Smart Contracts: Next Generation of Contracting?[1, 2]

Baptiste Lestienne

ABSTRACT

The blockchain smart contracting technology is a fresh topic constantly changing which fascinate and frighten people and institutional the same time. The purpose of this work is to get an overview of smart contract, compare their differences and their possibilities. First, I have used a Multi-Attribute Decision Making and second, a compensatory model for weighting the result. My work has highlighted the importance of security and decentralization for smart contracting regarding to the different alternative currently in the market. To conclude I would advise the Ethereum blockchain for his decentralization and community and the DPoS security system to secure a blockchain and their smart contract.

Key words: Smart contracts, Blockchain, Ethereum, Mining, Decentralization, Contract future, Online revolution, Transparency

INTRODUCTION

"Initially the term smart contract has been created by Nick Szabo"[3], computer scientist and cryptographer, in the early 1994. This term was used to describe digital engagement like protocols were both parties fulfill some commitment. At this time researcher like him, Mark S. Miller or "David Chaum"[4] were already convinced that strict execution of encrypted online protocol would be a high added value and a significant improvement of the traditional law.

[1] Editor's note: Student papers are authored by graduate or undergraduate students based on coursework at accredited universities or training programs. This paper was prepared for the course "International Contract Management" facilitated by Dr Paul D. Giammalvo of PT Mitratata Citragraha, Jakarta, Indonesia as an Adjunct Professor under contract to SKEMA Business School for the program Master of Science in Project and Programme Management and Business Development. http://www.skema.edu/programmes/masters-of-science. For more information on this global program (Lille and Paris in France; Belo Horizonte in Brazil), contact Dr Paul Gardiner, Global Programme Director, at paul.gardiner@skema.edu.

[2] How to cite this paper: Lestienne, B. (2019). Title, *PM World Journal*, Vol. VIII, Issue X, November.

[3] Nick Szabo. (2018, October 15). Retrieved from https://en.wikipedia.org/wiki/Nick_Szabo
[4] David Chaum. (2018, November 12). Retrieved from https://en.wikipedia.org/wiki/David_Chaum

> *New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts 'smart', because they are far more functional than their inanimate paper-based ancestors.*
>
> *Nick Szabo, 1996* [5]

In 2009 Satoshi Nakamoto release the bitcoin cryptocurrency based on the very first blockchain technology. Bitcoin blockchain is starting a huge digital revolution and in a way lay the foundation of smart contracting. The real revolution happened in 2013 with the creation of Ethereum blockchain by Vitalik Buterin. "Ethereum permit to create complex smart contract thanks to a new programming language calling Solidy"[6]. It allows developer to write complex process in a short time based in Ethereum blockchain.

When a classic legal contract just defines rules of an accord between parties, a smart contract will also freeze those rules inside a blockchain for ever and ensure the transfer of an asset if the contractual term approve it.

Smart contracts are pieces of software based inside blockchain which allow to transport and transfer assets and data without any middlemen. No human action is necessary, it lives by his own. The contract will be executed regarding the rules, that both parties agree on, and data certificate as accurate. Because of their resilience to tampering smart contracts are used in many domains, especially in those who require confidence and traceability, like money transfers, banking, insurance, respect certain agreed rules.

Over the years, many platforms allow now to create smart contract but the main one is still Ethereum. Beside it, alternative solution has been created by Ripples, Stellar or Monax. In a flourished environment the number of cryptocurrency and smart contract have skyrocket those past 3 years. CoinMarketcap is now listing more than 2080 cryptocurrencies vs 36 cryptocurrencies at the same date in 2013. The same thing had happened with smart contracts. Hundreds of thousand smart contracts are created every quarter.

[5] Smart Contracts. (n.d.). Retrieved from http://www.alamut.com/subj/economics/nick_szabo/smartContracts.html
[6] Solidity — Solidity 0.4.24 documentation. (n.d.). Retrieved from https://solidity.readthedocs.io/en/v0.4.24/

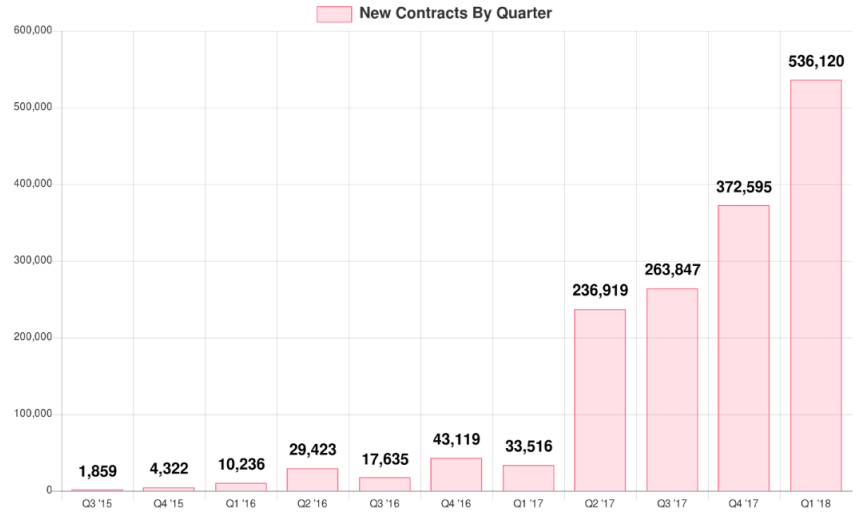


Figure 1: Number of new Smart-Contracts created each quarter[7]

Mass adoption had really begun at the Q2 of 2017, when the hype concerning blockchain and cryptocurrency was high. Even if blockchain and smart contracts are hype word, most of the people don't really understand the potential and the benefits of this technology, the trustworthiness and the security that it provides. Smart contract could also have weakness, without deep knowledge, the consequence of an unsafe code choice, design, structure can be dramatic. Because of programming error, a smart contract can pass from intangible to extremely weak ("50 million in crypto were stolen during the DAO smart contract case"[8]).

[7] Chandersekhar, P. (2018, May 23). Ethereum Smart-Contracts: Most of them are rarely used! Retrieved from https://hackernoon.com/ethereum-smart-contracts-most-of-them-are-rarely-used-f45749730d3e
[8] Falkon, S. (2017, December 24). The Story of the DAO? Its History and Consequences. Retrieved from https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

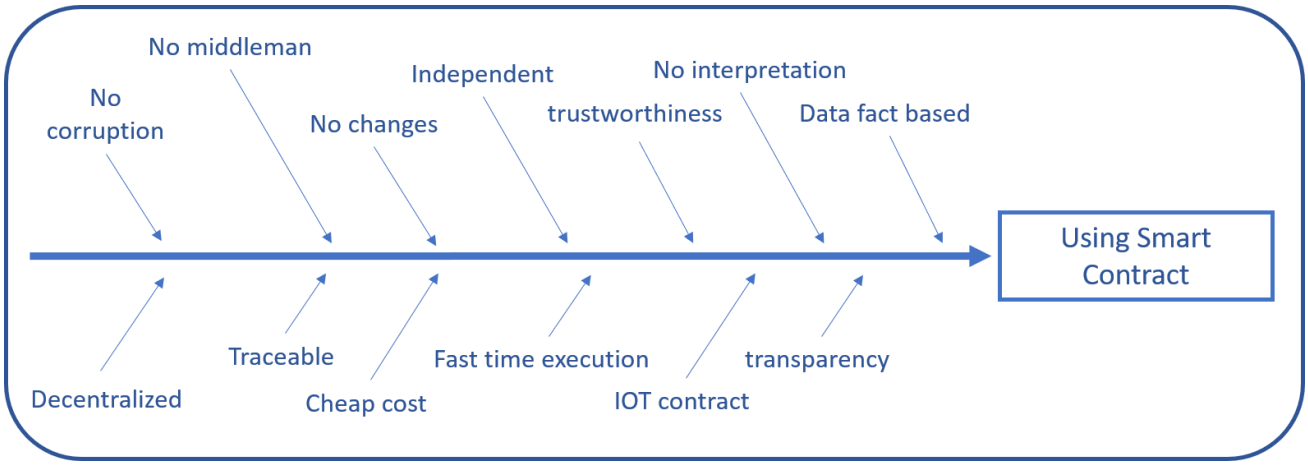


Figure 2: Root cause analysis of using smart contract[9]

Understand what smart contract are, how they are working and what are their benefit and limit must be the main development point for layer and jurist if they want gain from it. It requires technicity and new competences that those classic profession doesn't have for the moment. Smart contracts will, for sure, find their utility into strategic centenary domain like finance, insurance and audit. Moreover, into daily tasks, hundreds of future smart contracts will be used. There is a huge interest concerning the IOT, regarding how fast the technology is moving into our daily life, smart contract and blockchain will be the intangible link between every component around us.

[9] By author

METHODOLOGY

Step 1: Summarize

As introduced, Smart contract are for sure the future of contracting, but with their complexity we need to deal with 3 aspects of smart contract: scalability, decentralization and security. We need want to show which smart contract is the best if we care more about scalability or decentralization:

- Decentralization of Smart Contract.
- Security of smart contract

Step 2: Identification of alternative solutions

Firstly, we need to explain more about the 3 main aspects of a smart contract: Decentralization, security and scalability. Those 3 aspects are called the "Blockchain trilemma [10]by Vilatik Buterin", the founder of Ethereum. Developing a blockchain and smart contract without compromising either one of those key aspect is almost impossible. A decent Blockchain can only achieve 2 out of 3 of those key concepts at one time. Like Vitalik I think that scalability is not a big issue comparing to decentralization and security. Security and decentralization are the core of blockchain and smart contract, it can't be compromise while scalability is a 2nd plan problem and can be looked at alongside ideas of decentralization and security.

Alternative Solution

As we need to find two solutions, we will make two lists of alternative solutions. One solution will be about decentralization of Smart contract and the other one will be about Security of smart contract. We will compare different mart contract type regarding to decentralization and different type of security protocol.

Decentralization of Smart Contract

- **Ethereum**

Founded in 2013 by "Vitalik Buterin[11]", Ethereum is a blockchain based on Proof of Work which enable developer to create complex smart contract with a unique language call Solidy and on a "dedicated platform call virtual machine[12]".

[10] Wang, T. (2018, August 10). Tackling the Scalability Trilemma? Hacker Noon. Retrieved from https://hackernoon.com/tackling-the-scalability-trilemma-1627fa3f6936
[11] Vitalik Buterin. (2018, December 4). Retrieved from https://en.wikipedia.org/wiki/Vitalik_Buterin
[12] pirapira/awesome-ethereum-virtual-machine. (2018, 5). Retrieved from https://github.com/pirapira/awesome-ethereum-virtual-machine

Ethereum is the very first blockchain having real smart contract and application not only for finance. Currently the new metropolis update is going to improve event more Smart contract and over the long term new update will help smart contract to become even more User friendly.

Ethereum is extremely decentralized, with a strong community, minors, user and developer all over the word. It has an open source spirit and share most of their code on gihub.

Vitalik Buterin is still the main leader of this Blockchain, with clear roadmap he is developing the next generation of Ethereum. Anyway, the community and minor need to approve it before to adopt it. they need a consensus through a hard fork to accept some change in the blockchain.

- **Neo**[13]

Usually call as the "Chinese Ethereum" Neo is a decentralize blockchain launched in 2014 and rename Neo in 2017. It's a "real time open source project based on github[14]". Like Ethereum neo is providing Smart contract possibility, Dapps, ICO support. Neo is based on DBFT security system.

Neo is calling himself government friendly and try to respect local rules, it is currently working with the Chinese government. The Neo's core team is composed of 30 people based in china, they represent the "off chain governance" of the Neo blockchain.

Neo's smart contract can be develop through a Virtual machine in mostly every modern language (c/c++/java/python/ruby)

- **EOS**

"EOS[15] is a decentralized operating system" which can support decentralized application. It provides the possibility to create smart contract through a docker in different kind of classic language. Eos is one of the direct competitors to Ethereum and wish to overpass it one day.

Eos is developing by Block.one company based in Blacksburg and Hong kong. The software EOSIO is an open source software with clear compromise.

EOS is using a delegating proof of stake (dPoS) security system so they were able to increase the scalability of their blockchain. However, EOS is for now less decentralize than Ethereum and the community need to growth.

- **Ripple**[16]

"Ripple is an Us company based near San Francisco" which has created its private blockchain and different financial protocol. They are using the technology of blockchain to provide services like

[13] NEO White Paper. (n.d.). Retrieved from http://docs.neo.org/en-us/whitepaper.html
[14] The Neo Project. (n.d.). Retrieved from https://github.com/neo-project
[15] eosio | Blockchain software architecture. (n.d.). Retrieved from https://eos.io/
[16] Ripple - One Frictionless Experience To Send Money Globally | Ripple. (n.d.). Retrieved from https://ripple.com/

financial transaction or smart contract. Ripple is using a defined list of validator call UNL to validate every transaction and action made on its blockchain.

They have recently relaunched a new "smart contract platform call Codius[17]" to improve the development of smart contract on their blockchain.

Security of smart contract

- **"Proof of Work (PoW)[18]"**

The proof of work protocol is the initial protocol invented by Satoshi Nakamoto with Bitcoin invented to secure a blockchain. This algorithm is used to transfer information and secure in on the blockchain. With the PoW "minors" are in competition to solve a complex mathematical problem to verify the information on the blockchain. Each new data and transaction are linked inside block with are checked by minors through computing power. The complexity of the mathematical problem is adapted to be solved in a determined amount of time (10 min for Bitcoin, 15 second for Ethereum).

Minors are responsible of the security of a PoW blockchain. PoW provide huge security level for blockchain with a strong resistance to Dos attack, it limits the possibility of action inside the blockchain, computing power is independent from amount of money own in the blockchain, over cost every possible attack ("51% attack[19] is too expensive and not profitable")

PoW is consuming a lot of energy, that's the main negative point about this system. It also faces some scalability issue due to the difficulty to verify every transaction.

- **"Proof Of Stake (PoS)[20]"**

A proof of stake system requires a user to put a certain number of cryptocurrency units at stake to be able to verify transactions. Creating of new block is not based on competition between minor. The creator of a new block is chosen to regard some criteria and a random factor. It will depend of the user wealth and the number of coins at stake. Once the user is selected, he will create and validate a new block.

The security of this system depends of the creator of the new block. If a forger validates a fraudulent transaction, they lose their holdings, as well as their future rights to participate as a forger.

- **"Delegated Proof of Stake (DPoS)[21]"**

[17] Codius - Open-source Hosting Platform for Smart Programs. (n.d.). Retrieved from https://codius.org/
[18] Proof of work - Bitcoin Wiki. (n.d.). Retrieved December 11, 2018, from https://en.bitcoin.it/wiki/Proof_of_work
[19] Floyd, D. (2016, September 7). 51% Attack. Retrieved from https://www.investopedia.com/terms/1/51-attack.asp
[20] What is Proof of Stake? (n.d.). Retrieved from https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-stake
[21] What is Delegated Proof of Stake? (n.d.). Retrieved from https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake

"Delegating Proof Of Stake system have been created by Daniel Larimer[22]". It's an improvement of the PoS system. It increases speed and scalability.

Like in PoS system a unique user creates and validate new blocks, but here user vote to select witnesses. Those top witnesses will be the ones able to create and validate new blocks. Vote is weighed regarding the size of each voter's stake User can also delegate their voting power to someone they trust.

The number of witnesses is limited and depend of the blockchain, they are responsible of validating the good blocks and check their accuracy, they can't change any details in the block. Those witnesses are using a security system to validate the block like a proof of work system.

Attributes to measure, assess or evaluate each alternative

We need to analyse those alternatives. We will use a Multi-Attribute Decision Making (MADM).

Here are the ranking criteria used for this method:

Decentralization of Smart Contract

- **Knowledge and power are decentralized**
  It's a key aspect for Blockchain and smart contract, "Knowledge and power are the main two possibility to control a blockchain[23]". We want here to understand and evaluate how well are they decentralized. Knowledge in a decentralize organisation have to be accessible to everyone everywhere, it needs to be open source and trustable. Every knowledge has to be share to the community and the network. Power is who and how can people interact and influence the blockchain and smart contract. Power must be free of access, without restriction, from the biggest player to the weakest with not difference in the fundamental rules.

- **Change are made by consensus**
  "Consensus[24] is the second key aspect for blockchain" and smart contract, they are based on it. Consensus is the fact that everyone agrees to something, consensus is the fundamental rules agreement and while everyone work with them without trouble it worked. Consensus had to happen also when some rules changes are decided. If the community and the network approve the new rule, then the rule can be followed otherwise there is no consensus, so we stay on the old consensus. We need to evaluate

[22] Daniel Larimer. (2018, December 7). Retrieved from https://en.wikipedia.org/wiki/Daniel_Larimer
[23] Buterin, V. (2017, February 6). The Meaning of Decentralization? Vitalik Buterin? Medium. Retrieved from https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
[24] Seth, S. (2018, April 3). Consensus Mechanism (Cryptocurrency). Retrieved from https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp

here how change are made, is there is a global consensus each time or does some group can overpass other and decide for new rules?

- **Type of blockchain**
  Smart contract are based on blockchain and the type of blockchain deeply influence how decentralize they are. There is "3 mains type of Blockchain[25]": public, federated and private. It gives us a clear idea of how decentralised they are.

- **Working group communicate with each other directly**
  In a decentralized point of view working group communicate with each other directly[26], at the contrary in a centralized pint of view working group communicate through intermediaries. Do you need to pass by a middle man to use it and work on it?

- **People in charge**
  Concretely is there is "someone in charge of the blockchain[27]"? Someone might be responsible of a blockchain or smart contract and work with a team on it. It means in this case that the leadership and development team is a centralize processes. In decentralized context the development team in charge would be changing, open to everyone and collaborative to the all community.

- **Headquarter location**
  Last key attribute, does the smart contract or the blockchain have a real localisation? It means that the blockchain is centralize in a headquarter somewhere. A decentralize organisation haven't got any headquarter or office. Headquarter mean country and rules, that's in opposition with decentralization spirit.

  Here is a pair-wise comparison for the different attributes for decentralization of contract:

[25] Blockchains & Distributed Ledger Technologies. (n.d.). Retrieved from https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/
[26] Jayasinghe, T. (2018, June 20). Ethereum Blockchain 'Hello World? Smart Contract with JAVA. Retrieved from https://medium.com/coinmonks/ethereum-blockchain-hello-world-smart-contract-with-java-9b6ae2961ad1
[27] The People Leading the Blockchain Revolution. (2018, October 22). Retrieved from https://www.nytimes.com/2018/06/27/business/dealbook/blockchain-stars.html

attributes/solution	There isn't headquarter	Who is in charge	Knowledge and power are decentralized	Working group communicate with each other directly	Change are made by consensus	Type of blockchain	total
There isn't headquarter	X	0	0	0	0	0	0
Who is in charge	1	X	0	0	0	0	1
Knowledge and power are decentralized	1	1	X	1	1	1	5
Working group communicate with each other directly	1	1	0	X	0	0	2
Change are made by consensus	1	1	0	1	X	1	4
Type of blockchain	1	1	0	1	0	X	3

Figure 3: Pair-Wise comparison for decentralization of smart contract

As we can see with the total, we have a ranking of our attribute

Security of smart contract

- **Security level**
  "We need to consider the direct level of security of the blockchain [28]" which host the smart contract. The direct level of protection that it provides to information contained inside it. This security level differs depending the type of blockchain and security protocol.

- **Trustability of "block's validator"**
  "The block validator will be the one providing the security to the blockchain" [29]and smart contract. If people can trust the validator the smart contract and blockchain are secure. The validator is chosen by many ways, depend on the technique but being the validator of a block can be a very demanding a complicated process to be selected or just random. The trustability of the block's validator represent a part of the security of a smart contract blockchain.

- **Possibility of validator mistake**
  It is essential to consider that even "the most secured and trustable validator [30]" could be attacked or could simply validate a wrong or fake block. Can he do it and what would be the direct consequence for him. Depend on the method use, some technique prevents more this case from other. The possibility off intentional or unintentional mistake can affect the security of the all smart contract.

[28] Orcutt, M. (2018, April 25). How secure is blockchain really? Retrieved from https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/
[29] Stone, A. (2016, December 2). Block and Transaction Validation Analysis? Andrew Stone? Medium. Retrieved from https://medium.com/@g.andrew.stone/proposed-bitcoin-unlimited-excessive-defaults-for-block-validation-326417f944fa
[30] Stone, A. (2016, December 2). Block and Transaction Validation Analysis? Andrew Stone? Medium. Retrieved from https://medium.com/@g.andrew.stone/proposed-bitcoin-unlimited-excessive-defaults-for-block-validation-326417f944fa

- **51% attack resistance**
  "51% attack is one of the main worries for blockchain"[31] and smart contract. It means that someone have 51% of the global power of the blockchain and is able to control and corrupt it. It's a difficult type of attack but a huge weakness for blockchain. We need to consider how well the blockchain and smart contract are resistant to that type of attack.

- **Quantum computing resistance**
  "Quantum computing is the next generation of computing machine [32]" and technique. It will and already affect the foundation of modern computing. It will definitely have an impact on blockchain technologies. We need to consider the security resistance of smart contract and blockchain type t this kind of new quantum computing power.

- **Potential for the future**
  We need also to consider the "future of the blockchain[33]", the level of security might decline with time. Future of blockchain in term of security can be check with their roadmap, their community, their possible evolution, their flexibility and adaptability to changeset. Security is at a T-time instant but also on the future improvement and evolution.

  Here is a pair-wise comparison for the different attributes for security of contract:

Ordinal Ranking	51% attack resistance	Potential for the future	Security level	Possibility of validator mistake	Quantum computing resistance	Trustability of "block's validator"	Total
51% attack resistance	X	1	0	0	1	0	2
Potential for the future	0	X	0	0	0	0	0
Security level	1	1	X	1	1	1	5
Possibility of validator mistake	1	1	0	X	1	0	3
Quantum computing resistance	0	1	0	0	X	0	1
Trustability of "block's validator"	1	1	0	1	1	X	4

Figure 4: Pair-Wise comparison for security of smart contract

As we can see with the total, we have a ranking of our attribute

[31] Floyd, D. (2016, September 7). 51% Attack. Retrieved from https://www.investopedia.com/terms/1/51-attack.asp
[32] STUDIOS, B. (n.d.). Quantum Computing and Building Resistance into Proof of Stake. Retrieved from https://bitcoinmagazine.com/articles/quantum-computing-and-building-resistance-proof-stake/
[33] http://webcache.googleusercontent.com/search'q=cache://www.forbes.com/sites/forbescoachescouncil/2018/08/02/the-future-of-blockchain-and-its-potential-impact-on-our-world/. (2018, August 2). Retrieved from https://www.forbes.com/sites/forbescoachescouncil/2018/08/02/the-future-of-blockchain-and-its-potential-impact-on-our-world/#16ca7b0e1f69

Step 3: Development of Feasible Alternatives

We will now rank each attribute to perform this analyze, from the most important (1) to the least (6). It will help us to perform our MADM.

(1) We will give an ordinal ranking (1 is the best and 6 the worst) of each evaluating attribute brought up in the previous part and choose the marking greed.
(2) Then we will mark each criterion following the marking greed.

Decentralization of Smart Contract

(1) [34]Ordinal ranking and marking greed

Ordinal Ranking		Possible mark from better to the worst		
1	Knowledge and power are decentralized	decentralized	depending of the kind of informations	centralized
2	Change are made by consensus	Yes	medium way	No
3	Type of blockchain	public	Mix	private
4	Working group communicate with each other directly	Yes	medium	No
5	Who is in charge	No one	Depending	Someone
6	There isn't headquarter	No headquarter	temporary headquarter	centralize headquarter

Figure 5 : Ordinal ranking and marking greed Marking for Decentralization of smart contract

(2) [35]Marking

[34] By Author
[35] By Author

attributes/solution		Ethereum	NEO	EOS	Ripple
1	Knowledge and power are decentralized	decentralized	decentralized	decentralized	centralized
2	Change are made by consensus	Yes	Yes	Yes	No
3	Type of blockchain	public	public	public	private
4	Working group communicate with each other directly	Yes	medium	Yes	medium
5	Who is in charge	Depending	Someone	Someone	Someone
6	There isn't headquarter	temporary headquarter	centralized headquarter	centralized headquarter	centralized headquarter

Figure 6 : Marking for Decentralization of smart contract

We can see that Ethereum seems better.

Security of smart contract

(1) [36]Ordinal ranking and marking greed

Ordinal Ranking		Possible mark from better to the worst		
1	Security level	High	Medium	Weak
2	Trustability of "block's validator"	High	Medium	Low
3	Possibility of validator mistake	Low	Medium	High
4	51% attack resistance	High	Medium	Low
5	Quantum computing resistance	High	Medium	Low
6	Potential for the future	High	medium	Low

Figure 7 : Ordinal ranking and marking greed Marking for Security of smart contract

[36] By Author

(2) [37]Marking

attributes/solution		PoW	PoS	DPoS
1	Security level	High	Medium	High
2	Trustability of "block's validator"	High	Low	High
3	Possibility of validator mistake	Low	Medium	Medium
4	51% attack resistance	Medium	High	High
5	Quantum computing resistance	Low	High	High
6	Potential for the future	medium	medium	High

Figure 8 : Marking for Security of smart contract

We can see that DPoS seems better.

Step 4: Sorting and weighting

We will now use the compensatory model to weight the result. Before doing this model, we can already reject one solution, the Ripple one (having a centralized blockchain is completely contrary to the concept of decentralized smart contract itself).

(1) We will first give a weight for each solution following this grid (particular case for viability, four different weights):

Color			
Attribute weight	0	0,5	1

Figure 9: Weight grid[38]

The bigger the weight, the better for the company.

(2) Moreover, then weight these attributes to obtain the relative weighted result.

Decentralization of Smart Contract

(1) [39]Weight:

[37] By Author
[38] By Author
[39] By Author

attributes/solution		Ethereum	NEO	EOS
1	Knowledge and power are decentralized	1	1	1
2	Change are made by consensus	1	1	1
3	Type of blockchain	1	1	1
5	Working group communicate with each other directly	1	0,5	1
6	Who is in charge	0,5	0	0
7	There isn't headquarter	0,5	0	0

Figure 10: Weight: Decentralization of smart Contract

(2) [40]Relative weight:

Attribute	Normalization				Ethereum		NEO		EOS	
	Relative Rank	Normalized Weight (A)			(B)	(A)*(B)	(B)	(A)*(B)	(B)	(A)*(B)
Knowledge and power are decentralized	1	0,285714286	=	0,285714286	1	0,285714286	1	0,285714286	1	0,285714286
Change are made by consensus	2	0,238095238	=	0,238095238	1	0,238095238	1	0,238095238	1	0,238095238
Type of blockchain	3	0,19047619	=	0,19047619	1	0,19047619	1	0,19047619	1	0,19047619
Working group communicate with each other directly	5	0,142857143	=	0,142857143	1	0,142857143	0,5	0,071428571	1	0,142857143
Who is in charge	6	0,095238095	=	0,095238095	0,5	0,047619048	0	0	0	0
There isn't headquarter	7	0,047619048	=	0,047619048	0,5	0,023809524	0	0	0	0
SUM	21		SUM	1	SUM	0,928571429	SUM	0,785714286	SUM	0,857142857

Figure 11: Relative Weight: Decentralization of Smart Contract

With these relative ranks, Ethereum seem to be the best solutions. We will analyse this in the next part: Findings.

Security of smart contract

(1) Weight:

[40] By Author

attributes/solution		PoW	PoS	DPoS
1	Security level	1	0,5	1
2	Trustability of "block's validator"	1	0	1
3	Possibility of validator mistake	1	0,5	0,5
4	51% attack resistance	0,5	1	1
5	Quantum computing resistance	0	1	1
6	Potential for the future	0,5	0,5	1

Figure 12: Weight: Security of smart Contract

(2) [41]Relative Weight:

Attribute	Normalization				PoW		PoS		DPoS	
	Relative Rank	Normalized Weight (A)			(B)	(A)*(B)	(B)	(A)*(B)	(B)	(A)*(B)
Security level	1	0,285714286	=	0,285714286	1	0,285714286	0,5	0,142857143	1	0,285714286
Trustability of "block's validator"	2	0,238095238	=	0,238095238	1	0,238095238	0	0	1	0,238095238
Possibility of validator mistake	3	0,19047619	=	0,19047619	1	0,19047619	0,5	0,095238095	0,5	0,095238095
51% attack resistance	4	0,142857143	=	0,142857143	0,5	0,071428571	1	0,142857143	1	0,142857143
Quantum computing resistance	5	0,095238095		0,095238095	0	0	1	0,095238095	1	0,095238095
Potential for the future	6	0,047619048		0,047619048	0,5	0,023809524	0,5	0,023809524	1	0,047619048
SUM	21		SUM	1	SUM	0,80952381	SUM	0,5	SUM	0,904761905

Figure 13: Relative Weight: Security of Smart Contract

With these relative ranks, DPoS seem to be the best solutions. We will analyse this in the next part: Findings.

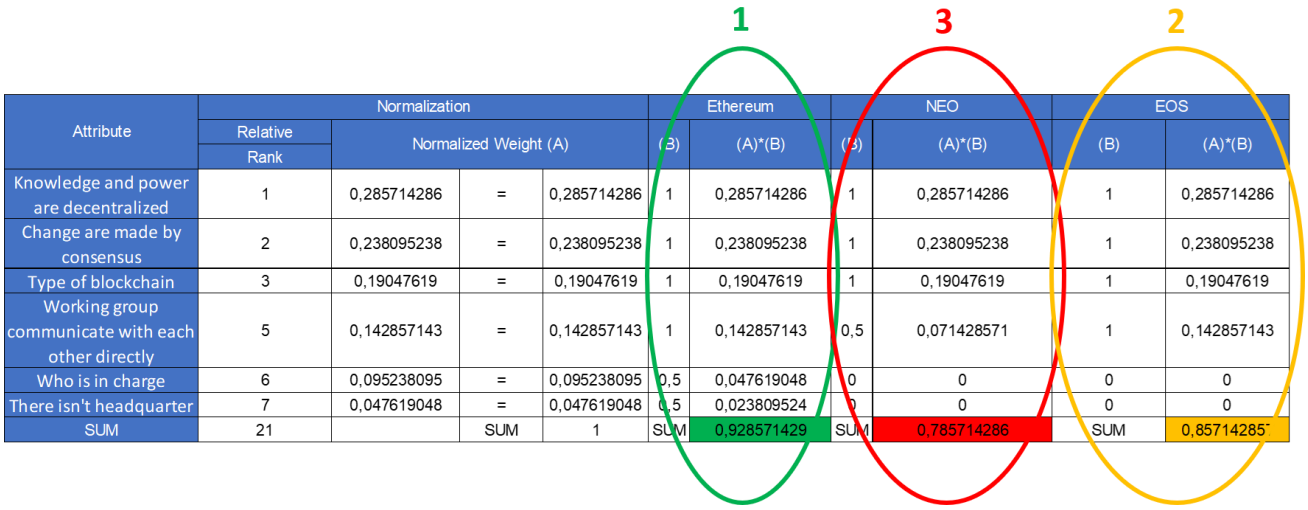
FINDINGS

Step 5: Summarize

Here the rank order we get from the step 4 (from 1 the best to 3 the worst):

Decentralization of Smart Contract

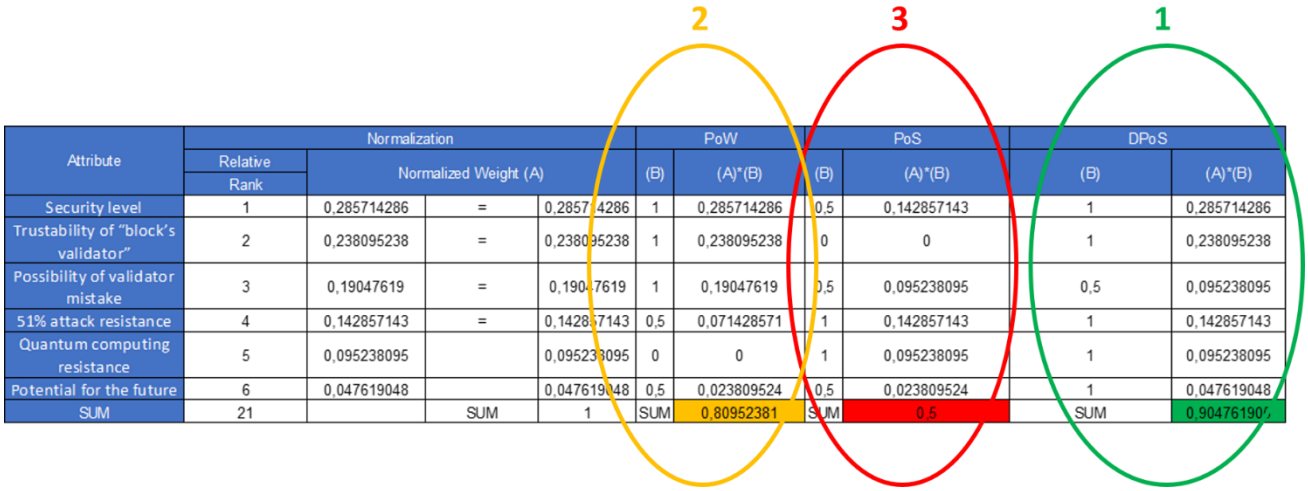
[41] By Author



Attribute	Normalization				Ethereum		NEO		EOS	
	Relative Rank	Normalized Weight (A)			(B)	(A)*(B)	(B)	(A)*(B)	(B)	(A)*(B)
Knowledge and power are decentralized	1	0,285714286	=	0,285714286	1	0,285714286	1	0,285714286	1	0,285714286
Change are made by consensus	2	0,238095238	=	0,238095238	1	0,238095238	1	0,238095238	1	0,238095238
Type of blockchain	3	0,19047619	=	0,19047619	1	0,19047619	1	0,19047619	1	0,19047619
Working group communicate with each other directly	5	0,142857143	=	0,142857143	1	0,142857143	0,5	0,071428571	1	0,142857143
Who is in charge	6	0,095238095	=	0,095238095	0,5	0,047619048	0	0	0	0
There isn't headquarter	7	0,047619048	=	0,047619048	0,5	0,023809524	0	0	0	0
SUM	21		SUM	1	SUM	0,928571429	SUM	0,785714286	SUM	0,85714285

Figure 14 : Rank order for alternative of decentralization of smart contract[42]

Security of smart contract:



Attribute	Normalization				PoW		PoS		DPoS	
	Relative Rank	Normalized Weight (A)			(B)	(A)*(B)	(B)	(A)*(B)	(B)	(A)*(B)
Security level	1	0,285714286	=	0,285714286	1	0,285714286	0,5	0,142857143	1	0,285714286
Trustability of "block's validator"	2	0,238095238	=	0,238095238	1	0,238095238	0	0	1	0,238095238
Possibility of validator mistake	3	0,19047619	=	0,19047619	1	0,19047619	0,5	0,095238095	0,5	0,095238095
51% attack resistance	4	0,142857143	=	0,142857143	0,5	0,071428571	1	0,142857143	1	0,142857143
Quantum computing resistance	5	0,095238095		0,095238095	0	0	1	0,095238095	1	0,095238095
Potential for the future	6	0,047619048		0,047619048	0,5	0,023809524	0,5	0,023809524	1	0,047619048
SUM	21		SUM	1	SUM	0,80952381	SUM	0,5	SUM	0,90476190

Figure 15 : Rank order for alternative of security of smart contract[43]

Following these two ranking, we can exclude NEO and the PoS that are too far behind following the weighting of the step 4.

[42] By author
[43] By author

Step 6: Selection of the preferred alternative

Decentralization of Smart Contract:

Following the step 5, Ethereum seems the best solutions. The NEO solution is too behind And If we compare with EOS on the attribute the differences between the two are the team in charge and the headquarter. "Ethereum is the best solution also thanks to his huge community[44]", bigger than EOS's one.

Knowledge and power are completely decentralized, Ethereum is open source and based on a PoW security protocol (which decentralized power)

Change are always made by consensus, Ethereum only accept hard fork so anytime a change needs to be made it need to be approved by the all community, user and minors.

It's a public blockchain where working group can communicate directly with each other, Ethereum blockchain is making the link between every actor. Smart contract are based on it and are unique for that.

Ethereum is develop by some known developer and also hugely help by decentralized developers all around the world. The team is constantly changing and moving from one place to another.

Security of smart contract:

Following the step 5, DPoS seems to be the best solution. The classic PoS solution is way too behind and if we compare with PoW on the attributes the differences between the two are the possibility of a validator mistake and the resistance to 51% attack and quantum computing.

DPoS is providing a great level of security and an excellent trustability of the block validator. In DPoS the block validator is elected and is the main responsible of the security, he is using a derivate of PoW to validate the different blocks.

The validator is still able to make some mistake, but the probability is really low, he will have to face huge consequence if he validates the wrong block.

DPoS have also a huge resistance to 51% attack because it mean that in a DPoS context you need to own more than 51% of the total stake market value (Ethereum value is today around 16 billions $).

"DPoS are also a solution to quantum computing[45]". Because the power is based on stake owning, quantum computing power have no impact in it.

[44] Ethereum Community Forum. (n.d.). Retrieved from https://forum.ethereum.org/
[45] STUDIOS, B. (n.d.). Quantum Computing and Building Resistance into Proof of Stake. Retrieved from https://bitcoinmagazine.com/articles/quantum-computing-and-building-resistance-proof-stake/

Step 7: Follow up

Those chosen alternatives answers the current contracting challenge and issue. The main problem of contracting it trustability, it's the key base of contracting.

To demonstrate that our recommendation considerably reduces the challenges of the changing environment, we will conduct a before and after Pareto Analysis. According to the Pareto Law, "80% of the problems come from 20% of the potential causes"[46]. We will be focusing on the company efficiency or here inefficiency main causes.

Thus 80% of our problem are caused by Middleman trustability and human interpretation of contract.

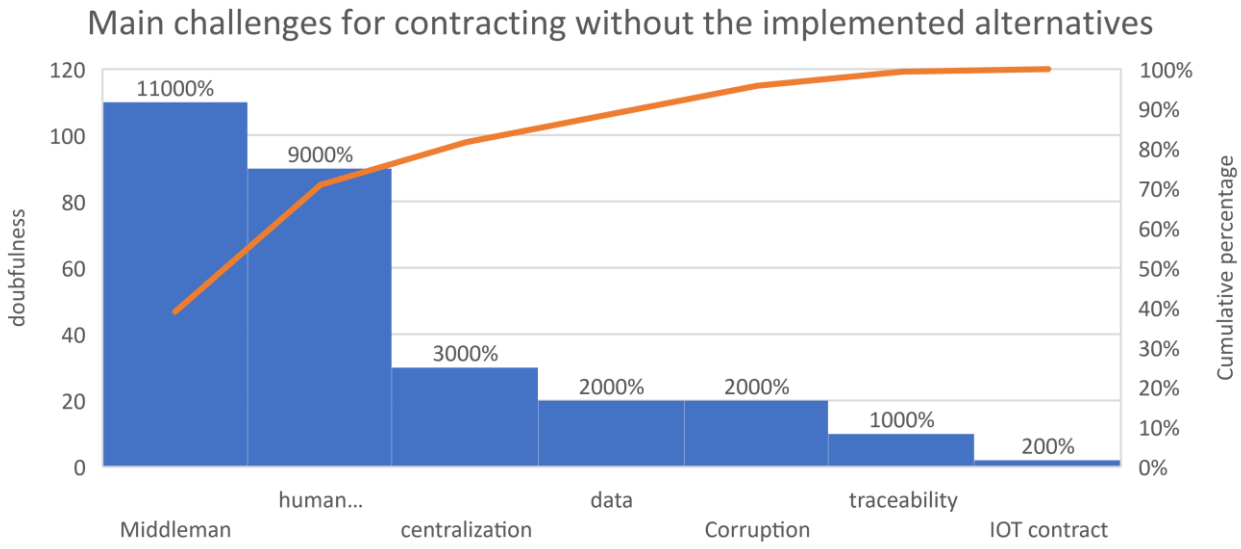


Figure 16: Pareto analysis: Main challenges for contracting without the implemented alternatives[47]

In this first analysis, we can see that middleman trustability and human interpretation of the contract will deeply impact the doubtfulness of a contract.

Let's see now the impact on the trustability of a contract with Smart contract solution. The smart contract can replace the middleman in 90% of the cases and is not subject ot interpretation. "A smart contract is a data fact-based contract[48]" without any possibility of misunderstanding and

[46] GUILD OF PROJECT CONTROLS COMPENDIUM and REFERENCE (CaR) | Project Controls - planning, scheduling, cost management and forensic analysis (Planning Planet). (n.d.). Retrieved from http://www.planningplanet.com/guild/gpccar/risk-opportunity-monitoring-and-control
[47] By Author
[48] What is smart contract? - Definition from WhatIs.com. (n.d.). Retrieved from https://searchcompliance.techtarget.com/definition/smart-contract

rules interpretations. A smart contract is also by nature completely decentralized, traceable and extremely resistant to corruption.

Here Is the new pareto with the impact of the smart contract solution:

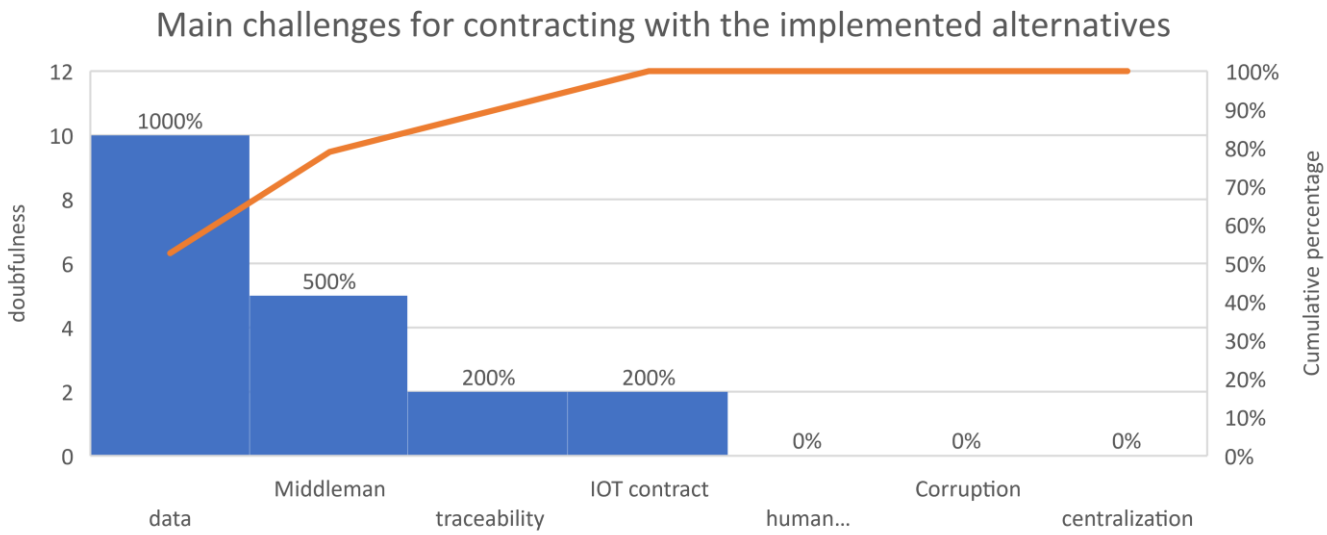


Figure 17: Pareto analysis: Main challenges for contracting with the implemented alternatives[49]

We can see that doubtfulness relating to human interpretation, corruption and centralization have completely disappear. By nature, the smart contract avoids completely those risk of doubtfulness. "It also reduces by 95% the middleman impact, with smart contract only few cases need real middleman[50]".

CONCLUSION

The goal of this paper was to answer the following question: Does the smart contract are the future of contracting. Taking into consideration that smart contract depends on blockchain we have focus on the trilemma dilemma and in particular on the security issue and decentralization. Those 2 criteria are the mains baseline for blockchain and smart contract.

Through this paper we have assessed the reality on two side: security and decentralization. First, we have started with lot of alternative for both sides. Then we have selected through a MADM process: Ethereum was elected for his high capacity of decentralisation and DPoS security protocol was elected for his high level of security. With the Pareto analysis we have seen the

[49] By author
[50] Guida, J. (2018, March 22). Will Smart Contracts be the Death of the Middleman? Retrieved from https://medium.com/@Joebg002/will-smart-contracts-be-the-death-of-the-middleman-7cba39987282

huge positive impact of smart contract on the trustability of a contract. Most of the doubtfulness issue of contract were resolve or highly attenuated.

The ideal smart contract then would have the decentralization of the Ethereum blockchain and the security of the DPoS protocol. Luckily "Ethereum international development team just reveal that they would hard fork the Ethereum blockchain mid-december 2019 [51]"which mean that "Ethereum is going to enter in a new phase and pass from a PoW security protocol to a DPoS protocol.[52]" Did this new improvement will affect the mass adoption of smart contract? How long will it take to use smart contract inside daily use case? Their future seems bright and full of possibilities.

CONCLUSIONS

BIBLIOGRAPHY

- Cassano, J. (2014, September 17). What Are Smart Contracts? Cryptocurrency's Killer App. Retrieved from https://www.fastcompany.com/3035723/smart-contracts-could-be-cryptocurrencys-killer-app

- Chandersekhar, P. (2018, May 23). Ethereum Smart-Contracts: Most of them are rarely used ! Retrieved from https://hackernoon.com/ethereum-smart-contracts-most-of-them-are-rarely-used-f45749730d3e

- "Contracts Ex Machina" by Kevin Werbach and Nicolas Cornell. (n.d.). Retrieved from https://scholarship.law.duke.edu/dlj/vol67/iss2/2/

- Could Blockchain Technology Improve Project Success? - Smart Projex. (2018, January 10). Retrieved from http://www.smartprojex.com/could-blockchain-technology-improve-project-success/

- Formalizing and Securing Relationships on Public Networks | Szabo | First Monday. (n.d.). Retrieved from https://ojphi.org/ojs/index.php/fm/article/view/548/469

- Haapio, H. (n.d.). Visualization: Seeing Contracts for What They Are, and What They Could Become. Retrieved from https://scholarlycommons.law.cwsl.edu/fs/11/

[51] Ethereum Istanbul Hard Fork released date confirmed by core developer - Cointelegraph. (2019, November 8). Retrieved from https://cointelegraph.com/news/ethereum-istanbul-hard-fork-release-date-confirmed-by-core-developer

[52] Ethereum Roadmap Update [2018]: Casper & Sharding Release Date - Mango Research. (2018, October 3). Retrieved from https://www.mangoresearch.co/ethereum-roadmap-update/

- How blockchain will revolutionise far more than money ? Dominic Frisby | Aeon Essays. (2016, April 21). Retrieved from https://aeon.co/essays/how-blockchain-will-revolutionise-far-more-than-money

- How many Ethereum smart contracts are there? - CoinDiligent. (2018, November 8). Retrieved from https://coindiligent.com/how-many-ethereum-smart-contracts

- Medina, E. (n.d.). How is blockchain going to change project management. Retrieved from https://blog.workep.com/how-is-blockchain-going-to-change-project-management

- Nick Szabo. (2018, October 15). Retrieved from https://en.wikipedia.org/wiki/Nick_Szabo

- Smart contract. (2018, November 7). Retrieved from https://en.wikipedia.org/wiki/Smart_contract

- Smart Contracts: Interview with Ethereum on the Future of Contracting. (2015, December 31). Retrieved from https://legal-tech-blog.de/smart-contracts-ethereum-future-of-contracting

- Standard form contracts and a smart contract future. (2018, May 15). Retrieved from https://policyreview.info/articles/analysis/standard-form-contracts-and-smart-contract-future

- STUDIOS, B. (n.d.). Blockchain-Based Architecture For Project Management. Retrieved from https://bitcoinmagazine.com/articles/alehubs-new-blockchain-based-architecture-project-manageme/

- Varadarajan, T. (2017, September 22). The Blockchain Is the Internet of Money. Retrieved from https://www.wsj.com/articles/the-blockchain-is-the-internet-of-money-1506119424?utm_medium=social&utm_source=twitter

- What Are Smart Contracts? A Beginner's Guide to Smart Contracts. (n.d.). Retrieved from https://blockgeeks.com/guides/smart-contracts/

- [1608.00771] Smart Contract Templates: foundations, design landscape and research directions. (n.d.). Retrieved from https://arxiv.org/abs/1608.00771

- David Chaum. (2018, November 12). Retrieved from https://en.wikipedia.org/wiki/David_Chaum

- Solidity — Solidity 0.4.24 documentation. (n.d.). Retrieved from https://solidity.readthedocs.io/en/v0.4.24/

- Falkon, S. (2017, December 24). The Story of the DAO ? Its History and Consequences. Retrieved from https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

- Applicature. (2018, September 3). EOS Smart-Contract Development ? Applicature ? Medium. Retrieved from https://medium.com/applicature/eos-smart-contract-development-a62c66e8faac

- A Deeper Look at Different Smart Contract Platforms (Blockgeeks Guide). (n.d.). Retrieved from https://blockgeeks.com/guides/different-smart-contract-platforms/

- Ethereum Roadmap Update [2018]: Casper & Sharding Release Date - Mango Research. (2018, October 3). Retrieved from https://www.mangoresearch.co/ethereum-roadmap-update/

- Galas, G. (2018, May 14). Analyse et comparaison des mécanismes de consensus dans la blockchain. Retrieved from https://medium.com/@godefroy.galas/analyse-et-comparaison-des-m%C3%A9canismes-de-consensus-dans-la-blockchain-f91aee511ea3

- Guide: Proof of Work (PoW) vs Proof of Stake (PoS) vs Delegated Proof of Stake (DPoS) — Steemit. (n.d.). Retrieved from https://steemit.com/bitcoin/@mooncryption/guide-proof-of-work-pow-vs-proof-of-stake-pos-vs-delegated-proof-of-stake-dpos

- La sécurité des smart contracts Ethereum. (2017, June 7). Retrieved from https://www.ethereum-france.com/la-securite-des-smart-contracts-ethereum/

- Levenson, N. (2017, December 29). Cardano: Ethereum and NEO Killer or Overhyped and Overpriced? Retrieved from https://hackernoon.com/cardano-ethereum-and-neo-killer-or-overhyped-and-overpriced-8fcd5f8abcdf

- NEO White Paper. (n.d.). Retrieved from http://docs.neo.org/en-us/whitepaper.html

- Ray, S. (2018, April 23). The Difference Between Traditional and Delegated Proof of Stake. Retrieved from https://hackernoon.com/the-difference-between-traditional-and-delegated-proof-of-stake-36a3e3f25f7d

- What Is Hyperledger? The Most Comprehensive Guide Ever! (n.d.). Retrieved from https://blockgeeks.com/guides/hyperledger/

- What is Delegated Proof of Stake? (n.d.). Retrieved from https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake

- Daniel Larimer. (2018, December 7). Retrieved from https://en.wikipedia.org/wiki/Daniel_Larimer

- Ripple - One Frictionless Experience To Send Money Globally | Ripple. (n.d.). Retrieved from https://ripple.com/

- Codius - Open-source Hosting Platform for Smart Programs. (n.d.). Retrieved from https://codius.org/

- Proof of work - Bitcoin Wiki. (n.d.). Retrieved December 11, 2018, from https://en.bitcoin.it/wiki/Proof_of_work

- Floyd, D. (2016, September 7). 51% Attack. Retrieved from https://www.investopedia.com/terms/1/51-attack.asp

- What is Proof of Stake? (n.d.). Retrieved from https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-stake

- Ethereum's Geth Software Upgrades Ahead of January Hard Fork - CoinDesk. (2018, December 12). Retrieved from https://www.coindesk.com/ethereums-geth-software-adds-activation-time-for-january-hard-fork

- Stone, A. (2016, December 2). Block and Transaction Validation Analysis? Andrew Stone? Medium. Retrieved from https://medium.com/@g.andrew.stone/proposed-bitcoin-unlimited-excessive-defaults-for-block-validation-326417f944fa

- http://webcache.googleusercontent.com/search'q=cache://www.forbes.com/sites/forbescoachescouncil/2018/08/02/the-future-of-blockchain-and-its-potential-impact-on-our-world/ . (2018, August 2). Retrieved from https://www.forbes.com/sites/forbescoachescouncil/2018/08/02/the-future-of-blockchain-and-its-potential-impact-on-our-world/#16ca7b0e1f69

- Nash, G. (2018, May 7). Beginnings of Bitcoin: The First 3000 ? Crypto Currently ? Medium. Retrieved from https://medium.com/crypto-currently/beginnings-of-bitcoin-the-first-3000-778b8a05b5b

- Ethereum Roadmap Update [2018]: Casper & Sharding Release Date - Mango Research. (2018, October 3). Retrieved from https://www.mangoresearch.co/ethereum-roadmap-update/

- Ethereum Community Forum. (n.d.). Retrieved from https://forum.ethereum.org/

- GUILD OF PROJECT CONTROLS COMPENDIUM and REFERENCE (CaR) | Project Controls - planning, scheduling, cost management and forensic analysis (Planning Planet). (n.d.). Retrieved from http://www.planningplanet.com/guild/gpccar/risk-opportunity-monitoring-and-control

- What is smart contract? - Definition from WhatIs.com. (n.d.). Retrieved from https://searchcompliance.techtarget.com/definition/smart-contract

- Guida, J. (2018, March 22). Will Smart Contracts be the Death of the Middleman? Retrieved from https://medium.com/@Joebg002/will-smart-contracts-be-the-death-of-the-middleman-7cba39987282

- PolySwarm. (2018, April 6). What Smart Contracts Mean for the Future of Business. Retrieved from https://medium.com/polyswarm/what-smart-contracts-mean-for-the-future-of-business-bee84dc629a3

- Smart Contracts and the Future of Financial Operations - DZone Security. (2018, August 29). Retrieved from https://dzone.com/articles/smart-contracts-and-a-future-of-financial-operatio

- Stewart, B. (2018, July 3). Future of Work: Connecting the Real and Digital Worlds via Smart Contract Events. Retrieved from https://medium.com/blackboxtoken/future-of-work-connecting-the-real-and-digital-worlds-via-smart-contract-events-7d924a21d22d

- Tan, E. (2018, April 8). The Evolution of Smart Contracts ? Hacker Noon. Retrieved from https://hackernoon.com/are-smart-contracts-the-future-1d9028f49743

About the Author

Baptiste Lestienne

Lille, France

Baptiste Lestienne is 22 years old French student. Recently graduated of ITEEM Centrale Lille Master speciality industry and entrepreneurship option Logistics. He had pursued in parallel a Master of Science degree in Project and Programme Management and Business Development at Skema Business School, Lille Campus.

His schools provide him a complete dual competence in engineering and commerce and made him completely able to work into complex project. He is certified AgilePm, Prince2 and passed the TOEIC (840).

He is currently working for Accenture Consulting as technology advisory analyst in the financial services. He helps banks, capital markets and insurance firms create business value through technology. He also helps clients to capture the value trapped in existing and emerging technologies, such as cloud and artificial intelligence, and use these assets to drive operational efficiency and strengthen business models.

He has integrated Decathlon Philippines for his 8 months internships. He laid the supply chain and logistic foundation with the initial decathlon team to open the very first Decathlon in Philippines. His tutor and him were handling the logistic and supply chain part of the opening: finance, custom, products, transport warehousing, deliveries, supply chain, recruitment and management.

He is highly interested and passionate about new technologies in particularity about blockchain technologies and cryptocurrency: How the financial world is changing and will change. Blockchain is one of the key technologies which will change the next decade.

Through many projects in different fields, he developed a strong experience in project management and business development. He is optimist, engaged and hard-working. He is a great team member but is also able to manage a long-term project and demonstrate leadership.

Baptiste lives in Lille and Paris, France and can be contacted at Baptlestienne@gmail.com
You can have further information about his experience on his LinkedIn profile: https://www.linkedin.com/in/baptiste-lestienne/