



#ESERPTrabajandoDesdeCasa
#ESERPLiveStreaming

Blockchain N. 1

Avv. Maria Bruccoleri
[www. avvocatobruccoleri.it](http://www.avvocatobruccoleri.it)
Linkedin: <https://www.linkedin.com/in/maria-bruccoleri-648440135/>

ESERP Business & Law School
C/ Costa Rica 9. 28016 Madrid
www.eserp.com

Piazza A. Diaz, 6
Milano, 20123
Cell 328 8871062
E-mail: studiolegalebruccoleri@gmail.com

Studio Legale
Avv. Maria Bruccoleri

Via Gioacchino di Marzo 5
Palermo, 90144
Tel. 091 309131
Tel/Fax 091 308038
PEC: avvmariabruccoleri@legamail.it

BLOCKCHAIN PRESENTATION

SLIDES DESCRIPTION

www.avvocatobruccoleri.it

In this slide, we will be listing the important topics that we are going to cover in the blockchain presentation. The topics will include the following.

1. What is blockchain technology
2. Must know blockchain terms
3. Smart contracts
4. Blockchain digital transformation
5. Impact of blockchain on the world

WHAT IS BLOCKCHAIN?

- The blockchain is defined as an open ledger that offers decentralization to the parties. In addition, it also offers transparency, immutability, and security. It has many features including being open, distributed, ledger, P2P and permanent.
- Blockchain term was first introduced in the white paper of Bitcoin in 2009 by Satoshi Nakamoto. From there, it has come a long way as more and more organizations are interested in it. Right now, Bitcoin is on its way to implementing lightning network and other advanced features.

HOW DOES A BLOCKCHAIN WORK?

The function of a blockchain is straightforward. As it is a peer-to-peer network, a user needs to start a transaction. Once done, a block is allocated to the said transaction. The transaction block is also broadcasted to the network, and all the nodes in the network get the said information. The block is then mined and validated. It is also added to the chain, followed by a successful transaction.

REMARKABLE BENEFITS OF BLOCKCHAIN TECHNOLOGY

Blockchain technology is feature-rich. It is also extremely beneficial. For example, it lets the user do faster settlement compared to traditional methods. It is also immutable and more secure. When compared to a traditional network, blockchain technology is more capable and have improved network capacity. With decentralization built-in, it can be used to build a shared and distributed blockchain.

PUBLIC VS PRIVATE BLOCKCHAIN NETWORK

The slides discuss the difference between public and private blockchain network. The main difference between them is how they function. Public blockchain network is permissionless whereas the private blockchain is permissioned one. This means that the public blockchain is an open network which is not controlled by anyone. Anyone can access it. The private blockchain, on the other hand, is permissioned which means that there is an authority that manages who can use the network.

CENTRALIZED VS DECENTRALIZED VS DISTRIBUTED NETWORK: AN OVERVIEW

There is a vital difference between centralized, decentralized and distributed network. That's what the slide is all about.

- *Centralized:* All the nodes come under a single authority
- *Decentralized:* There is no centralized authority and everyone can take part in the network.
- *Distributed:* Independent nodes interact with each other. Also, each node is interconnected.

MUST KNOW BLOCKCHAIN TERMS

It is hard for a beginner to know blockchain terms and this can easily make them confused. This slide list 10 important must know blockchain terms out there. For example, it covers bitcoin, airdrop, dApp, ICO and others.

SMART CONTRACT EXPLAINED

Smart contracts are similar to a legal document and create terms between two parties. The two parties that are dealing with using smart contracts. Also, the contracts use public ledger for storage purposes. Smart contracts are triggered when a condition is met, and are completely autonomous. It just executes based on the code that defines the pre-condition. To make sure that they work as intended, they are analyzed and managed by regulators. It is also helpful in understanding trends and predicts market uncertainties.

HOW DO SMART CONTRACT WORK?

- Smart contract works between two parties. It is used to do buyer and seller matchmaking. Furthermore, it can be used for transactions. Banks and other institutes can use smart contracts to receive assets and distribute it.
- The three key features of smart contracts include registered, automated settlement of contracts and there is no need for the third party

ADVANTAGE OF SMART CONTRACTS?

The slide discusses the advantages of smart contracts. The few advantages include total transparency, no paperwork, total transparency, trustworthy, guaranteed outcomes and so on.

DISADVANTAGES OF SMART CONTRACTS

- Smart contracts are not free from disadvantages. It does have some disadvantage. Few of the major disadvantages include error, confidentiality and rouge contracts.
- Smart contracts are made up by humans. This makes them open for human-errors. Also, they are not 100% confidential. It can leak some vital info which can be read by a 3rd party. Not only that, there are rouge contracts that can act like a real one and make fraud possible.

SMART CONTRACTS USE CASES

There are many uses cases for smart contracts. They can be used in different verticals, and can also be used to make things efficient. Few of its main uses cases include trading activities, supply chains, copyright protection, real estate market, government voting, and so on. It also has very useful use cases in Internet-of-things(IoT) where it can help protect the network as well.

IS THE BLOCKCHAIN OVERHYPED?

Is the blockchain overhyped? It is one of the biggest questions that need to be addressed. The general population doesn't understand what blockchain has to offer. This leads to assumptions and many calling it overhyped. Right now, the blockchain technology is not yet one decade old. We have already crossed the disappointment phase and are moving towards a better implementation in the future. Bitcoin, for example, will see new updates soon. Other blockchain technologies are also innovating at a rapid pace.

VERTICALS OF BLOCKCHAIN TRANSFORMATIONS

- Currently, the whole industry is going through a blockchain transformation. Its impact is seen everywhere. That's why the slide shares the nine verticals of blockchain transformation. They include the following:
 1. Technology
 2. Law and Crime
 3. Government Service
 4. Finance
 5. Human Rights
 6. Entertainment
 7. Media
 8. Transportation
 9. Contracts

2017-2018 LEADING SECTORS

- There are also many sectors that are leading in the blockchain technology implementation. The two sectors that are leading the most include Fintech and supply chains. However, that's not all as there are other sectors which are slowly but steadily adopting blockchain technology including healthcare, shipping, retail, insurance, and mining. With time, we will see almost every sector to use some form of blockchain technology. Few sectors will see better implementation due to better suitability than other sectors.
- Enterprises are very keen on implementing blockchain

WEB 3.0: THE SUCCESSOR OF WEB 2.0

Blockchain will also begin Web 3.0 which is the 3rd generation of the internet. The internet will take advantage of the blockchain network and bring a truly decentralized network that is way more advanced than what we have right now. The current web is more focused on server-based databases and hence provide limited functionality. The new internet will be more focused on users which means that it will be better connected and offer a secure platform for everyone out there.

WEB 3.0 BENEFITS

This slide continues with the topic of Web 3.0 and lists Web 3.0 benefits. As discussed earlier, Web 3.0 offers better functionality and features. It will be permissionless which means that there will be no centralized authority controlling it. It will also be free from any monopoly and will also provide tons of privacy to the users. The network is secure, and the data ownership stays with the end users who can keep it to themselves or sell it to the media companies. The Web 3.0 will also be ubiquitous and offer a semantic web.

REMEMBER: CENTRALIZED VS DECENTRALIZED INTERNET

- The core difference between the centralized and decentralized network is the absence of central authority. It is a decentralized internet which has its unique data flow, new business models and dApps. The slide also presents the difference in a visual way.

WEB 3.0 ECOSYSTEM

In the end, we will get a Web 3.0 ecosystem will be better and offer a wide variety of services. The slide list the different components of the ecosystem and gives you a glimpse of what you can expect from the Web 3.0. Each component or service is also presented with an example which gives you a glimpse of what to expect from Web 3.0.

BLOCKCHAIN VS DATABASE

- The blockchain is decentralized which also stores data. However, it is different from databases. In this slide, we discuss the blockchain vs. database topic. The four categories in which they differ include writing access, cost, integrity, and trust. The major difference is, of course, the absence of a centralized authority. Data written on blockchain is also immutable which in turn provides integrity. The database, on the other hand, offers you CRUD operation. There are also significant differences which are covered in the slide itself.

DIFFERENT TYPES OF TOKENS

In this slide, we discuss different types of tokens. They include currency, asset, utility, and equity tokens.

CONCLUSION

This slide not only covers the introduction to the blockchain but also introduces the reader to different new concepts, ideas, and information.

- A Blockchain is a type of diary or spreadsheet containing information about transactions.
- Each transaction generates a hash.
- Each block refers to the previous block and together make the Blockchain.
- A Blockchain is effective as it is spread over many computers, each of which have a copy of the Blockchain.

- In the simplest terms, Blockchain can be described as a data structure that holds transactional records and while ensuring security, transparency, and decentralization. You can also think of it as a chain or records stored in the forms of blocks which are controlled by no single authority.

- A blockchain, originally block chain, is a growing list of records, called blocks, that are linked using cryptography.
- By design, a blockchain is resistant to modification of the data. It is “an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way”.

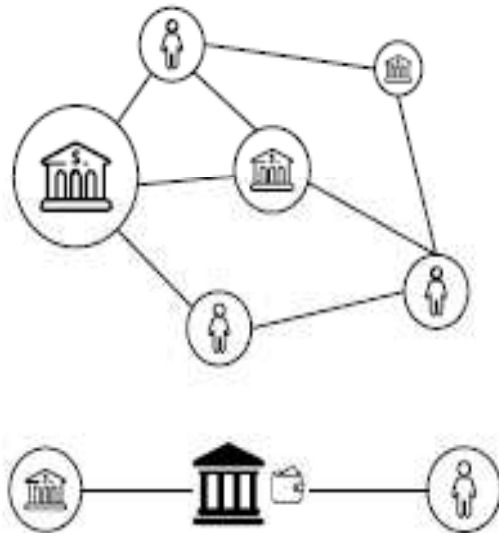
Decentralized consensus has therefore been claimed with a blockchain.

Blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin.

The identity of Satoshi nakamoto is unknown.

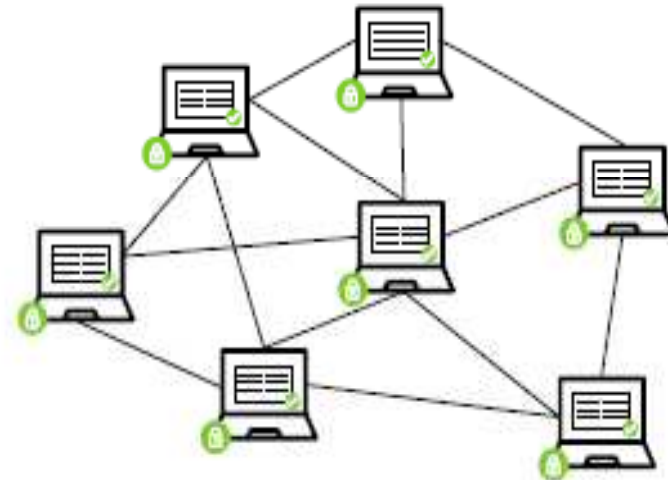
WHAT IS BLOCKCHAIN

Current Financial System



- Central authorities (bank, fed, notary, escrow, etc.) transfer actual value between two parties
- Multiple intermediaries and record-keeping are required to facilitate transfer of assets and create trust

BlockChain System



- Distributed network of computers (nodes) that maintain a shared source of information
- Transaction data is immutable
- Peer to Peer transactions using digital tokens to represent assets and value

BLOCKCHAIN VS BITCOIN



Bitcoin

- A digital currency which was in a lot of ways the first demonstrable use of BlockChain
- A protocol that supports a decentralized, pseudo-anonymous, peer-to-peer digital currency

BlockChain

- Distributed
- Secure
- Log file

INTRODUCTION TO BLOCKCHAIN

A **BlockChain** is a distributed secure log file or **shared ledger** with technology to trust transactions without a central authority

A **shared ledger** technology allowing any participant in the business network to see the **established (via distributed consensus) system of record (ledger)**

Each **peer address is anonymous** and **multiple addresses** may map to the same transactor



Every **viable transaction** is stored in the **shared public ledger**

Transactions are placed in **blocks**, which are linked by **one way hashes**

Operates in a **peer to peer mode** and is mostly based on DNS and **"seed nodes"**

WHAT IS BLOCKCHAIN

A Brief Intro:

- **BlockChains** are essentially facilitated on a platform of distributed databases with some inbuilt pre-agreed technical and business logic criteria, kept in sync via peer-to-peer mechanisms and pre-agreed consensus algorithms. These are the BlockChain Ledgers.
 - **Data stored on BlockChains are considered Immutable.** Immutable means that something is unchanging over time or unable to be changed.
 - In a BlockChain context, once data has been written to a BlockChain no one, not even a system administrator, can change it. This provides benefits for audit. As a provider of data you can prove that your data hasn't been altered, and as a recipient of data you can be sure that the data hasn't been altered. These benefits are useful for databases of financial transactions.
 - **With respect to immutability, the way the data is structured is significant. There are two key ideas: Hashes and Blocks.**
-

WHAT IS BLOCKCHAIN

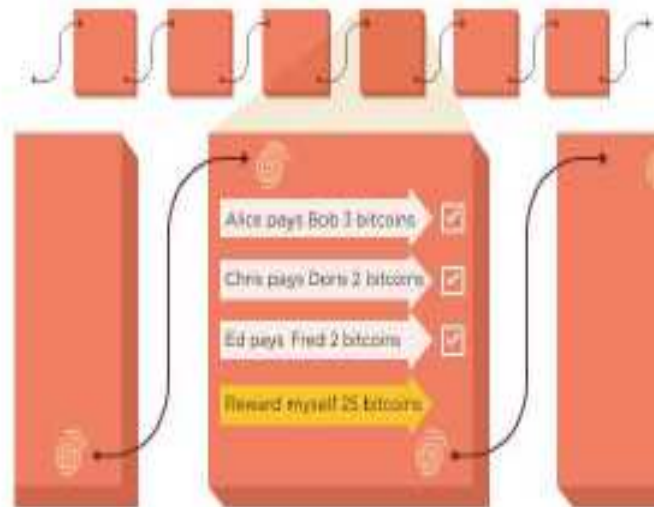
A Brief Intro:

- Hashes
 - A hash function is a type of mathematical function which turns data into a fingerprint of that data called a hash. It's like a formula or algorithm which takes the input data (any data, whether it's the entire Encyclopedia Britannica, or just the number '1') and turns it into an output of a fixed length, which represents the fingerprint of the data. There are many types of hash functions e.g. SHA-256
 - When you mash the phrase "Hello from Bits on Blocks!" through this function, you get this fingerprint out:
`389f9ef3822e5c88f4b140db82c459064711a52182a3e438b4ebc7ecda62b9bb` (SHA-256 hash of the phrase).
 - Two relevant properties of a good hash function are:
 1. It's hard to back-calculate the original data from the hash
 2. If the input data changes in the slightest, the hash changes in an unpredictable way

WHAT IS BLOCKCHAIN

A Brief Intro:

- **Blocks**
 - An important idea in BlockChain is that transactions are bundled into blocks. Blocks contain a number of transactions (e.g. payments) and also some other data including the previous block's hash. As each block includes the previous block's hash as part of its data, a chain of blocks is formed.



WHAT IS BLOCKCHAIN

A Brief Intro:

- **Blocks**
 - Creating a ledger of transactions with blocks that refer to previous blocks is a much better idea than numbering pages in a book (in the case of a book ledger).
 - In a book ledger with numbered pages, 1, 2, 3, etc. it would be easy to tear out page 40 and replace it with another page 40 with slightly different transactions.
 - The book's integrity remains intact, with pages 39, 40, 41 becoming 39, 40, 41 – no change. Also there is nothing in the page number '40' that reflects any of the content in that page and the ordering of the pages is implicit from the page numbers.
 - However in a BlockChain, instead of referring to block numbers, blocks are referenced by their hash and each block explicitly specifies which block (hash) it is building on.
 - So, blocks are explicitly ordered by reference to previous block hashes, which reflect content, instead of being ordered implicitly by a numbering system (1, 2, 3) which is content-agnostic.

WHAT IS BLOCKCHAIN

A Brief Intro:

- Blocks
 - Key points
 - Each block's hash is derived from the contents of the block
 - Each block refers to the previous block's hash, not a sequential number
 - Data in a Blockchain is internally consistent, that is you can run some checks on it, and if the data and hashes don't match up, there has definitely been some tinkering.



BLOCKCHAIN BENEFITS OVERVIEW

KEEPING SECURE RECORDS

- **Records and validates each and every transaction made in a cryptographic manner**
 - Multi-Signatures [public key cryptography, specifically ECC due to key-strength and shorter keys]
 - Encrypted Communication [in particular for generalized B2B transactions]
 - True Non-Repudiation: Transaction unlinkability while incorporating identity management and auditability

EFFICIENT VALUE TRANSFER

- **Blockchain mining discards the need of any third-party or central authority for P2P transactions needed to transfer value between two parties: *Process and Cost Efficiency; Reduced internal risks; Mitigate Man in the Middle***

SMART CONTRACTS

- **Decentralization of the technology and distributed Ledger for smart contracts development, exchange and signature**
- **Transfer over Internet by anyone with computer or smart phone**

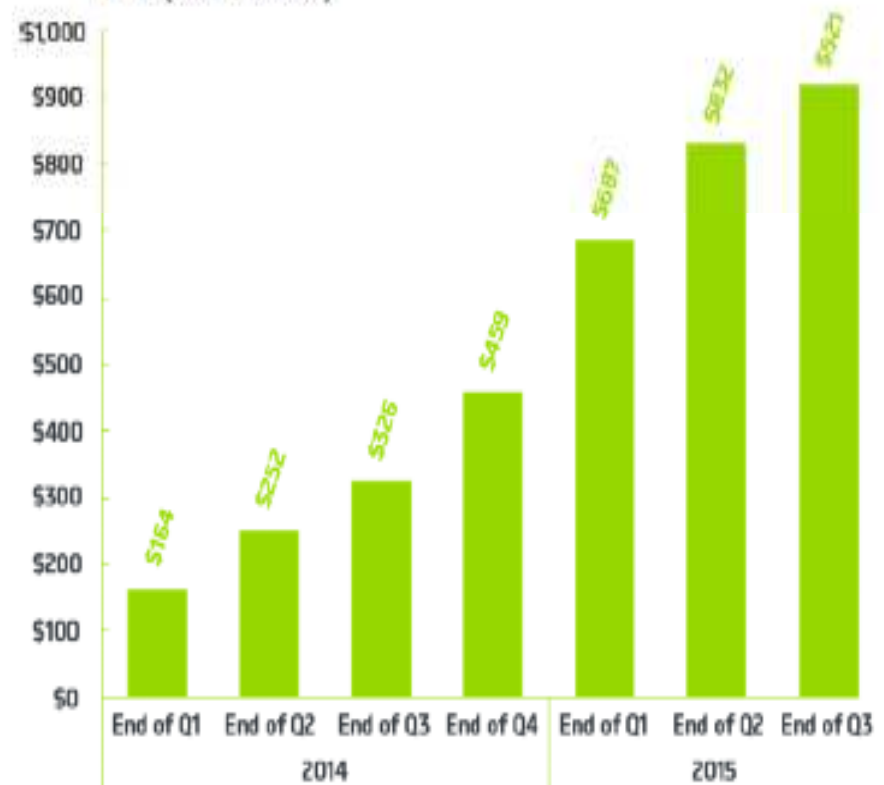
BLOCKCHAIN CHALLENGES

Challenges

- **Blockchain significantly alters the need for trusted third-party authentication through a financial institution**
 - Challenges of legacy infrastructure
- **Challenges in understanding the technology**
 - Complex cryptosystems
 - Decentralized cryptosystems
- **Attacks on Cryptosystems**
- **Government backing and standards are currently in exploratory phase only**
- **Can facilitate money laundering, crime**
- **Currently cannot support a large number of transactions and is not fast enough**

• Increased Investment

Cumulative VC Investment in Virtual Currency & Blockchain Tech (USD millions)



PERMISSIONED BLOCKCHAINS

A **Permissioned Blockchain** is a distributed secure log file or **shared ledger** where the ledger is maintained in a private and secure walled garden of participants

A **shared ledger** technology allowing any participant in the business network to see the **established (via distributed consensus) system of record (ledger)**

Each **peer address is discrete and known** and **access** is controlled by a common trust infrastructure of PKI based trust anchors

Every **viable transaction** is stored in the **shared private ledger**

Transactions are placed in **blocks**, which are linked by **one way hashes**

Operates in a **peer to peer mode** but among a known community of private databases or ledgers



WHAT IS A BLOCKCHAIN?

- **IMMUTABLE LEDGER:** write-only distributed database registering immutable record of every transaction that occurs
- **SMART CONTRACTS:** ethereum blockchain store and execute programs on the blockchain
- **CRYPTOGRAPHY:** uses private key infrastructure to create system that is tamper-proof and secure
- **DECENTRALIZED CONSENSUS:**
 1. Many replicas of the blockchain database
 2. No one participant can tamper it
 3. Consensus among majority of participants is needed to update database.

WHAT IS A BLOCKCHAIN?

- **REDUCE COSTS:**

- ✓ Removes cost of intermediaries
- ✓ Smart contract automation reduces manual processing, re-work, and processing errors

- **INCREASE REVENUES:**

- ✓ Creation of new products and services
- ✓ Capture value from demonstrating provable provenance

WHAT IS A BLOCKCHAIN?

- **REDUCE RISK:**

- ✓ No single point of failure or attack
- ✓ Non repudiability reduces fraud risk
- ✓ Immutable audit trail and provenance

- **IMPROVE SPEED AND EXPERIENCE:**

- ✓ Simplify value chain by removing intermediaries
- ✓ Allow T+0 settlement

BLOCKCHAIN ENABLERS

- **ASSET TOKENIZATION:** tokenization of physical and digital assets for trading and settlement with multiple parties
- **CUSTIDY & ESCROW:** trustless transaction with asset in escrow managed by smart contract
- **PROVENANCE TRACKING:** single source of truth that conveys information about asset across its journey from one custodian to another
- **ACCOUNTING & RECONCILIATIONS:** new accounting where every debit and credit is recorded with immutable entry on blockchain

BLOCKCHAIN ENABLERS

- **DIGITAL IDENTITY:** consolidation and management of ID with attributes stored and verified on blockchain
- **REAL-TIME TRANSACTION:** atomic transaction ensure trade is settlement, removing lag time
- **MICRO PAYMENTS & FUNDING:** transactions of minimum value enable P2P payments, M2M payments and capital raising
- **AUTOMATED EXECUTION:** full automatic of contract lifecycle from issuance, transfers, revisions and execution

Piazza A. Diaz, 6
Milano, 20123
Cell 328 8871062
E-mail: studiolegalebruccoleri@gmail.com

Studio Legale
Avv. Maria Bruccoleri

Via Gioacchino di Marzo 5
Palermo, 90144
Tel. 091 309131
Tel/Fax 091 308038
PEC: avvmariabruccoleri@legamail.it

Thanks for your attention

www.avvocatobruccoleri.it