Fondation Vallet & Benin Excellence & UNDP

VALLET fondation

Ecole d'Eté sur
L'INTELLIGENCE ARTIFICIELLE
DU 18 JUILLET AU 13 AOÛT 2022

BE
BENIN EXCELLENCE

PNUD
Bénin
laboratoire d'accélération

Blockchain: Its Origin and Applications

Vincent Whannou de Dravo

Presentation Outline

1. Foreword
2. Introduction
3. Origin
   - Concept Genesis
   - Working Definitions
   - Others
4. Applications
   - Cryptocurrencies
   - Government
   - Industry
   - Healthcare
   - Others
5. Conclusion

This conference was given as part of the second edition of the Summer School in Artificial Intelligence initiated by *La Fondation Vallet*, *Benin Excellence* and *UNDP*. Before this conference, I had to give conferences in a private university in Benin about blockchain, cryptocurrencies, NFTs, artificial intelligence, IoT, and robotics. It was during one of them that Dr. Espéran Padonou and I had hosted conferences on artificial intelligence for the first and on NFTs for the second. I would like to thank Dr. Esṕeran for this opportunity of the summer school, but also Mrs. Francine Lucette Batossi and Dr. Alao Adjassa who are respectively Module Teacher and Director of Training in the said university who allowed me to lead conferences at the IRGIB at the time. Great gratitude to all.

This presentation is an essay of answers on the origins of the Blockchain and its applications. We show in this presentation that even though the concept was introduced thanks to the discovery on how digital money could work of a certain Satoshi Nakamoto, it is obvious that on the algorithmic or architectural level, a number of innovations before Nakamoto facilitated the first implementation of this technology. To this end, we will see some progress in the field of algorithms and system architecture that have facilitated this innovation. It is good to note that bitcoin, which is therefore the first virtual currency to respond to a crucial problem to which its predecessors have not been able to respond to, continue to be improved by its community (with more than 300 proposals for improvement to date: https://en.bitcoin.it/wiki/Category:BIP)

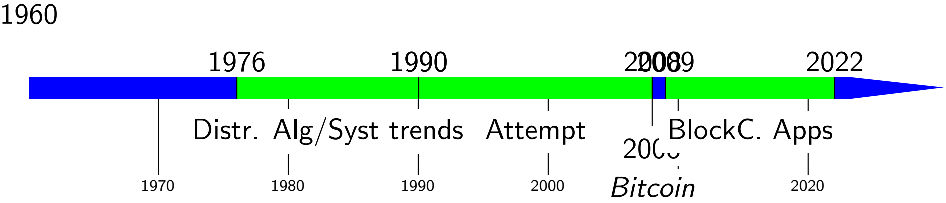
Questions about blockchain applications

- What is a blockchain?
- How do nodes communicate in a blockchain network?
- What is a consensus, and what is a protocol?
- Why do we need a decentralized or peer-to-peer distributed network for this type of technology?
- How one can use Blockchain and AI in the same applications?

Origin

A number of innovations are at the heart of the first conceptualization of blockchain technology. These innovations can be deduced from Satoshi Nakamoto's white paper[9] when he said: *In this paper, we propose a solution to the* **double-spending problem** *using a* **peer-to-peer distributed timestamp server** *to generate* **computational proof of the chronological order of transactions**. *The system is secure as long as* **honest nodes collectively control more CPU power** *than any cooperating group of attacker nodes.*

Origin (Cont'n): Timeline



Origin (Cont'n): Timeline

1980: Byzantine generals (Byzantine Agreement) problem algorithm [7].
1991: Time Stamping digital Document [5],
1992: Merkle tree,
2002: Data Storage in blocks (Byzantine Storage),
2004: Reusable Proof of Work (RPoW) by Hal Finney
2005: Bitgold by Nick Szabo
2008: Bitcoin First Proposal [9]
2009: Bitcoin Genesis block

Origin (Cont'n): Some Algorithms

There are several algorithms that allowed the implementation of the first publicly known blockchain [9]. Here we evoke 4 algorithms essentially but there are other algorithms:

1. the Byzantine generals (or Byzantine Agreement) problem algorithm by Pease, Shostak and Lamport [7].
2. Election algorithm (not Lelann [6], Chang and Roberts)
3. Merkle Tree Algorithm
4. the electronic document timestamp algorithm [5]

Distributed computing

Definition 3.1

A distributed system can be defined as a set of computer networks in which individual computers are physically distributed in a given geographical area. There are other equivalent definitions, but two properties are essential to this type of architecture:

1. there are several independent computing entities with their own memory and sharing a common code
2. the entities communicate with each other by message passing

Distributed computing (Cont'n): Types of Networks

Example 3.2

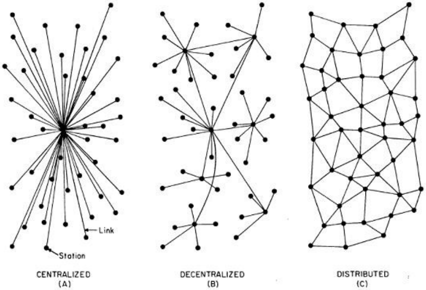


Figure 1: Network Types. Source: https://medium.com/@RobinCRLee/decentralized-yet-still-clustered-

Distributed computing (Cont'n): System Perspective and Algorithmic challenges

1. Synchronization
2. Fault tolerance
3. Security
4. Application Programming Interface (API)
5. Scalability and modularity
6. Data storage and access
7. Consistency and replication
8. ...

Distributed computing (Cont'n): System Perspective and Algorithmic challenges

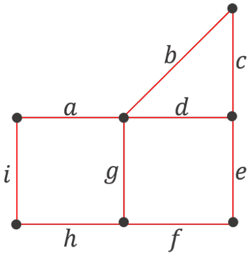
1. Designing useful execution models and frameworks
2. Dynamic distributed graph algorithms and distributed routing algorithms
3. Time and global state in a distributed system.
4. Synchronization/ coordination mechanisms.
5. Group communication, multicast, and ordered message delivery
6. Distributed program design and verification tools
7. Debugging distributed programs.
8. Load balancing.
9. Real-time scheduling.
10. Performance.

Working Definitions (Cont'n): What is a peer to peer network?

Definition 3.3

A peer-to-peer (P2P) network is a distributed architecture that distributes tasks or workloads among peers, and in which peers are identically privileged.

Example 3.4



Working Definitions (Cont'n): what is double spending

Definition 3.5

Double spending is a potential flaw in a digital currency system in which the same digital token can be spent more than once. There are three major risks to digital currency.

Devaluation of the digital currency when this failure occurs.

1. Inflation
2. Loss of confidence on the money system
3. Devaluation of the digital currency

Working Definitions (Cont'n): How double spending can be performed?

1. Race Attack
2. 51% attack
3. Finney attack

Blockchain

Definition 3.6

Blockchain is the technology that enables its participants to verify existing blocks of information and add new ones based on a consensus algorithm. It generates timestamped chunks of information encapsulated in blocks secured by hash signature and is immutable by nature[1].

Blockchain main characteristics

Remark 3.7

Here are the main characteristics:

- *Open Source*
- *Anonymity*
- *Transparent*
- *Decentralization*
- *Immutable*
- *Autonomy*

Consensus models vs Smart Contract vs Protocols

1. Consensus: They are rules and they are many type of consensus :
   - Consensus about rules: How do nodes communicate? what kind of data is sent over the network? What makes a transaction valid? How do changes occur in the protocol definition? Minor changes vs Bitcoin Improvement Proposal?
   - Consensus about history: what is the correct blockchain chain (honnest nodes)?
   - Consensus by value: is there a values attached to it? How do we decide it?
2. Smart Contract: Agreement on the rules
3. Protocol: Implementation of rules

Ideology

- Making the world fairer (political, social, economic – a fairer monetary system-, cultural change, etc.)
- Solving banks' problems → economic crises
- Making transactions between individuals more reliable
- Cypherpunks (a.k.a. Cyberpunks) Communities

Financial services: Cryptocurrencies, Banks, etc

Blockchain [10, 2]:

- provides end-to-end visibility of the financial resources
- helps in reducing number of disputes and time to resolve disputes and simplify the business processes
- resolves the traditional banking problems such as non-repudiation, transparency, traceability in a cost-effective way.

Example 4.1

Bank of America Merrill Lynch, Santander, UniCredit, Standard Chartered, Westpac Banking Corporation, and Royal Bank of Canada are the founding members of the network, known as the Global Payments Steering Group (GPSG) → Ripple's (XRP) Global Payments Steering Group

Government uses

Blockchain [10]:

- provides better solution to the existing procedures
- enhance operations performance by automating governance: citizen identification certificates, maintaining the records of the public assets, tracking its uses, record keeping and maintaining legal documents related to the public and private entities, various permissions issuing to the stakeholders, tax payments
- could help in designing online voting system long with the integration of government services as blockchain records are immutable, traceable, decentralized public ledgers along with great transparency.

Industrial applications

Blockchain technology can help in the following areas[10]:

- purchase management,
- customer relationship management,
- supply chain management,
- production, and operations management
- any business or industry tracking of movement of goods under process or processed good

Healthcare

Blockchain technology can help in the following areas[3]:

- E-Health Record system (EHR)
- Medical fraud deduction system
- Clinical research
- Pharmaceutical industry research
- Neuroscience

IoT applications

This application is mostly based on smart devices interaction. This is one of the most challenging but yet growing field in which smart devices interact with each other using the Internet. Major issues are: security of data generated within distributed nature of wireless networks[10].

NFT

Definition 4.2

NFTs : Non-Fungible Tokens represent non-Fungible items. That is, they can't be freely exchanged or replaced by similar items. For example, diamonds are non-fungible. Each diamond is unique—size, color, clarity, and cut. If you bought a particular diamond, it would not be easily interchangeable with another diamond.

Remark 4.3

Every NFT is really a piece of programming code, which on the Ethereum blockchain is known as a smart contract. Non-fungible tokens have certain characteristics that set them apart from regular fungible tokens. As mentioned, fungible tokens on the Ethereum network are also known as ERC20 tokens. NFTs on the Ethereum network are ERC721 or ERC1155 tokens[8].

NFT

Example 4.4

They can take one of the following form[8]:

- Audio, Images, GIFs, Videos, 3D Model
- Books and Prose
- In-Game Items
- Digital Trading Cards
- Digital real Estate: Sandbox
- Domain names
- Event Tickets
- Tweets J. Dorsey first tweet at $2.9 million

NFT (Premise): Desmond Paul Henry

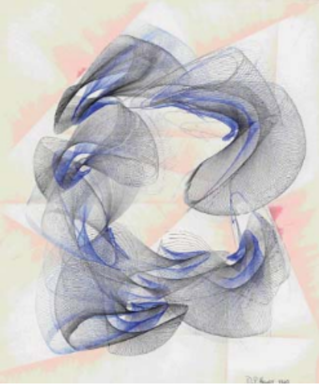


Figure 2: Desmond Paul Henry, first drawing—Courtesy of the Estate of Desmond Paul Henry

NFT: CryptoPunk 606

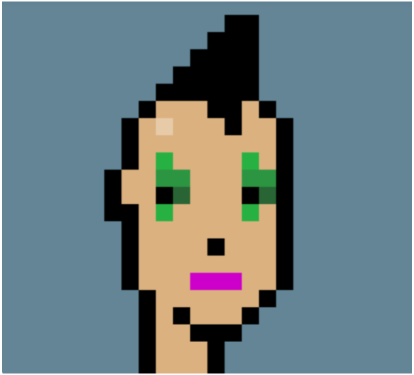


Figure 3: CryptoPunk #606. Source: `https://opensea.io/assets/ethereum/0xb47e3cd837ddf8e4c57f05d70ab865de6e193bbb/606`.

Metaverse: What is it exactly?

"Instead of simply seeing stuff, you are immersed in it," Mark Zuckerberg said in a July 2021 interview with tech site The Verge, distinguishing the concept of the Metaverse and the traditional "two-dimensional" webpages that now occupy the internet.

Remark 4.5

The Metaverse exists as an augmentation of the actual world, a three-dimensional environment that allows individuals to penetrate and engage. It will very certainly become the most popular location globally, but it will almost certainly not be flawless from the start. It will take time for a comprehensive virtual reality to mature into a fully digitalized world. Neal Stephenson initially presented the notion of the Metaverse in his book "Snow Crash" about 1992[4].

Metaverse (Cont'n): What is it exactly?

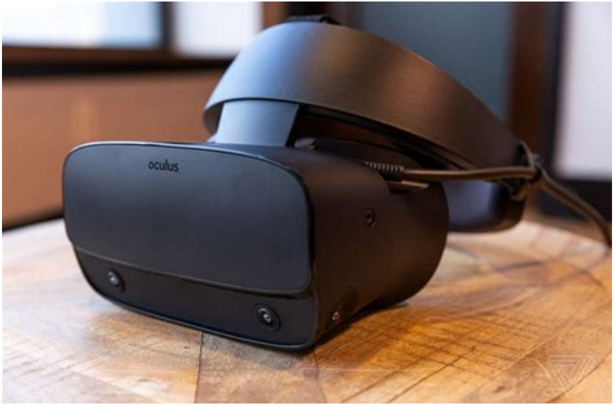


Figure 4: Oculus. Source: https://www.jahshaka.com/oculus-unveils-the-rift-s-a-higher-resolution-vr-headset-with-built-in-tracking/.

dApps or decentralized Applications

They are apps running on **decentralized servers** and using a specific **blockchain** for **data storage** and **smart contracts** (backend codes).

Recommendations

- All these technologies (the blockchain in particular), and their applications, have their limits and can present dangers of which we have no idea. A potential danger that we can already draw from the design of the blockchain is it is not a technology controlled by a single entity, but rather that several independent, transparent and honest entities are in charge of our data in a consensual way. One way to achieve this is to be engaged in the world of Open Source to improve what could contain flaws (especially ethical ones) of these technologies.
- Associate these technologies with respect for human, animal and environmental life
- Do not stop in such a good way

Thank You!

List of References

[1] Naseem Ahamed. *Introduction to the Blockchain Technology behind Shared Information*. Ed. by Panda Sandeep Kumar et al. 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742 and 2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN: CRC Press and Winston, 2020.

[2] Freed Associates. *Innovative Blockchain Uses in Health Care*. 2022. URL: https://www.freedassociates.com/knowledge-center/innovative-blockchain-uses-in-health-care/ (visited on 07/20/2022).

[3] Girish BVS. *Innovative Blockchain Uses in Health Care*. 2022. URL: https://www.sasken.com/insights/white-papers/blockchain-technology-concepts (visited on 07/20/2022).

List of References

[4] Andrew Clemens. *Metaverse For Beginners: A Guide To Help You Learn About Metaverse, Virtual Reality And Investing In NFTs*. 2022.

[5] Stuart Haber and W. Scott Stornetta. "How to Time-stamp a Digital Document". In: *Journal of Cryptology* 3 (1991), pp. 99–111.

[6] Gerard Le Lann. "Distributed Systems - Towards a Formal Approach.". In: Jan. 1977, pp. 155–160.

[7] Pease Marshall, Shostak Robert, and Leslie Lamport. "Reaching Agreement in the Presence of Faults". In: *Journal of the Association for Computing Machinery* 27.2 (Apr. 1980), pp. 228–234.

[8] Fortnow Matt and Terry QuHarrison. *The NFT Handbook: How to Create, Sell and Buy Non-Fungible Tokens*. New Jersey, USA, 2022.

List of References

[9] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Tech. rep. 2008, pp. 1–9.

[10] Michael Nofer et al. “Blockchain”. In: *Business & Information Systems Engineering* 59 (Mar. 2017), pp. 183–187.