Université Libre de Bruxelles

Computer Science Department

INFO-F530 Computer science seminar

Report of

Seminar 2

Blockchain, Opportunities and challenges

—

Use case FAB Framework:

Solving the Scalability Dilemma to Enable High Performance Enterprise Applications

(by Mohamed El Kandri – March 19, 2018 [El 18])

Olivier Pirson – opi@opimedia.be

Master 2

June 4, 2018

Contents

(Illustration of the title page from [El 18].)

1 Provide an outline of the content of the seminar in your own words.

Today almost everybody talks about blockchains. And it is probably only the beginning. The number of *cryptocurrencies* [1], and other applications build on them are growing strongly. The total market capitalization of all cryptocurrencies was really exploded in the last two years! And the forecasts is that will have a big impact on the economy. A lot of companies, organizations, countries, etc. work on some use of this, or want to work on this. It is difficult to know how many people invest for business perspectives and how many invest for research perspectives, and a lot of tries failed; but maybe it's a revolution on the move. "*Virtually every industry & aspect of society will be affected*". [El 18]

Technically a *blockchain* [2] is a list of *blocks*. Each block recording information and contains a date/time and a hash of the previous block that ensures by design the resistance of the modification of the information. The list is distributed on a decentralized network and provides a decentralized consensus system usable for transactions that require trust. Trust is based on mathematics instead authority or intermediary.

Not technically a blockchain can be defined by these properties: "*What I see is what you see, and we both know that we see the same thing, and we both know that this is what has been reported to the regulator.*" (Richard Brown, CTO of R3 [4]) [5]

Today there is more centralization than decentralization. The promise according to Mohamed El Kandri [El 18] it will be the opposite in the future.

For some uses it can be interesting to restrain the access to not publicly expose all information. For that some private blockchains are build. But they loose the spirit of blockchain, the decentralization.

The decentralization is the cornerstone that potentially provides a lot of benefits, like the resistance to abuse of trust and power, corruption, censorship, etc. That could "*change how we organize and interact with one another*". [El 18]

This resistance is possible because some computer work is required to validate transactions (*Proof-of-work*, PoW) and the required power is enough to normally prevent attack. [7]

The cryptocurrencies are the first generation of blockchain applications. The applications of the second generation are the smart contracts. They are contracts that can be (at least partially) executed or enforced automatically . The third generation could be touch all sector activities.

All that possibilities are wonderful, but there is a big issue. These processes are too slow to work at a very large scale.

Mohamed El Kandri finished its talk by the presentation [FAB18] of a solution to remove this bottleneck without loose desirable properties. FAB, for Fast Access Blockchain [El] is a public blockchain application platform with a very high speed. This goal is achieved by the design of subsets of blockchain for specific applications.

[1] A decentralized digital money build with strong cryptography.

[2] This technology was originally invented by the creator of the cryptocurrency Bitcoin [3] to build it.

[3] https://bitcoin.org/en/

[4] https://www.r3.com/

[5] In fact he said that about Corda [6]. [Åsl16]

[6] https://www.corda.net/

[7] Other consensus systems like *Proof-of-stake* (PoS) are studied but it is not clear today what it is possible or not.

2 Which were the major points discussed by the speaker? List and explain their importance.

- What it can be possible to use, not how build it.

  Mohamed El Kandri talked about the possible applications instead to explains the theory or the technology.

  "*Value is not about the technology, value is also about the business value.*" [El 18]

- Decentralization: the spirit of the blockchains.

  Like already mentioned the decentralization is the cornerstone of this technology. Without enough decentralization it is not possible to ensure the desirable properties of the system.

  Note that the decentralization is also the spirit of Internet and some concentrations threat it. Note also that the today importance of social networks and the centralization of major of them is a big problem which should be solved by the use of open and decentralized social networks like diaspora* [8] and Mastodon [9].

- Big issue of scalability.

  The principles used to ensure the resistance of the modification of the information have a harmful consequence: the process is too slow to be use in a large scale. This technological challenge maybe could be resolved in different ways. It is opportunity to make research.

3 For which discipline in computer science is the topic relevant and why (explain)?

The blockchain technology implies knowledge on several computer science disciplines: network, cryptography, security, algorithmic, language [10] , etc.

So the necessary researches on these disciplines to improve existing blockchain knowledge may be also change all these computer science disciplines. Especially if the blockchain revolution (from the applications point of view) is coming.

4 Suggest two or three articles discussing similar work (not necessarily published by the speaker). Explain why they are related.

- *Bitcoin: A peer-to-peer electronic cash system* [Nak08]

  The seminal paper by Satoshi Nakamoto [11] that created the first decentralized cryptocurrency called Bitcoin and the first blockchain to build it.

[8] https://diasporafoundation.org/

[9] https://joinmastodon.org/

[10] The project Ethereum proposes a Turing-complete programming language for smart contracts.

[10] https://www.ethereum.org/

[11] A pseudonym for an unknown person or maybe a group of unknown persons.

- *On Stake and Consensus* [Poe15]

  This paper by Andrew Poelstra is an updated version of an analyse by the same author of the feasibility of proof-of-stake as an alternative to the heavy proof-of-work. The author claims that *"proof-of-stake and similar mechanisms are fundamentally unable to produce a distributed consensus within Bitcoin's trust model."* [Poe15] It seems that the scientific community needs time to clarify that.

- The dossier of *Pour la Science* mentioned after the seminar: *Les nouveau monde des cryptomonnaies et des blockchains* [Pav18], *Faire sauter la banque avec des cryptomonnaies* [LP18], *La blockchain, instrument de confiance ?* [Smo18]

5 Propose two scientific questions relevant for the topic discussed in this seminar.

- This new technology promises a lot of wonderful possibilities for the common interest. But probably a lot of want to use it are dictated by personal interests. Are there some scientific studies on this human issue? Economic studies, sociological studies, maybe other studies?

- What is the paper with the most pessimistic point of view about the promises of this technology but nevertheless well argued? In other words, can you presented the minimum changes that will be sure in the future with this technology? The worst case scenario.

6 Would you like to know more about this field? Do you have particular critiques about the scientific content? Provide a brief motivation for your answers.

This talk was more a presentation of the huge potential of the blockchains than a scientific presentation of this technology.

Even if the blockchain do not will all their promises, this technology will become probably very important, so it seems to me that is crucial to have some knowledge about it.

There is a recent podcast called *ProofOfCast* [Cha] about this topic in French, with the Belgian Lionel Dricot [12] like contributor. It is a pleasant way to have news. It was in an episode that I learned the existence of the question of the feasibility or not of the proof-of-stake.

[12] https://uclouvain.be/crypto/people/show/531

References

[Åsl16] Oskar Erik Åslund. **Confronting the Blockchain - Incumbents' Active Involvement in Disruptive Niche Innovations**. Master's thesis. 2016. url: https://www.duo.uio.no/handle/10852/55347 (cit. on p. 2).

[Cha] ChainSkills. **ProofOfCast**. url: http://chainskills.com/category/proofofcast/ (cit. on p. 4).

[El] Mohamed El Kandri. **FAB: Fast Access Blockchain**. url: https://fabcoin.co/ (cit. on p. 2).

[El 18] Mohamed El Kandri. **Blockchain, Opportunities and challenges – Use case FAB Framework: Solving the Scalability Dilemma to Enable High Performance Enterprise Applications**. Université Libre de Bruxelles, Mar. 19, 2018. url: http://bit.ly/2Jk9qFr (cit. on pp. 1–3).

[FAB18] FAB Coin Info. **How does Fast Access Blockchain FAB work?** 2018. url: https://www.youtube.com/watch?v=Kh4m0vqNP9Y (cit. on p. 2).

[LP18] Alexander Lipton and Alex Pentland. **Faire sauter la banque avec des cryptomonnaies**. In: *Pour la Science* 485 (Mar. 2018), pp. 36–42 (cit. on p. 4).

[Nak08] Satoshi Nakamoto. **Bitcoin: A peer-to-peer electronic cash system**. Oct. 2008. url: https://bitcoin.org/bitcoin.pdf (cit. on p. 3).

[Pav18] John Pavlus. **Les nouveau monde des cryptomonnaies et des blockchains**. In: *Pour la Science* 485 (Mar. 2018), pp. 28–34 (cit. on p. 4).

[Poe15] Andrew Poelstra. **On Stake and Consensus**. Mar. 22, 2015, p. 12. url: https://nakamotoinstitute.org/research/on-stake-and-consensus/ (cit. on p. 4).

[Smo18] Natalie Smolenski. **La blockchain, instrument de confiance ?** In: *Pour la Science* 485 (Mar. 2018), pp. 44–47 (cit. on p. 4).