

Francesco Corea [Follow](#)

Complexity scientist, data strategist, tech investor and AI advisor. All opinions are my own.

Dec 1 · 14 min read

The convergence of AI and Blockchain: what's the deal?

Why a decentralized intelligence may affect our future



Image Credit: Zapp2Photo/Shutterstock

It is undeniable that AI and blockchain are two of the major technologies that are catalyzing the pace of innovation and introducing radical shifts in every industry. Each technology has its own degree of technical complexity as well as business implications but the joint use of the two may be able to redesign the entire technological (and human) paradigm from scratch.

This article wants to give a flavor of the potentialities realized at the intersection of AI and Blockchain and discuss standard definitions, challenges, and benefits of this alliance, as well as about some interesting player in this space.

...

I. Setting the stage

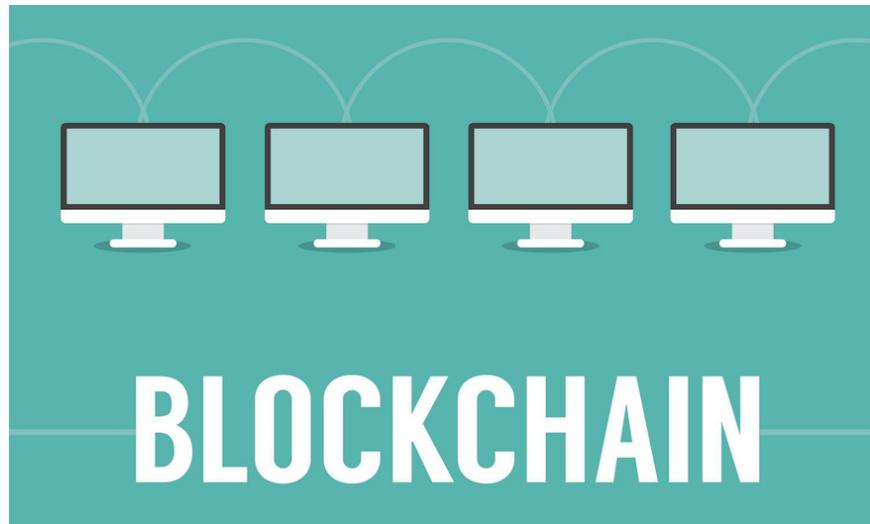


Image Credit: 4zevar/Shutterstock

I have been talking and writing about AI since a while now, so I will not waste any time defining what it is and what is not (if you want to know more about it, you can check [my explanation](#) or a [brief history of AI](#)).

However, I never touched upon blockchain and cryptocurrencies so far, so I will dedicate this first block to describe what it is and how it works.

A blockchain is a **secure distributed immutable database shared by all parties in a distributed network** where transaction data can be recorded (either *on-chain* for basic information or *off-chain* in case of extra attachments) and easily audited.

A blockchain is a secure distributed immutable database shared by all parties in a distributed network

Put simply (with Bank of England's words), the blockchain is “*a technology that allows people who don't know each other to trust a shared record of events*”.

The data are stored in rigid structures called **blocks**, which are connected to each other in a **chain** through a **hash** (each block also

includes a *timestamp* and a link to the previous block via its *hash*). The blocks have a header, which includes metadata, and a content, which includes the real transaction data. Since every block is connected to the previous one, as the number of participants and blocks grow, it is extremely hard to modify any information without having the network consensus.

The network can validate the transaction through different mechanisms, but mainly through either a “*proof-of-work*” or a “*proof-of-stake*”. A **proof-of-work** (Nakamoto, 2008) asks the participants (called “*miners*”) to solve complex mathematical problems in order to add a block, which in turn require a ton of energy and hardware capacity to be decoded. A **proof-of-stake** (Vasin, 2014) instead tries to solve this energy efficiency issue attributing (roughly) more mining power to participants who own more coins (there are many variations of it and some skepticism around its famous “*nothing at stake*” problem —see [Buterin’s blog post](#) to know more on this).

Additional mechanisms are the Byzantine-fault-tolerant algorithm (Castro and Liskov, 2002), the Quorum slicing (Mazieres, 2016), as well as variations of the Proof-of-stake (Mingxiao et al., 2017), but we will not get into those now.

The final characteristic that needs to be explained is the category of blockchain based on the different network access permission, i.e., whether it is free for anyone to view it (**permissionless vs permissioned**) or to participate in the consensus formation (**public vs private**). In the former case, anyone can access and read or write data from the ledger, while in the latter one predetermined participants have the power to join the network (and of course only in the public permissionless case a reward structure for miners has been designed).

It should be clear by now the intrinsic power of this technology, which is not simply a disruptive innovation but rather a *foundational technology* that aims to “*change the scope of intermediation*” (Catalini and Gans, 2017). Distributed ledger technologies will indeed reduce both the costs of verification and networking, influencing then the market structure and eventually allowing the creation of new marketplaces. Iansiti and Lakhani (2017) also drew a brilliant parallel between blockchain and TCP/IP in a recent work (which I highly recommend), showing how blockchain is slowly going through the four

phases that identify previous foundational technologies such as the TCP/IP, i.e., single-use, localized use, substitution, and transformation. As they explained, the “*novelty*” of such a technology makes it harder for people to understand the solution domain, while its “*complexity*” requires a larger institutional change to foster an easy adoption.

However, it is also true that the blockchain is shifting the traditional business models distributing value in an opposite way with respect to previous stacks: if it made more sense to invest in applications rather than protocol technologies fifteen years ago, in a blockchain world the value is concentrated in the shared protocol layer and only marginally at the application level (see the “***Fat Protocol***” theory by Joel Monegro).

It's a stack with "fat" protocols and "thin" applications (Joel Monegro).

To conclude this introductory section, I will just mention on the fly the possibility for the blockchain to not simply allow for transactions but also the possibility to create (**smart**) **contracts** that are triggered by specific events and threshold and that are traceable and auditable without effort.

• • •

Bonus Paragraph: Initial Coin Offerings (ICOs)

A big hype is nowadays surrounding this new phenomenon of the *Initial Coin Offerings* (ICOs). Even if many people are pouring money into that because of its resemblance to the most common (and valuable) Initial Public Offerings (IPOs), an ICO is nothing more than a **token sale**, where a token is the *smallest functional unit of a specific network* (or application).

ICOs experts (if any) will forgive my approximate definition, but an ICO is a hybrid concept that has elements of a **shares allocation**, a **pre-sales/crowdfunding** campaign, and a **currency** with a limited power and application’s domain.

It is definitely an interesting innovation that introduces new unregulated ways to raise capitals, but it also poses several issues to an unprepared community. I am happy to receive feedback on this, but I would distill the key points of an ICO evaluation in what follows:

- a token has an additional utility with respect to the exchange of value and companies selling token with the **only goal of raising capital are sending a bad signal** to the market. Tokens are needed to create a users' base and to incentivize stakeholders to participate in the ecosystem at the earliest stage. **A good white paper is not enough;**
 - Be wary of token sales that are **uncapped**;
 - Be wary of token sales that have **no time limit**;
 - Be wary of token sales that do not clearly state the (present and future) **number** as well as the **value of the token** (it could sound absurd, but you may be surprised of how non-transparent an ICO can look like).
- . . .

II. How AI can change Blockchain

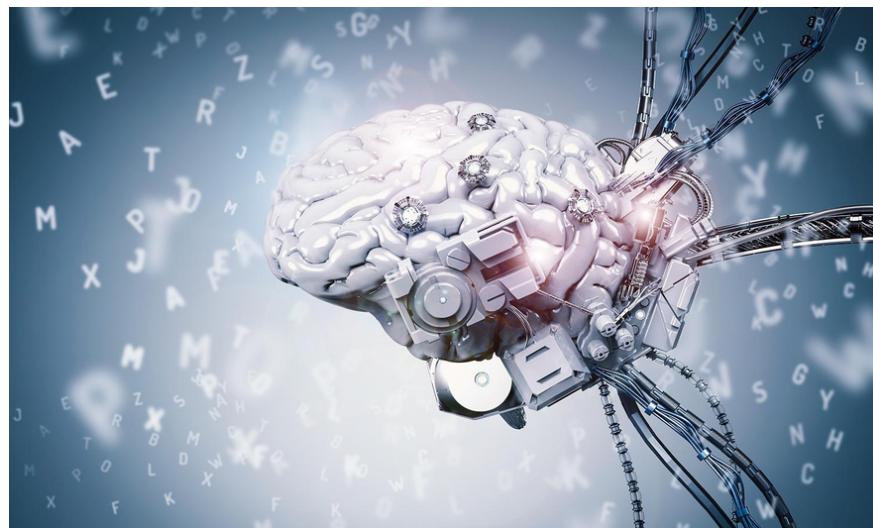


Image Credit: Phonlamai Photo/Shutterstock

Although extremely powerful, a blockchain has its own limitations as well. Some of them are technology-related while others come

from the old-minded culture inherited from the financial services sector, but all of them can be affected by AI in a way or another:

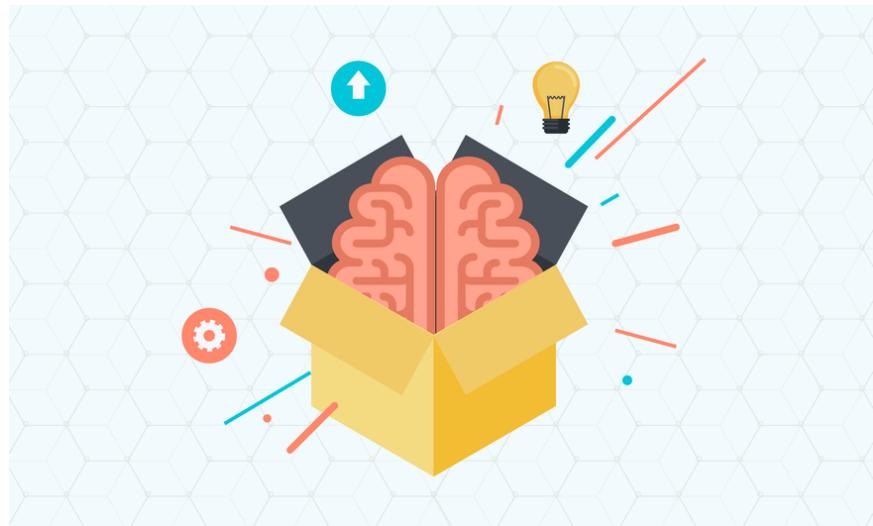
- **Energy consumption:** *mining* is an incredibly hard task that requires a ton of energy (and then money) to be completed (O'Dwyer and David Malone, 2014). AI has already proven to be very efficient in optimizing energy consumption, so I believe similar results can be achieved for the blockchain as well. This would probably also result in lower investments in mining hardware;
- **Scalability:** the blockchain is growing at a steady pace of 1MB every 10 minutes and it already adds up to 85GB. Satoshi (2008) first mentioned “*blockchain pruning*” (i.e., deleting unnecessary data about fully spent transactions in order to not hold the entire blockchain on a single laptop) as a possible solution but AI can introduce new decentralized learning systems such as **federated learning**, for example, or new data sharding techniques to make the system more efficient;
- **Security:** even if the blockchain is almost impossible to hack, its further layers and applications are not so secure (e.g., the DAO, Mt Gox, Bitfinex, etc.). The incredible progress made by machine learning in the last two years makes AI a fantastic ally for the blockchain to guarantee a secure applications deployment, especially given the fixed structure of the system;
- **Privacy:** the privacy issue of owning personal data raises regulatory and strategic concerns for competitive advantages (Unicredit, 2016). *Homomorphic encryption* (performing operations directly on encrypted data), the **Enigma project** (Zyskind et al., 2015) or the **Zerocash project** (Sasson et al., 2014), are definitely potential solutions, but I see this problem as closely connected to the previous two, i.e., scalability and security, and I think they will go *pari passu*;
- **Efficiency:** Deloitte (2016) estimated the total running costs associated with validating and sharing transactions on the blockchain to be as much as \$600 million a year. An intelligent system might be eventually able to compute on the fly the likelihood for specific nodes to be the first performing a certain task, giving the possibility to other miners to shut down their efforts for that specific transaction and cut down the total costs.

Furthermore, even if some structural constraints are present, a better efficiency and a lower energy consumption may reduce the **network latency** allowing then faster transactions;

- **Hardware:** miners (and not necessarily companies but also individuals) poured an incredible amount of money into specialized hardware components. Since energy consumption has always been a key issue, many solutions have been proposed and much more will be introduced in the future. As soon as the system becomes more efficient, some piece of hardware might be converted (sometimes partially) for neural nets use (the mining colossus Bitmain is doing exactly this);
- **Lack of talent:** this is leap of faith, but in the same way we are trying to automate data science itself (unsuccessfully, to my current knowledge), I don't see why we couldn't create virtual agents that can create new ledgers themselves (and even interact on it and maintain it);
- **Data gates:** in a future where all our data will be available on a blockchain and companies will be able to directly buy them from us, we will need help to grant access, track data usage, and generally make sense of what happens to our personal information at a computer speed. This is a job for (intelligent) machines.

. . .

III. How Blockchain can change AI



<https://datafloq.com/read/how-cognitive-computing-can-revolutionize-business/3317>

In the previous section, we quickly touched upon the effects that AI might eventually have on the blockchain. Now instead, we will make the opposite exercise understanding what impact can the blockchain have on the development of machine learning systems. More in details, blockchain could:

- **Help AI explaining itself (and making us believe it):** the AI black-box suffers from an explainability problem. Having a clear audit trail can not only improve the **trustworthiness** of the data as well as of the models but also provide a clear route to trace back the machine decision process;
- **Increase AI effectiveness:** a secure data sharing means more data (and more training data), and then better models, better actions, better results...and better new data. Network effect is all that matter at the end of the day;
- **Lower the market barriers to entry:** let's go step by step. Blockchain technologies can secure your data. So why won't you store all your data privately and maybe sell it? Well, you probably will. So first of all, blockchain will foster the **creation of cleaner and more organized personal data**. Second, it will allow the emergence of **new marketplaces**: a *data marketplace* (low-hanging fruit); a *models marketplace* (much more interesting); and finally even an *AI marketplace* (see what **Ben Goertzel** is trying to do with SingularityNET). Hence, easy data-sharing and new marketplaces, jointly with blockchain data verification, will

provide a more fluid integration that lowers the barrier to entry for smaller players and shrinks the competitive advantage of tech giants. In the effort of lowering the barriers to entry, we are then actually solving two problems, i.e., providing a **wider data access** and a more efficient **data monetization mechanism**;

- **Increase artificial trust:** as soon as part of our tasks will be managed by autonomous virtual agents, having a clear audit trail will help **bots to trust each other** (and us to trust them). It will also eventually increase every **machine-to-machine interaction** (Outlier Ventures, 2017) and transaction providing a secure way to share data and coordinate decisions, as well as a robust mechanism to reach a quorum (extremely relevant for swarm robotics and multiple agents scenarios). **Rob May** expressed a similar concept in one of his last newsletters (that I highly recommend—you should definitely subscribe);
- **Reduce catastrophic risks scenario:** an AI coded in a DAO with specific smart contracts will be able to only perform those actions, and nothing more (it will have a limited action space then).

In spite of all the benefits that AI will receive from an interaction with blockchain technologies, I do have one big question with no answer whatsoever.

AI was born as in an open-source environment where data was the real moat. With this data democratization (and open-source software) how can we be sure that AI will prosper and will keep being developed? What would be the new moat? My only guess at the moment? Talent...

• • •

IV. Decentralized Intelligent Companies



Image Credit: Wit Olszewski/Shutterstock

There are plenty of landscapes of blockchain and cryptocurrencies startups out there. I am anyway only interested in those companies working at the intersection (or the *convergence*, as someone calls it) of AI and blockchain, which apparently are not that many. They are mainly concentrated in San Francisco area and London, but there are examples in New York, Australia, China, as well as some European countries.

They are indeed so few of them that is quite hard to classify them into clusters. I usually like to try to understand the underlying patterns and the type of impact/application certain groups of companies are having in the industry, but in this case is extremely difficult given the low number of data points so I will simply categorize them as follows:

- **Decentralized Intelligence:** TraneAI (training AI in a decentralized way); Neural (peer-to-peer AI supercomputing); SingularityNET (AI marketplace); Neuromation (synthetic datasets generation and algorithm training platform); AI Blockchain (multi-application intelligence); BurstIQ (healthcare data marketplace); AtMatrix (decentralized bots); OpenMined project (data marketplace to train machine learning locally);
- **Conversational Platform:** Green Running (home energy virtual assistant); Talla (chatbot); doc.ai (quantified biology and healthcare insights);

- **Prediction Platform:** Augur (collective intelligence); Sharpe Capital (crowd-source sentiment predictions);
- **Intellectual Property:** Loci.io (IP discovery and mining);
- **Data provenance:** KapeIQ (fraud detection on healthcare entities); Data Quarka (facts checking); Priops (data compliance); Signzy (KYC)
- **Trading:** Euklid (bitcoin investments); EthVentures (investments on digital tokens). For other (theoretical) applications in finance, see Lipton (2017);
- **Insurance:** Mutual.life (P2P insurance), Inari (general);
- **Miscellaneous:** Social Coin (citizens' reward systems); HealthyTail (pet analytics); Crowdz (e-commerce); DeepSee (media platform); ChainMind (cybersecurity).

A few general comments:

- It looks interesting that many AI-blockchain companies have **larger advisory board than teams**. It might be an early sign that the *convergence* is not fully realized yet and there are more things we don't understand than those ones we know;
- I am personally very excited to see the development of the first category (**decentralized intelligence**) but I also see a huge development in **conversational** and **prediction platforms** as well as **intellectual property**. I grouped other examples under "miscellaneous" because I don't think at this stage they represent a specific category but rather only single attempt to match AI and blockchain;
- **Those companies are incredibly hard to evaluate.** The websites are often cryptic enough to not really understand what they do and how (a bit paradoxical if you want to buy the blockchain transparency paradigm) and technology requires a high tech-education to be fully assessed. Cutting through the hype is a demanding task and this makes it very easy to be fooled. But let me give you a concrete example: **ever heard of Magos AI?** In the effort of researching companies for this post, I found myself reading several articles on this forecasting blockchain AI-driven platform company (Wired, Prnewswire, etc.), which just did an

ICO for over half a million dollars and that made great promises on its deliverables. The website didn't work—weird, if you consider that they need to share material/information on the ICOs. But you know, it might happen. I made then an extra effort because I read it on Wired and I was curious to know more about it. I was able to find its co-founders, which I couldn't find eventually on LinkedIn. Weird again. Well, there are people who do not like socials, fair enough, especially if you consider that until three months ago there was no proof of the company existence whatsoever. Let me look into the rest of the team. Nothing even there, and no traceable indications of their previous experiences (except for the CTO master in analytics, that I found no proof of). I tried to then dig into the technology: white papers, blue papers, yellow papers, you name it. I only found reviews of them, no original copies. Final two steps: I don't consider myself an expert in blockchain at all, but I read, a lot. And I also believe I am fairly knowledgeable when it comes to AI and what is happening in the industry. These guys claimed they created 5 different neural nets that could achieve the same accuracy in complex different domains than Libratus (or DeepStack) reached in Poker, but I never heard of them—very weird. Well, you know what? Maybe I could write them and meet them to understand. Their address points to the AXA office in Zurich. Ah.

After 5 minutes of research, I finally Google the two key words: "Magos scam". It seems these guys took the money and disappeared. They are surely building the 6 neural net somewhere, so stay tuned.

My point here is that exponential technologies are fantastic and can advance mankind, but as much as the benefits increase also the potential "*negative convergence*" increases exponentially. Stay alert.

V. Conclusion

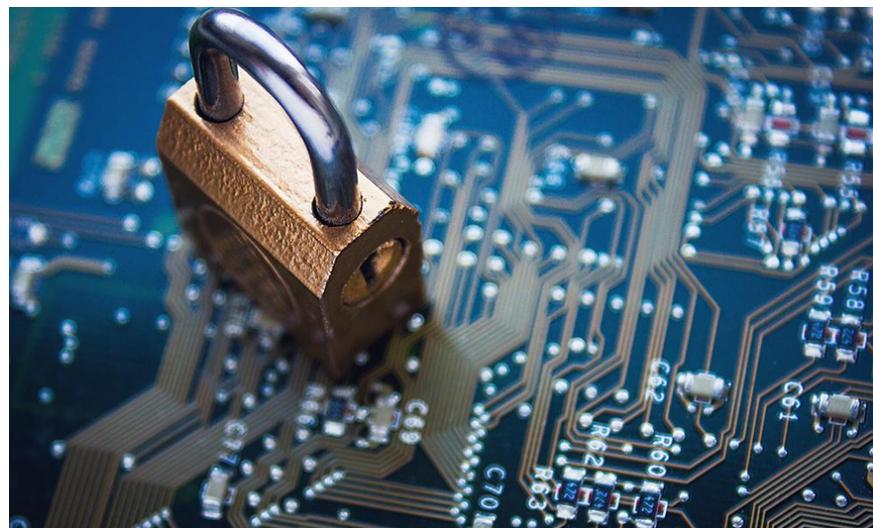


Image Credit: Sasun Bughdaryan/Shutterstock

Blockchain and AI are the two extreme sides of the technology spectrum: one fostering centralized intelligence on close data platforms, the other promoting decentralized applications in an open-data environment. However, if we find an intelligent way to make them working together, the total positive externalities could be amplified in a blink.

There are of course technical and ethical implications arising from the interaction between these two powerful technologies, as for example how do we edit (or even forget) data on a blockchain? Is an editable blockchain the solution? And is not an AI-blockchain pushing us to become data hoarder?

Honestly, I think the only thing we can do is keep experimenting.

References

Castro, M., Liskov, B. (2002). “Practical Byzantine Fault Tolerance and Proactive Recovery”. *ACM Transactions on Computer Systems*, 20(4): 398–461.

Catalini, C., Gans, J. S. (2017). “Some Simple Economics of the Blockchain”. *MIT Sloan School Working Paper*: 5191–16.

Deloitte (2016). “Blockchain Enigma. Paradox. Opportunity”. *White Paper*.

Iansiti, M., Lakhani, K. R. (2017). “The Truth About Blockchain”. *Harvard Business Review*, January–February 2017: 118–127.

Lipton, A. (2017). “Blockchains and Distributed Ledgers in Retrospective and Perspective”. [arXiv:1703.01505](https://arxiv.org/abs/1703.01505).

Mazieres, D. (2016). “The stellar consensus protocol: A federated model for internet-level consensus”. *White Paper*.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C. (2017). “A Review on Consensus Algorithm of Blockchain”. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* Banff Center, Banff, Canada, October 5–8, 2017

Nakamoto, S. (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System”. *White Paper*.

O'Dwyer, K. J., Malone, D. (2014). “Bitcoin mining and its energy footprint”. *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISCC 2014/CIIC 2014)*, Limerick, pp. 280–285.

Outlier Ventures (2017). “Blockchain-Enabled Convergence”. *White Paper*.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M. (2014). “Zerocash: Decentralized anonymous payments from bitcoin”. In *Security and Privacy (SP)*, 2014 IEEE Symposium on, pp. 459–474.

Unicredit (2016). “Blockchain Technology and Applications from a Financial Perspective”. *Technical Report*.

Vasin, P. (2014). “BlackCoin's Proof-of-Stake Protocol v2”. *White Paper*.

Zyskind, G., Nathan, O., Pentland, A. (2015). “Enigma: Decentralized computation platform with guaranteed privacy”. [arXiv:1506.03471](https://arxiv.org/abs/1506.03471).

