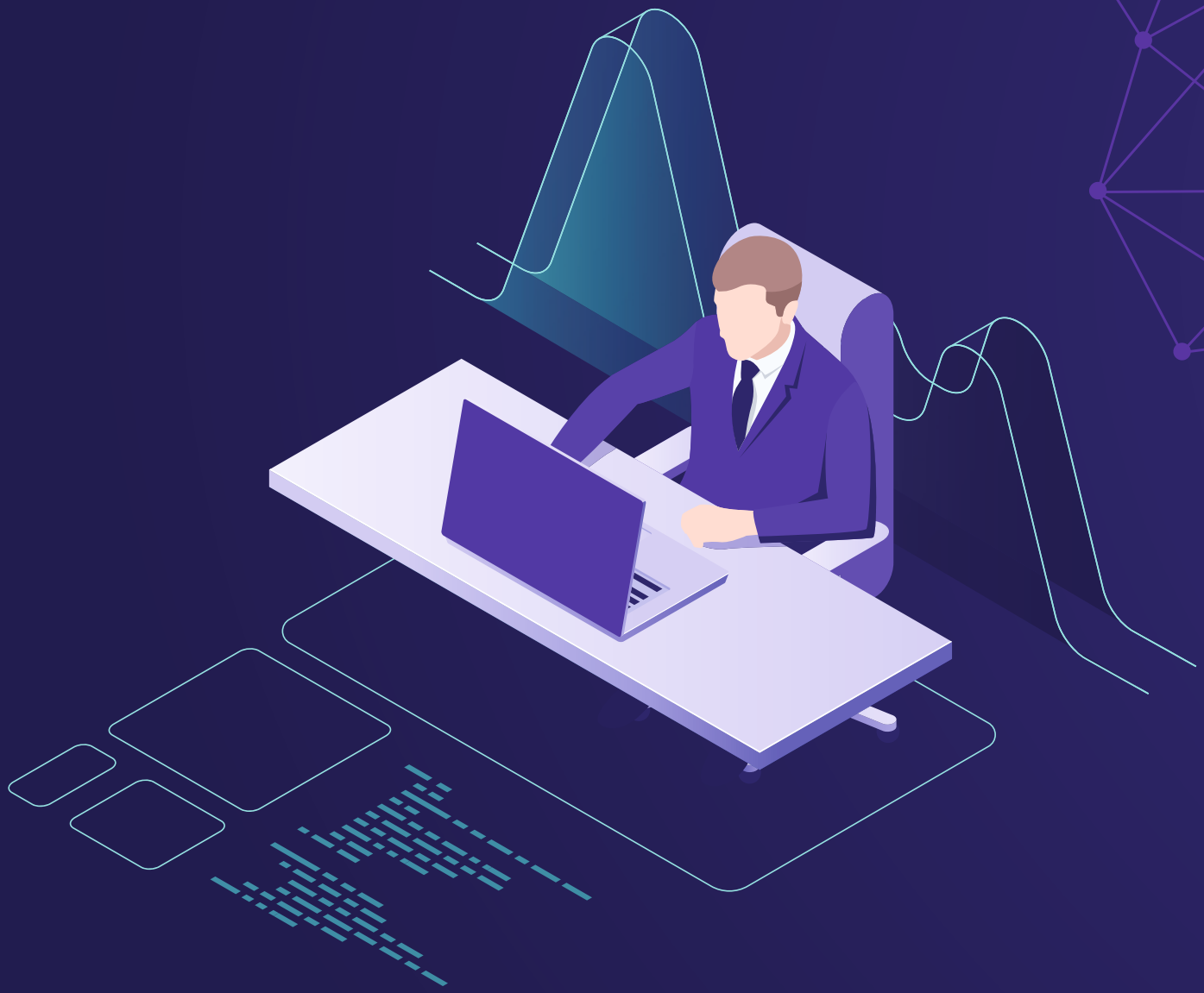
- 20% revenue for business domain address sales - worldwide.

SourceLess exchange:

0 TAX for any transaction made through SourceLess Exchange, regardless of currency (Bitcoin, Ethereum, Binance, etc.).

The uniqueness of a Str.Domain will confer maximum value to any domain, with the potential to grow any business by adding real value.

CHAPTER 6.
CASE STUDIES



CHAPTER 6. CASE STUDIES

CYBERSECURITY

In a report released in 2021, research firm Gartner forecast that global spending on information security and risk management services will jump to $150.4 billion this year, a gain of 12.4% from last year.

In the Gartner 2021 CIO Agenda Survey, cybersecurity was the top priority for new spending, with 61% of the more than 2,000 CIOs surveyed increasing investment in cyber/information security this year.

Security services including consulting, hardware support, implementation and outsourced services represent the largest category of spending in 2021, at almost $72.5 billion worldwide.

Information Security & Risk Management End User Spending by Segment, 2020-2021 (Millions of U.S. Dollars)

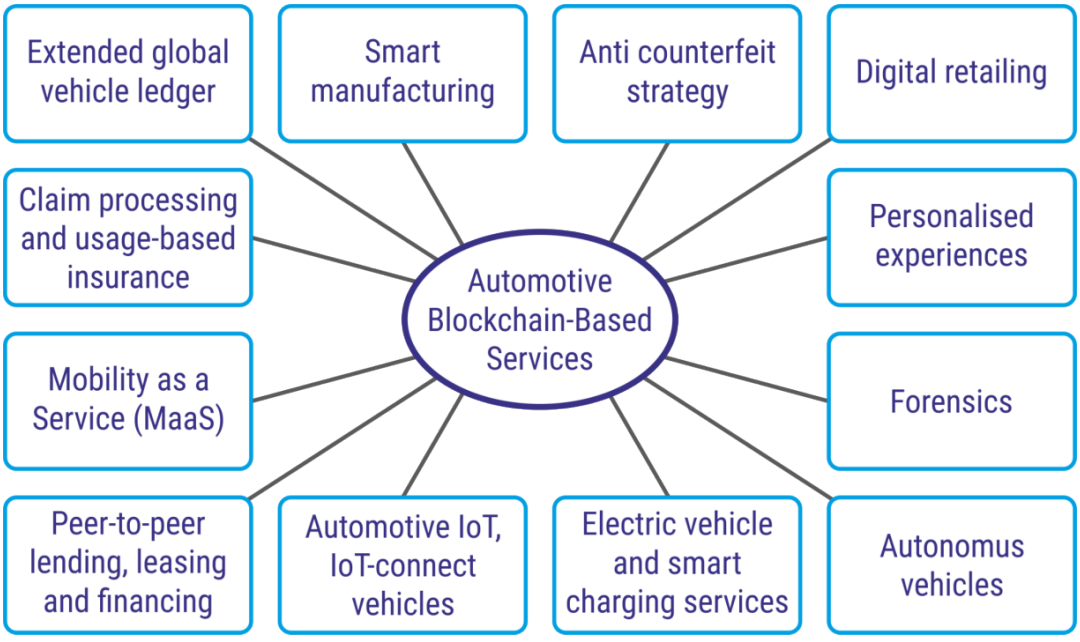
Market Segment	2020	2021	Growth (%)
Application Security	3,333	3,738	12.2
Cloud Security	595	841	41.2
Data Security	2,981	3,505	17.5
Identity Access Management	12,036	13,917	15.6
Infrastructure Protection	20,462	23,093	16.8
Integrated Risk Management	4,859	5,473	12.6
Network Security Equipment	15,626	17,020	8.9
Other Information Security Software	2,306	2,527	9.6
Security Services	65,070	72,497	11.4
Consumer Security Software	6,507	6,990	7.4
Total	**133,776**	**150,409**	**12.4**

Source: Gartner

www.gartner.com

May 17, 2021

THE AUTO INDUSTRY



While cars are getting closer to complete connectivity, electric and autonomous propulsion, the need for a well-developed and well-coordinated database increases. Also, the presence of technology in the manufacturing process of a car, can present a breach in security.

Lately it was not only shown that car theft is possible without the key in the ignition, but also manipulating various components of the vehicle while it is running, by people who have managed to breach the car's software.

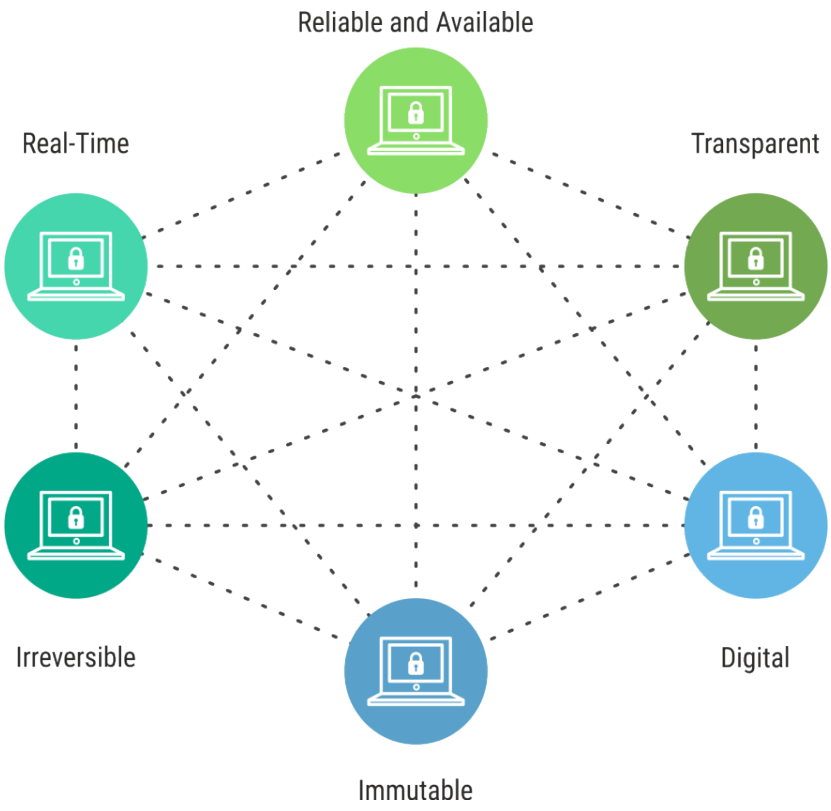
In 2015, an experiment performed by 2 IT experts has demonstrated that they can take complete control of a car from thousands of kilometers away.

SourceLess Blockchain allows for the installation of a node with a memory size below 1MB on the car's software in a way that any security issue will be cancelled, running in SourceLess Blockchain and not allowing any viruses or malware to execute.

Provisional Software Patent No.US63/294,483
ISO 20022 Compliant

If every car would have had a SourceLess Blockchain node (1 MB) preinstalled on the car's computer from the factory through the SourceLess Platform (str.domain), any eventual frauds and deficiencies that can show up could be verified:

- Changes to the real mileage;
- Changes to the car's parameters;
- Security;
- History of generic errors invalidated in the main computer;
- The unique digital identity of the property;
- The car history, regardless of the service where it was fixed;
- The instant reporting of the vehicle errors to the service;
- Reminders of the various legal inspections that need to be performed;
- Checks required in order to eliminate the risk of crashes;



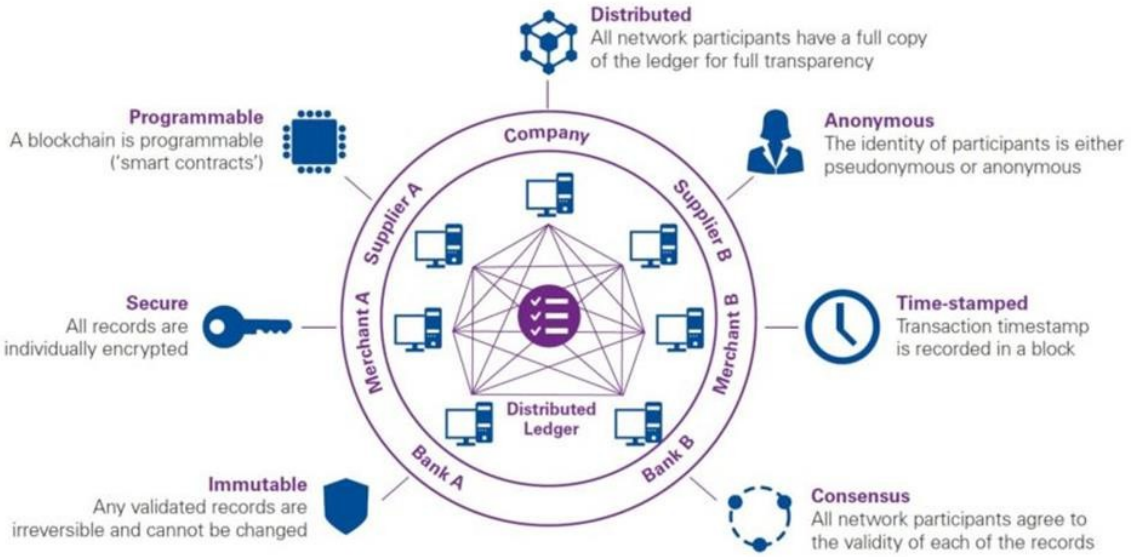
INSURANCES

The usage of SourceLess Blockchain through the SourceLess Platform allows insurance companies to introduce new innovative business models, to improve services, to optimize various operations and secure its entire network through encryption.

The SourceLess platform allows the complete control over all of the computers inside an insurance company, such that the company will streamline and maintain its network intact.

The SourceLess platform allows an insurance company to use all of the updated software within it, being able to choose the Public or the Private version based on the documents. Through the SourceLess Platform, insurance companies can utilize AI (artificial intelligence), being able to develop, improve and automate the current processes.

The Blockchain will introduce the security and transparency of the operations, helping companies in reducing costs and automate various operations. The combination of the blockchain with smart contracts and IoT can completely revolutionize the insurance sector and offer its users a transparent management system, incontestable and extremely responsible. It is enough to register any accord in the smart contract and to save it in the Blockchain, such that this will be automatically launched based on the terms previously established by both parties.



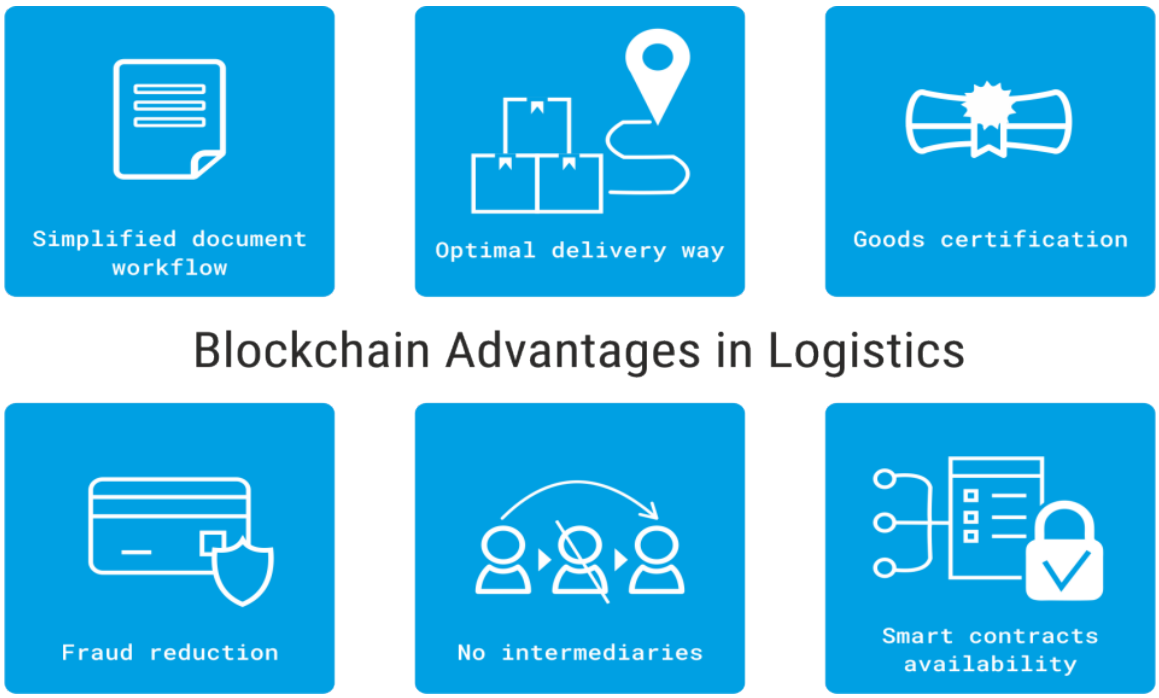
Through the SourceLess platform, any ensured good can

become a node in the SourceLess Blockchain network, thus having permanent awareness of its situation and with any fraud attempt being controllable.

If a car has a SourceLess Blockchain node installed, then the insurance company will be able to check all the LIFETIME technical data of the vehicle in real time. The same issues could be avoided in the case of house insurance or goods that can allow the minimum of connectivity (Alarms, Smart systems, etc.) through the SourceLess Platform. Through this method, potential frauds and litigations can be avoided.

The SourceLess Platform proves that it is capable of solving most problems, offering insurance companies and their partners a reliable and transparent instrument for the efficient capturing, storing, managing and utilization of data regarding vehicles and goods, thus removing potential frauds.

CERTIFICATION AND SCREENING OF GOODS



The manufacturers of goods from all around the world can use SourceLess Blockchain to create digital certificates for every product they have. This aspect can help both the consumers and the distributors to immediately detect the origin of a product, regardless of the reasoning behind the

request.

For example, such certificates can be used for food, which means that the route can be retraced in case a consumer finds an altered product or is simply not satisfied with the promised quality.

Through the same method, clothes and accessories (from standard to luxury items) can be certified in order to ensure not only their quality, but their authenticity as well. Thus, the number of counterfeit products on the market could be reduced.

HEALTH

Utilizing SourceLess Blockchain through the SourceLess Platform will allow medical companies to introduce innovative business models, improve services, optimize various operations, reduce cost, have complete security over their data through encryption and have total control over their network.

The SourceLess Platform allows full control over all the computers inside a medical company; therefore, the company will streamline and maintain its network intact, with the help of SourceLess Blockchain.

The SourceLess Platform allows a medical company to use all the updated software, being able to choose between the Public or Private version, based on the documents they are working with.

The SourceLess Platform offers the possibility of an instant connection between different entities of the medical field: Ministry-Company-Hospital-Doctor-Patient. Thanks to this, the useless bureaucracy is avoided, streamlining the process for everyone involved. For example, falsifying a patient's history will become impossible.

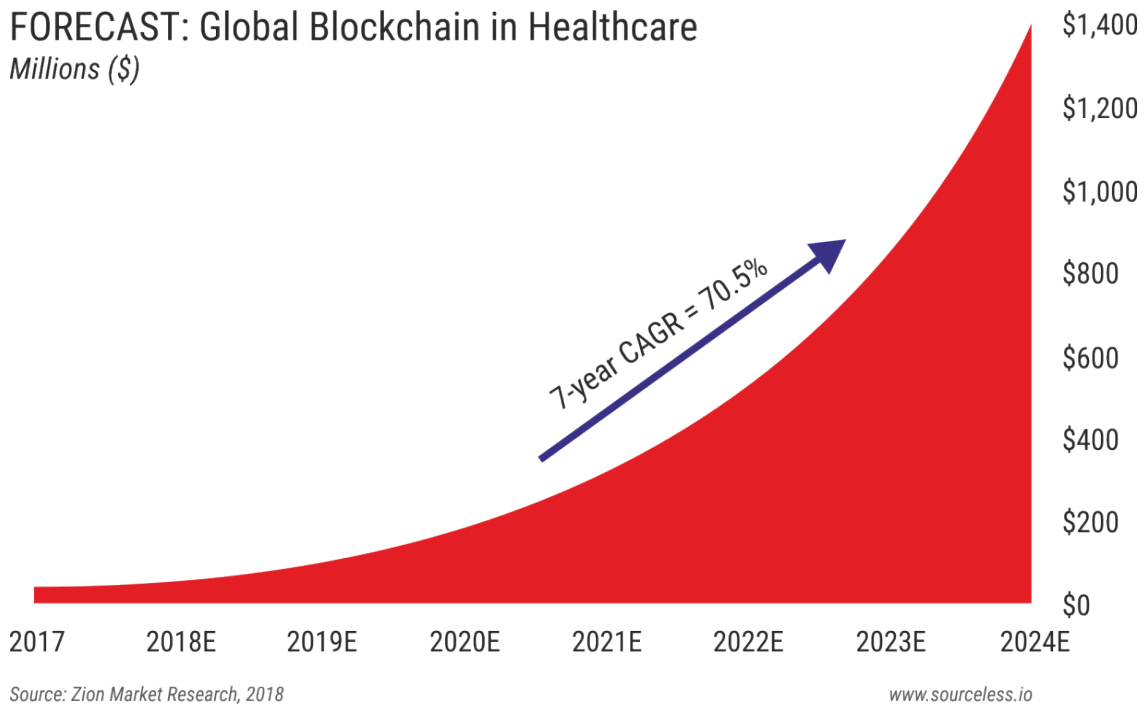
Medical research could benefit from AI software integrated in the SourceLess Platform, opening new horizons. Creating new patterns and methodologies through AI, the SourceLess Platform will allow everyone with permissions (private blockchain) to utilize, collaborate and put into practice.

The SourceLess Platform will allow the direct connection of the Medic to the Pharmaceutical systems (Health insurance

bureau - Pharmacy), thus eliminating any fraudulent attempt (digital signature) or system stoppage (the data of the patient is kept for life), basically thriving towards eliminating human error. The SourceLess platform will allow through AI software the development of treatment schedules that can be followed and updated based on the medication available on the market.

Taking into consideration all the data regarding the health of billions of people in the online field, the speed at which the information is processed by the AI and how fast this data is associated, will be reflected on the treatment practices.

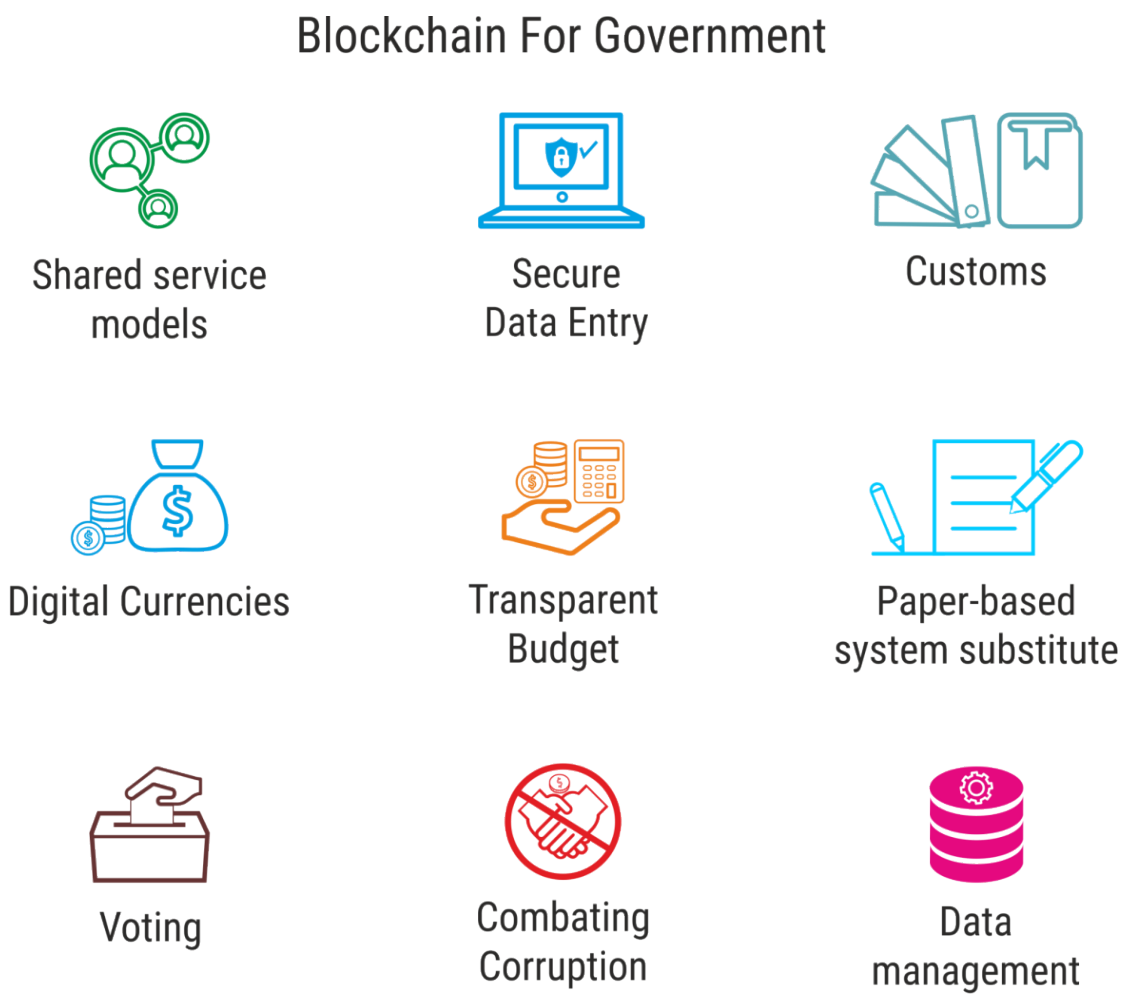
Pharmaceutical companies from around the world can use SourceLess Blockchain in order to create digital certificates for every product they have. This will help both consumers and distributors in finding and checking the origin of a product through the SourceLess Platform, regardless of the reason for the request.



THE PUBLIC SECTOR AND GOVERNMENTS

The public sector and governments which use the SourceLess Platform based on the SourceLess Blockchain network, benefit from the safety of data protection, streamlined processes, reduced fraud, waste and abuse, increasing in the meantime the trust and responsibility.

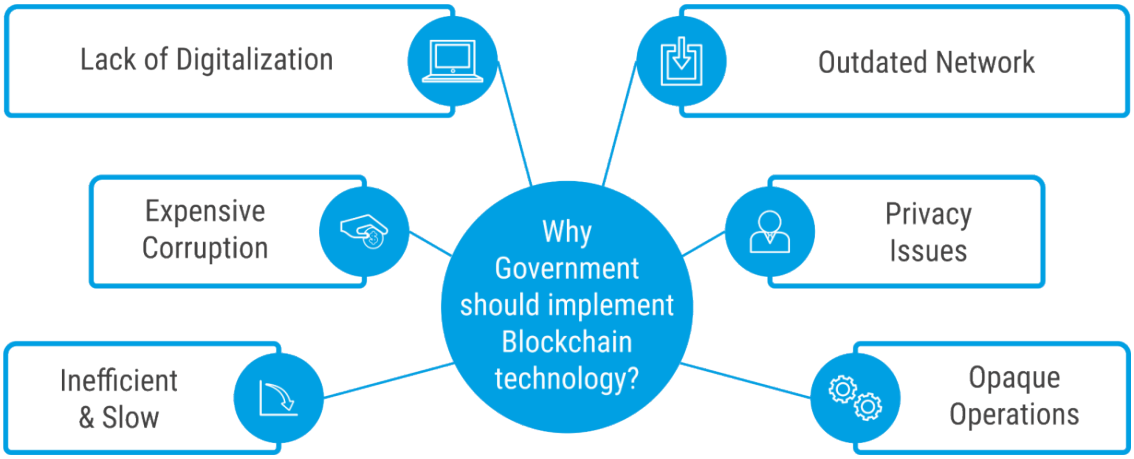
On a governance model based on the SourceLess Platform, individuals, governments and institutions share the resources through a registry distributed securely through encryption. This structure eliminates a single point of failure and inherently protects the citizen's and government's sensitive data. The SourceLess Platform can integrate all the software used by the central and local authorities, which can then be optimized and improved with the help of AI.



The SourceLess Platform used by governments and public institutions has the potential to solve inherited problems and allow for the following advantages:

- The safe storage of government, citizen and commercial data;
- Decreasing the number of work intensive processes;
- Reducing excessive costs associated with the handling of liability;
- Reduced potential for corruption and abuse;
- Increase of trust in the government and online civil systems;

The format of the shared registry can be used to support a series of government applications and from the public sector, including payments, registering of lands, identity management, supply chain tracking, healthcare, corporate registering, taxation of vote and the management of judicial personnel.



The SourceLess Platform ensures the following benefits:

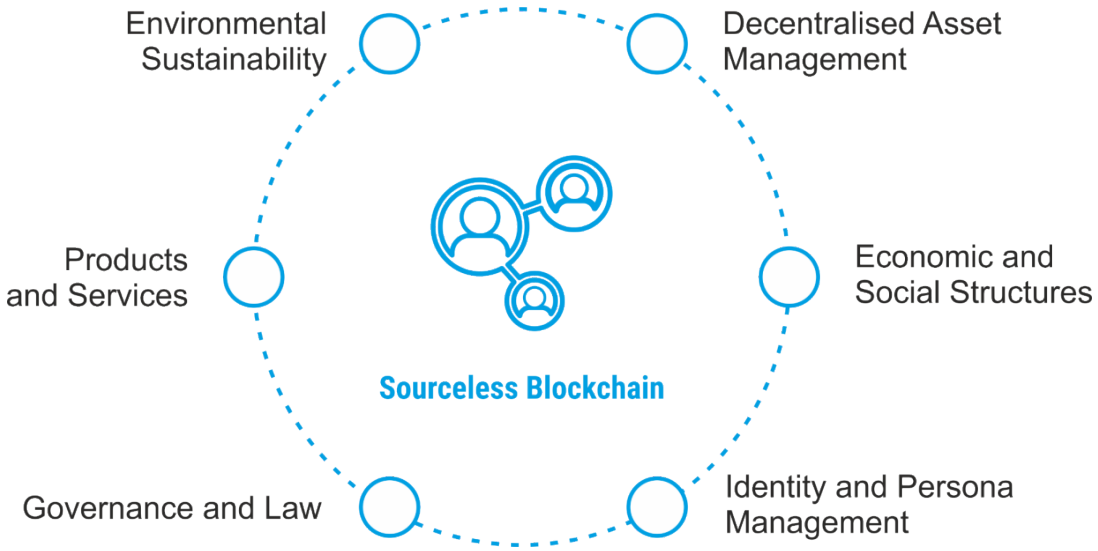
The proof of property rights and transfers

Land transactions and proof of ownership requests can encumber the government agencies with documents and administrative work.

By using SourceLess Blockchain, the governments can permanently stock active transactions such as lands, properties or vehicles, in a public registry.

In consequence, the government has greater transparency in land transactions, while interested citizens who are looking for a piece of land can gather the right information because all of the sales -actual and subsequent - are registered, marked and permanently stored.

This process can also reduce the possibility of corruption a lot, due to the implementation of the shared registry being safer by default.



Self-performing contracts

The traditional execution of legal contracts is expensive for both governments and their citizens. However, smart, self-executing contracts, enabled by the SOURCELESS PLATFORM, can eliminate the need for an intermediary and improve contract creation and execution. These contracts are publicly

accessible and secure within the network. The lack of an intermediary has reduced transaction time by over 90%.

Social benefits management

Government schemes that provide social benefits, such as unemployment, can be misused and infiltrated by certain individuals and groups, such as cyber attackers.

SOURCELESS PLATFORM can improve records management and provide protection against them although, privacy issues need to be addressed thoroughly. Keeping IDs and anonymized data in the employer database while storing the encrypted hash key (a fingerprint) in the SOURCELESS PLATFORM can help protect data.

With PLATFORMA SOURCELESS, a government can administer its retirement program with the additional benefit of reduced management costs.

Document validation

Governments are constantly looking for centralized, cloud-based solutions to validate documents for all their citizens, and SOURCELESS BLOCKCHAIN may be the solution.

SOURCELESS technology can store the hash values of citizen documents on the blockchain, allowing governments to provide a version of the document at any time permanently time-stamped electronic version of these documents.

Patent protection

Because the SOURCELESS PLATFORM can permanently tag transactions at any time, companies or individuals can file patents without experiencing the burdensome filing process. While the actual verification of the patent can take time, the stamp associated with the filing can help resolve many patent disputes and prevent costly lawsuits.

For example, in the SOURCELESS PLATFORM, a company could stamp a document before the full patent application and filing is submitted, so if a competitor tries to file a similar patent,

it is easy to prove original authorship of the creation in question. In addition, patent documents are given a transaction hash, providing encryption protection.

Security and fees

By using the SOURCELESS PLATFORM, authorities avoid any kind of cyber-attack, so losses of money, time and confidential data are automatically avoided.

In the wake of such attacks, CCTV systems in many cities have been hacked, and many of the essential data and images have been stolen.

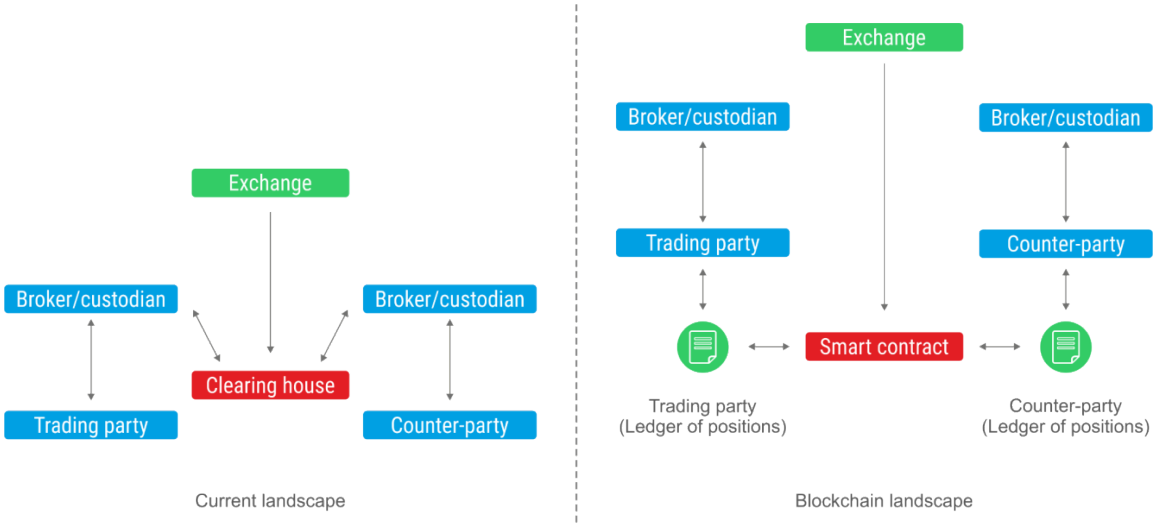
An integration of CCTV software into the SOURCELESS PLATFORM would mean total control of the stream of data and images. The traffic control system integrated into the SOURCELESS PLATFORM becomes stable without disturbances.

CAPITAL MARKET

Broadly speaking, there are four categories of market participants in the capital markets for whom SourceLess Blockchain-based solutions offer clear benefits.

The SourceLess Platform, based on the SourceLess Blockchain and AI software, will enable innovative solutions and the power of instant domain analytics.

Connecting into the SourceLess Platform will allow every entity to have instant access (public and private, depending on permissions) to any information and to verify in real-time the existence of any type of transaction.



For issuers

The SourceLess platform offers significant benefits to issuers, enabling easier, cheaper and faster access to capital through digital, programmable assets and securities. New securities can be issued in minutes, with corresponding rights and obligations codified and automated. This allows issuers to increase the speed of funding events.

The ability to schedule or encode terms and conditions into assets (in the case of securities issuance, for example) provides greater flexibility and customization than ever before. Blockchain technology can streamline KYC/AML processes and provide real-time updates and analytics with a single interface for investors, increasing transparency and efficiency.

One of the main advantages of digital assets is the ability to fractionalize each asset. Digital assets can be split into more affordable and transferable units, which creates an opportunity for greater liquidity and diversity for investors in certain markets. In addition, barriers to issuing an asset or security are significantly reduced, opening up greater opportunities for smaller issuers, while existing issuers benefit from new markets or forms of securities. Finally, the entire lifecycle of an asset has the potential to be automated from servicing investors to managing dividend events.

For fund managers

Fundamentally, SourceLess Blockchain enables peer-to-peer trading of any asset on a verifiable ledger. Funds benefit from faster and more transparent settlement and clearing, which reduces the risk of non-reimbursement in more solid markets. Faster processing means funds and managers have less tied-up capital and are able to use and allocate existing capital more efficiently. Funds will reduce costs from increased operational efficiencies, such as streamlining fund servicing, accounting, attribution and administration. Fees paid to third parties for services such as fund accounting and administration, transfer agency and even custody can be reduced or eliminated through automated fund services.

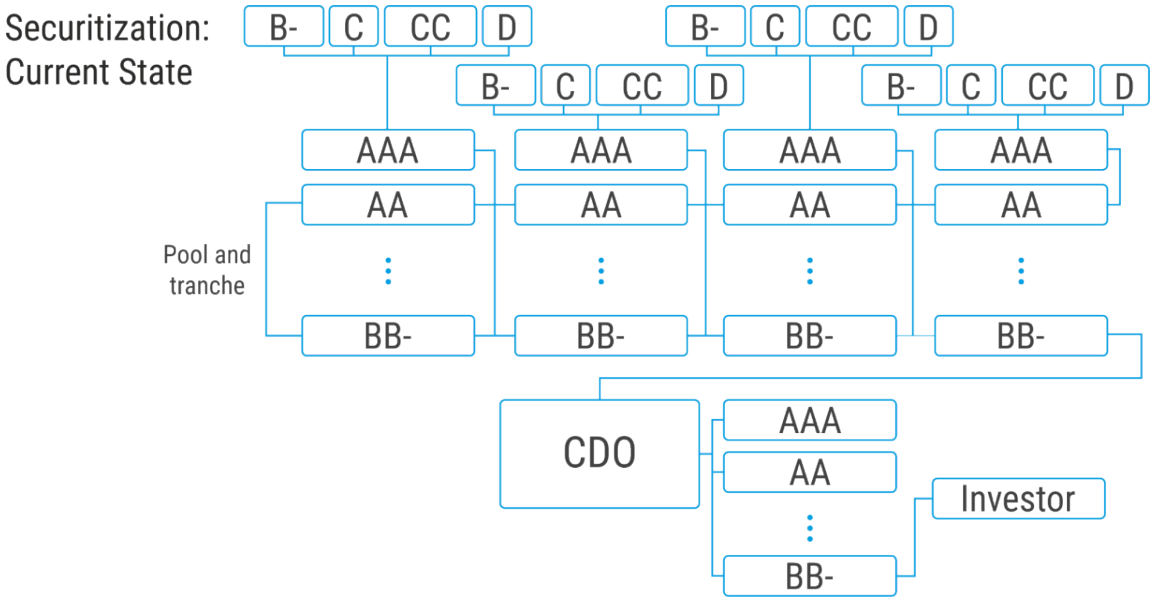
There will undoubtedly be many new types of financial products and instruments created, using the AI technology of the SourceLess Platform, which will in turn create new asset classes for capital attribution. While there will be an exploding array of financial products, most of these assets will share specific programmed standards, simplifying the structuring of new financial products or instruments.

The ability to issue digital assets and fractionalize existing assets will create a wider pool of investors, especially as newer investors are more comfortable with the idea of owning a portfolio of digital assets.

For investors

The SourceLess platform significantly reduces the barrier to issuing new assets or financial products. As the cost of issuing new securities decreases, and the speed of issuance consequently increases, issuers will be able to tailor new instruments to the personalized needs of each investor.

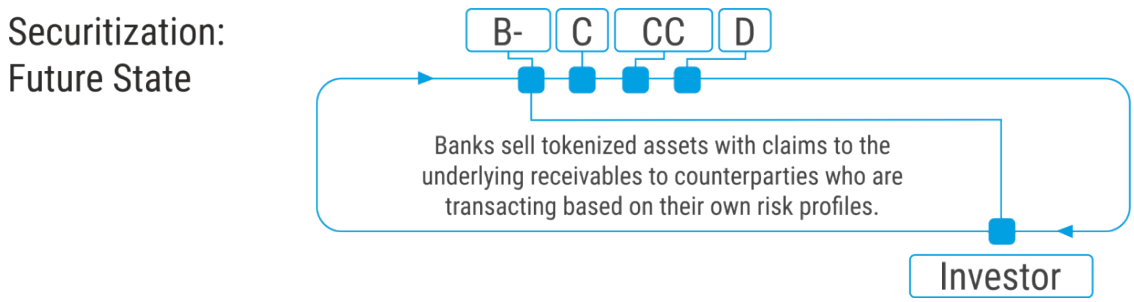
The improved ability to tailor investors' desire for yield, time horizon and risk appetite more precisely with customized digital instruments can have a profound impact on the investor-issuer relationship, creating a direct link between capital seekers and investors.



Investors seek to soften risk while increasing their potential rewards. One of the main risk factors is a lack of liquidity.

This is addressed by the programmable nature of digital assets and financial instruments, which allows for lower transaction costs, increasing the potential liquidity of an asset and enabling more comprehensive risk management. Combined with increased connectivity and efficiency in the capital markets, investors will see greater liquidity and a lower cost of capital.

In addition, the transparent and distributed blockchain ledger will enable reliable information on asset quality, which has the potential to improve the due diligence process.

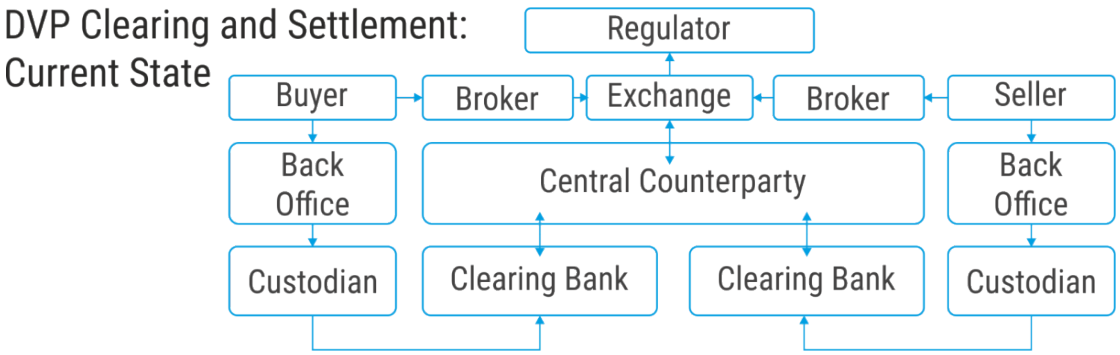


SourceLess Platform will enable risk integration and optimization through AI. At the same time, all current software systems that will work under the SourceLess Platform will be able to be interconnected through AI.

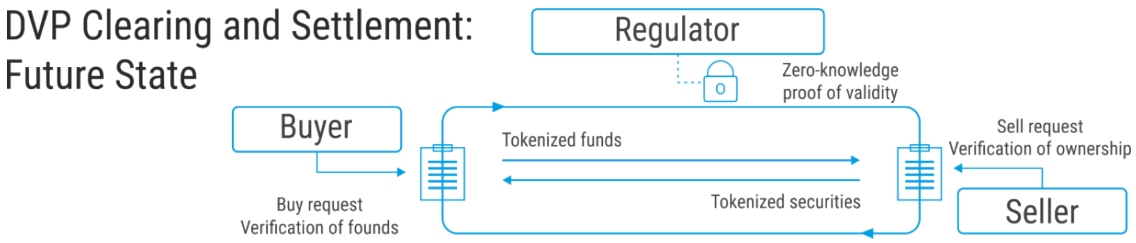
For regulatory

Securities regulators are often criticized for getting too involved in capital markets or not getting involved rapidly enough, as in the 2008 financial crisis. Government agencies and regulatory organizations can benefit from a distributed SourceLess Blockchain ledger which is transparent and verifiable at any time of the day.

The immutable nature of SourceLess Blockchain - transaction data cannot be changed - allows regulators to automate functions such as auditing and compliance.



As more institutions, investors and issuers use multiple blockchain networks to track their holdings and asset lifecycle events, regulators using the SourceLess Platform will be able to spend less time analyzing and predicting risk by learning the intricacies of each firm's system environment and customized representations of transactions.



The improved quality of data and disclosures enabled by the SourceLess Blockchain ledger will reduce overall costs and prevent potential systemic risk.

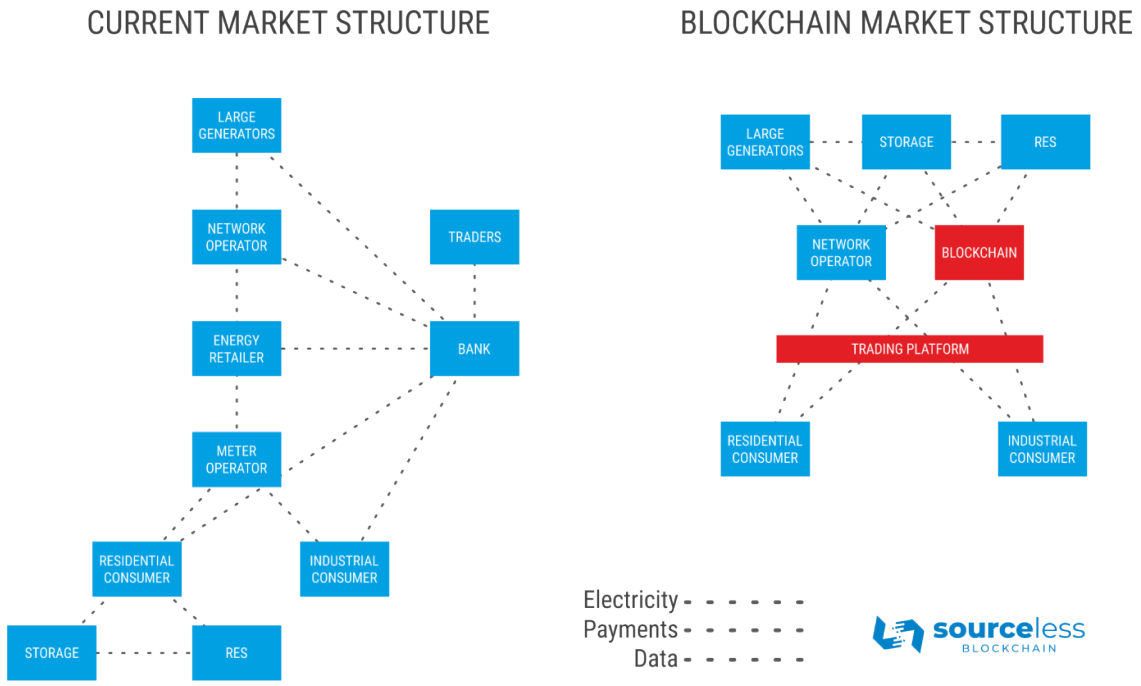
ENERGY MARKET

SourceLess Blockchain technology has the potential to transform the energy sector. The energy industry has been consistently catalyzed by innovations including rooftop solar, electric vehicles and smart metering, all of which can be enhanced and controlled through the SourceLess Platform.

The SourceLess Blockchain presents itself as the next emerging technology to drive growth in the energy sector through its smart contracts and system interoperability. Of the many use cases for blockchain, energy and sustainability are often less recognized.

However, the World Economic Forum, Stanford Woods Institute for the Environment and PwC have released a joint report identifying over 65 existing and emerging blockchain use cases for the environment.

These use cases include new business models for energy markets, real-time data management, and the transfer of carbon credits or renewable energy certificates to SourceLess Blockchain.



Distributed ledger technology has the potential to improve the efficiency of utility providers by tracking the chain of custody for network materials. Beyond source tracking, SourceLess Blockchain offers unique solutions for renewable energy distribution.

Long-established energy sectors such as oil and gas will also benefit from the implementation of SourceLess Platform solutions. Complex systems with multiple players have the opportunity to benefit from SourceLess Blockchain technology.

For example, oil is one of the most traded goods and requires a network of refineries, tankers, employees, governments and regulators. The complex network of participants suffers from isolated infrastructures and numerous inefficiencies along the way. Large oil and gas conglomerates are looking to invest in and implement blockchain technology because of its ability to reduce costs as well as its harmful environmental impact.

Oil and gas companies are particularly concerned about privacy and company trade secrets. The SourceLess Blockchain Network offers data permission and selective consortium permission to pre-approved parties.

The SourceLess platform connects all players in the energy market so each entity (public/private) will be able to access (depending on permissibility) different information.

The main benefits of Sourceless Blockchain in the energy sector are:

- Reduced costs;
- Environmental sustainability;
- Increased transparency for stakeholders without compromising confidentiality;
- SourceLess Blockchain is a carbon free ecosystem;

ENERGY DISTRIBUTION

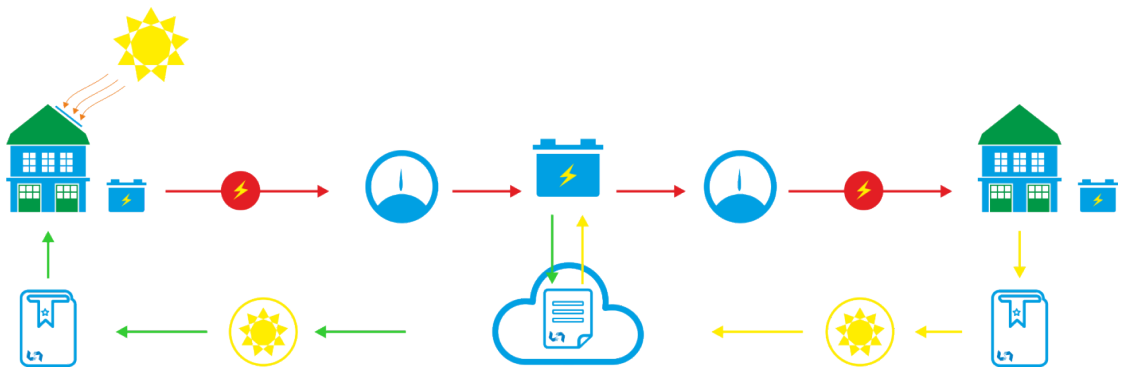
Companies looking to implement SourceLess Blockchain technology in wholesale electricity distribution are focusing on connecting end users to the grid.

The SourceLess platform through embedded AI will allow consumers to trade and buy energy directly from the grid rather than from traders.

The SourceLess platform through AI software becomes an exponent of the IoT, enabling control and efficiency of all components of a public/private, industrial/personal, producer/supplier energy system.

Supplementing merchants with the SourceLess Platform has the potential to reduce consumer bills by around 40%. By connecting users directly to the grid, the SourceLess Blockchain will allow users to buy energy from grid at the cost they want.

The result is a more equitable and stable energy market with lower electricity costs.



PEER-TO-PEER ENERGY TRADING

SourceLess Blockchain is a Peer-to-Peer Network

While wholesale energy distribution is a mainstream application for many companies, it is not the focus of all energy companies. Blockchain in Energy research by Wood Mackenzie shows that 59% of blockchain energy projects are building peer-to-peer energy marketplaces.

A peer-to-peer energy market is a shared network of people trading and buying excess energy from other participants. These energy markets benefit the masses because they reduce control from central authorities such as wholesale entities.

As more and more countries achieve energy parity, the cost of renewable energy becomes equal to or less than traditional energy for sale. People who produce their own energy will be able to trade it with their neighbors and peers. Australian-based company Power Ledger has connected communities together to create "microgrids".

Microgrids are a group of interconnected loads and distributed energy resources. Microgrids currently exist as a layer on top of the national grid; however, in theory they can be separate and self-sustaining.

MANAGING ENERGY CONSUMPTION

SourceLess platform can give consumers more efficiency and control over their energy sources. In addition, an immutable registry provides real-time updates of energy usage data. Efficiency and cost reduction is a goal of the SourceLess Platform through AI. Various types of energy data include market prices, marginal costs, energy compliance and fuel prices.

Data is often intentionally manipulated or misreported and omitted. The financial costs of intentional corruption and accidental administrative errors can be damaging to businesses and governments. In the spirit of transparency, the SourceLess Platform will allow the public to access records of transactions and prices. The transparency of public blockchains further reduces the chances of monetary or data mining.

ROBOTICS

Robotics is today's booming, multidisciplinary field and is spreading its roots deep into various fields of research, manufacturing industries, healthcare and even our everyday lives. However, as with any other evolving technology, robotics faces many challenges. In this context, blockchain technology has recently been identified as a promising technology to solve many of these problems, such as malicious/rogue node identification, malfunction/failures in automated processes, non-compliance with agreed privacy rules and regulations, security attacks.

Concretely, blockchain with features such as decentralization, immutability, provenance, low operational cost, strict access control and trusted operations, can provide significant improvements to new applications and use cases driven by robotics. Accordingly, the paper begins by exploring the key requirements and technical challenges faced by robots in general. It further provides a detailed overview of blockchain technology in a tutorial style.

Subsequently, the role of blockchain in different robotics use cases is analyzed. In addition, various technical challenges that need to be mitigated in order to harness the

full potential of blockchain for robotics are highlighted. Finally, future research directions that can pave the way forward for advances and profitable integration of blockchain in robotics are presented.

This is an area where SourceLess Blockchain technology offers a credible solution through the SourceLess Platform.

The SourceLess Platform enables the integration of any system and software in robotics, providing both SourceLess Blockchain security and AI integrated into the platform.

Swarm robotics is seen as an area where the combination of blockchain and AI can benefit the technology. The field consists of multiple physical robots working together in a "swarm" to perform tasks or operations. In this field, each robot is powered by AI to interact with its environment, following pre-determined rules. When these robots are connected, their collective behavior and interactive capability becomes robust and highly scalable.

By using the SourceLess Platform, based on the SourceLess Blockchain network of advanced encryption techniques such as cryptographic digital signatures and cryptographically secure public key cryptography, the SourceLess Platform provides optimal security for data across shared channels. Information accessibility is controlled by the specific private key available to a bot. While artificial intelligence-based robotics has emerged as a cutting-edge technology, blockchain empowers robotics with an optimal security solution.

A perfect elaboration of these problems and how they are solved by SourceLess Blockchain is detailed in the paper Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision-Making Scenario by:

- *Volker Strobel IRIDIA, Université libre de Bruxelles Brussels Brussels, Belgium vstrobel@ulb.ac.be*
- *Eduardo Castelló Ferrer MIT Media Lab Cambridge, Massachusetts, U.S. ecstll@media.mit.edu*
- *Marco Dorigo IRIDIA, Université libre de Bruxelles Brussels Brussels, Belgium mdorigo@ulb.ac.be*

AI IMPROVES BLOCKCHAIN

Saving energy: mining data requires huge computing power, and AI can be very efficient in monitoring this consumption;

Scalability: blockchain scalability can be used by AI to make room for decentralized learning and other processes;

Optimizing security: although blockchain is highly secure and tamper-proof, machine learning and deep learning technologies can make applications even more secure by running alongside blockchain;

Efficiency: AI can provide efficient use of resources to minimize costs associated with blockchain;

Hardware: data miners using blockchain technology continue to make investments on the hardware side. This is compounded in particular by the use of specialized hardware components. AI can play a tremendous role in procuring more efficient systems and capabilities.

Meeting talent needs: there are still very few experts and professionals working in the blockchain technology space. As the talent gap grows and demand for blockchain implementations steadily increases, AI-powered virtual agents can play a critical role in various tasks, such as creating new ledgers on their own.

Data verification: while the growing volume of data used in blockchain always makes personal data and privacy vulnerable, AI-powered screening and data gates can help monitor access to private data;

Provisional Software Patent No.US63/294,483
ISO 20022 Compliant

ACADEMIC SECTOR

The education industry faces the same challenges that have been dragging it down for years. These include inefficient paper record-keeping processes, lack of transparency, poor student and teacher accountability, lack of real motivation for students to learn and perform well in the classroom, and lack of trust in educational merit and academic credentials due to recurrent falsification of them.

The SOURCELESS PLATFORM can have a major impact on education and address these challenges by providing tangible solutions described in detail below.

Improved records and transparency

Using the SOURCELESS PLATFORM, the school registrar's office needs to create a one-time student record, this digital identity will then allow them access throughout the education system. After that, it becomes accessible to all participants in the education system and can even be shared between institutions.

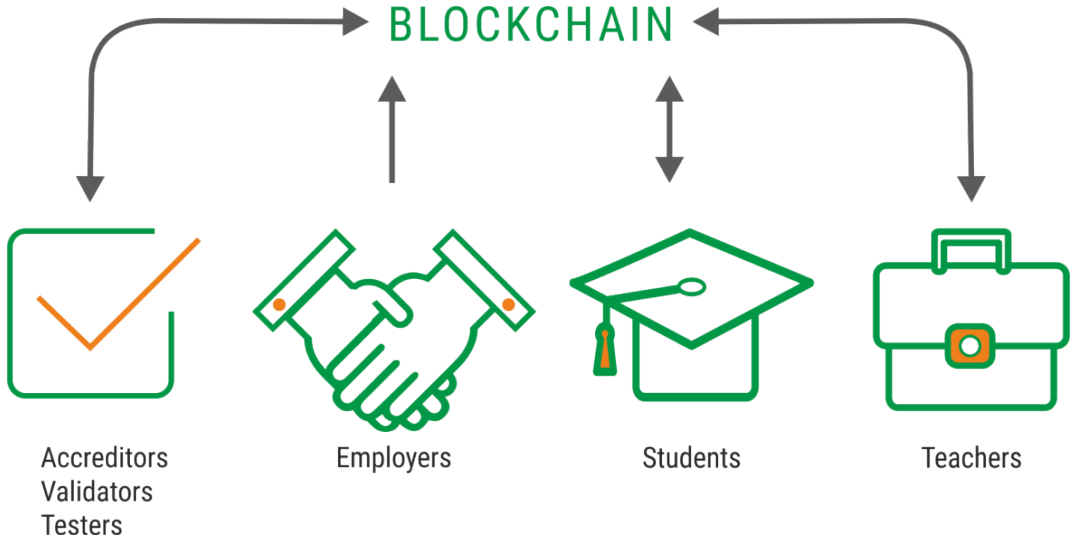
Each assignment, participation in curricular and extra-curricular activities are attached to the student's digital registration in the SOURCELESS PLATFORM in the student profile. This gives teachers, counsellors and school administrators a direct view of their students' progress.

In addition to maintaining student records, SOURCELESS PLATFORM can be used to oversee and facilitate accreditation of schools, colleges and universities to protect intellectual property rights and eliminate diploma and transcript forgery.

Educational records in SOURCELESS PLATFORM can be easily accessed and quickly transferred to other institutions and organizations, including potential employers.

A student's digital identity in SOURCELESS PLATFORM and the information that is entered into their subdomain is confidential data protected by the BLOCKCHAIN SOURCELESS network and can only be accessed by those with permission.

This type of system ensures complete authenticity of credentials and student records, as the complete history of signature changes is stored on the blockchain.



Student responsibility

Each assignment participating in curricular and extra-curricular activities are attached to the student's digital record in the SOURCELESS PLATFORM in the student profile. This gives teachers, counselors and school administrators a direct view of their students' progress. Through the SOURCELESS PLATFORM's Str.Talk CHAT, it will be possible to create work rooms, workspaces where each student will be able to resolve and upload/upload all required documents.

Each student will be permanently connected to all the information concerning him/her through the SOURCELESS PLATFORM (chat, blog, courses, workrooms, video), thus eliminating human error and having everything available for the development of the students' capabilities towards the desired career.

Future employers or sponsoring companies have the possibility to check in real time the student's activities, analyze performance and see the student's progress over time via the SOURCELESS PLATFORM.

Stimulating students and teachers to achieve better results

Token credits can be used to create effective reward systems that motivate students and encourage teachers to contribute to the educational process by creating new learning materials and participating in research. Smart contracts can be programmed to issue credit awards for completed tasks. Teachers will be able to further incentivize students by giving special credit to high performers.

Teachers will be able to be monitored through the SOURCELESS PLATFORM so they can be integrated into an award scheme.

SOURCELESS PLATFORM through AI can monitor and analyze the progress of all students and teachers, thus allowing the management of the educational institution to award prizes through token-credits.

SOURCELESS PLATFORM takes full advantage of the gamification element in modern education and can take it to the next level with tokenized credits, which can be used to pay off student loans, buy school supplies, teaching materials and cover other educational expenses. Rewards for graduating from a particular major and receiving a degree from the university could significantly reduce the number of students who drop out with no intention of returning to school.

Developing the learning environment and teachers

SOURCELESS PLATFORM will enable all teaching staff to use software and AI to better convey information, streamline the teaching process, structure and simplify assessment methods. With PLATFORMA SOURCELESS teachers will have all the attributes of modern communication at their disposal: chat, video, blog, work rooms, conference facilities.

SOURCELESS PLATFORM will allow all educational institutions to be connected so that information and data exchange between teachers will become a formality. Development or research groups will have access to the power of the SOURCELESS PLATFORM based on the SOURCELESS BLOCKCHAIN network.

On a global scale, the SOURCELESS PLATFORM could aggregate district, state and national performance statistics and increase healthy competition among schools, colleges and universities with the ultimate goal of providing the best education.

Through the SOURCELESS PLATFORM teachers can create new study patterns, new assessment techniques, new courses for a better level of efficiency in Romanian education and beyond.

Introducing student transcripts, verifiable for life

We've all been through the trouble of getting student transcripts from educational institutions. It is a time-consuming process, involving several parties to check credentials and compile the complete academic record.

SOURCELESS PLATFORM provides students with an online digital transcript, available whenever they need it. This verifiable transcript throughout the student's life could contain information about all educational achievements and streamline credential verification, making it easier for students to transfer between schools.

Providing students with a portfolio of educational achievements

The SOURCELESS PLATFORM allows students to create their own digital portfolios that would store all their educational merits such as:

- Major/minor degrees earned;
- Proven competences through experience;
- Certificates of completed courses;
- Micro-certificates for achievements;
- Additional credits and awards;
- Test scores and attendance records;

This portfolio can be shared publicly to prove a student's worthiness to enroll at a university or can be sent to an employer by a student seeking an employment opportunity.

Ultimately, a universal database of potential candidates could be created, and top-performing students could be sought out by companies, creating even more incentive to perform at school.

University management

The governing bodies of educational institutions will have the SOURCELESS PLATFORM with AI help to streamline expense management, eliminate human error, develop new curricula, and control institutional problems.

Research programs will be able to be evaluated by MANAGEMENT through the SOURCELESS PLATFORM. The SOURCELESS PLATFORM will allow the integration of all the software an educational institution works on.

Management through the SOURCELESS PLATFORM will be able to grant each participant in the system a certain degree of permissiveness, so that each participant will only have access to the information necessary to carry out their work.

Evaluation of employees will become an easy task with PLATFORMA SOURCELESS because all objectives of each student will be monitored by PLATFORMA SOURCELESS with the help of AI.

Internal security (alarm systems, fire systems, CCTV, etc.) is an area that SOURCELESS PLATFORM with AI takes to another level, all based on the SOURCELESS BLOCKCHAIN network.

SOURCELESS PLATFORM will allow the interconnection of all educational institutions, with educational collaboration being just a click away, research collaboration being perfectly transparent and efficient, and collaboration and curriculum completion being achieved with AI. Exchanges of experience (students/teachers, internal/external) are now made easier with the SOURCELESS PLATFORM, with all participants connected to the same system.

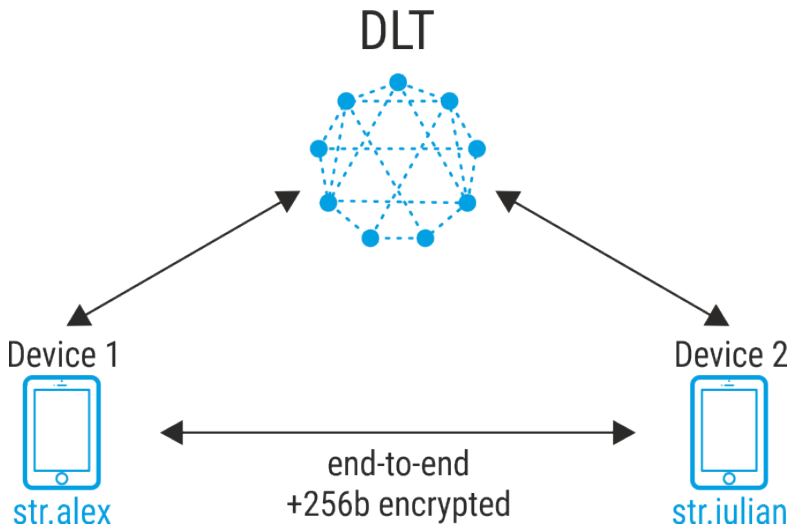
SOURCELESS PLATFORM will be made available to the TEACHING SYSTEM free of charge, SOURCELESS BLOCKCHAIN being a CARBON FREE system.

STR.TALK
(Communication)

STR.TALK (Communication)

Str.Talk is a social media platform built on the SourceLess Blockchain. The platform will use the peer-to-peer system without the help of a central administrator so participants (computers, mobile phones, etc.) are linked together with equal permissions and responsibilities for data processing.

The functionalities of Str.Talk platform are similar to the well-known social media platforms already in existence: Facebook, Twitter, Instagram, etc. Instead, information will be encrypted and sent strictly between participants, without going through a central administrator, avoiding information interception and data/identity theft.



Each user will have a Str.Domain (WNFT) identifier, a unique and non-interchangeable datum stored on a digital ledger. This solution will provide all Str.Talk and SourceLess users, of course, with privacy and data security, becoming owners of their own domain/account.

Basically, Str.Talk is at the core of a p2p (peer-to-peer) social media communication platform, which tailors its options and functionality to the user. Whether this user is an individual or a company, an NGO or a university, the features of this platform will be optimized according to the industry to which the user belongs.

SourceLess Blockchain Board Members

ALEXANDRU STRATULAT
Founder

alex@sourceless.io
+40 727 338 819

IULIAN BONDARI
Co-Founder

iulian@sourceless.io
+40 736 595 004

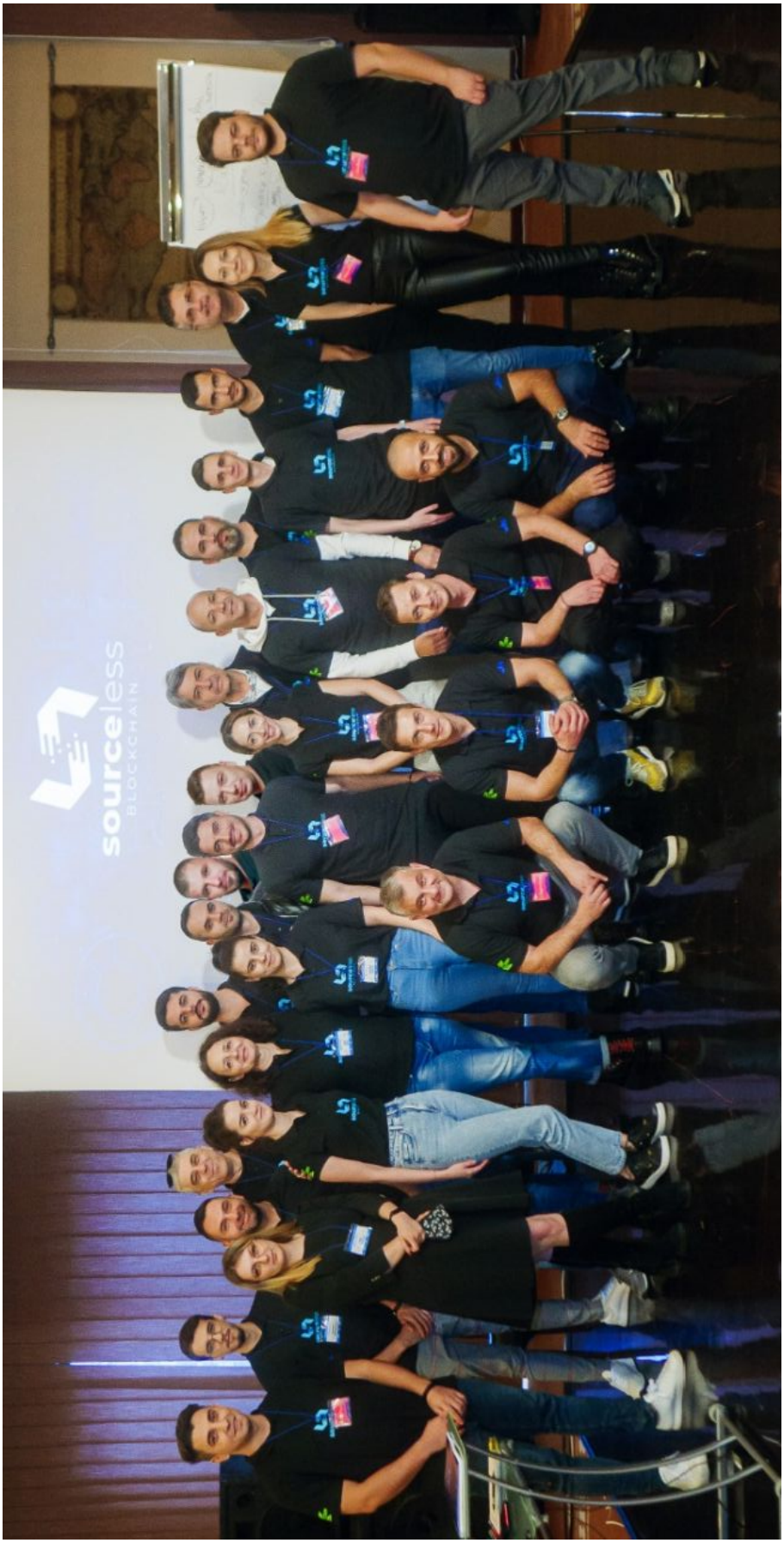
BOGDAN VOINEA
Co-Founder

bogdan@sourceless.io
+40 763 600 637

Sourceless Inc.

www.sourceless.io

Provisional Software Patent No.US63/294,483
ISO 20022 Compliant


sourceless
BLOCKCHAIN