BTRM

The Certificate of Bank Treasury Risk Management

Is Blockchain the real failure?

Thought Leadership Series #8

Dr Periklis Thivaios CFA FRM BTRM

January 2023

The bankruptcy of FTX and other recent crypto ecosystem failures have not shaken the pervasive belief in the value and potential of blockchain, the technology underlying cryptos. Yet, blockchain applications have (up until now, at least) failed to transform – let alone disrupt – any industry, despite the billions of dollars invested in the technology over the past decade.

This article takes a slightly contrarian view summarised as follows:

- Cryptos are here to stay. They don't need anyone's permission to exist and support real use cases (money laundering and fraud included), regardless of whether we deem such uses acceptable or not.
- We should not get excited about blockchain because we believe in cryptos, nor should we fall in the trap of assuming that blockchain is valuable even if cryptos are not perceived to be.
- Instead, we should frame the future of blockchain in the context of what this technological method can do well, instead of what it could do.
- Due to their design, blockchain based solutions are suited to support only a narrow and rather specific set of challenges.

This conclusion is not a criticism of blockchain, but of our unfounded exuberance to apply the technology to problems it was not designed to solve.

Some recent high profile (yet low publicity) blockchain failures

In the midst of the FTX saga, little attention was paid to the expensive failure of the blockchain implementation at Australia's ASX. Almost 5 years and hundred million dollars of investment after the evangelical initial press release, the project was put on hold and the capitalised software investment was written off.

The ASX debacle is only the latest amongst a stream of similar project failures or technology pivots. For example, Trade Finance was another area where distributed ledger technologies (DLT) were envisioned to be the solution for the highly manual and multi-party nature of the process. Yet, despite well intended predictions that "Blockchain could well become the future of trade infrastructure and the biggest disruptor [...] since the invention of the container", such endeavours failed to succeed. This year alone, we.trade went into liquidation and several other trade finance platforms opted to pivot away from blockchain based approaches.

We could continue this list for a long time, as examples abound: in November 2022, Maersk and IBM decided to discontinue TradeLens; HP's celebratory "enterprise-grade blockchain deployments" page was last updated in 2019; the hailed State of Delaware Blockchain Initiative (DBI) equally seems to be dead; and so on and so forth.

Of course, this is not to say that all blockchain implementations have failed; nor that the main cause of project failures has been the choice of technology alone. Yet when one reads about successful blockchain projects, such as Walmart Canada's supply chain management system or the management of land registries, one should still question whether blockchain is the most efficient and effective approach.

Cryptos are here to stay (at least some of them)

Being 'bearish' about blockchain yet seeing a future for cryptos may sound paradoxical. However, and despite loud arguments to the contrary, cryptos are useful indeed. Even if we follow the critics' line of argumentation, the facilitation of illicit transactions and speculation are real use cases – whether we like them or not.

In addition, central bank digital currencies (CBDCs) – whether blockchain based or, more likely, not – may have the potential to increase the efficiency of cross border transactions but will not address a related genuine problem: facilitating the legitimate remittance of cash to all countries. Few, if any, central banks will allow their CBDC settlement systems to offer money transfers to family members in Iran and the recent withdrawal of correspondent banks from Lebanon indicates that efficient cross border payments are not hampered by existing technologies alone.

More importantly, (some) cryptos are here to stay because they do not need anyone's permission to exist. Whether legitimised by regulation or not, digital tokens serve practical needs, unacceptable though some of them they may appear or be.

When is blockchain the right solution?

Simplistically speaking, blockchain was 'first' implemented in order to provide a peer-to-peer electronic payment system utilising a decentralised, trustless, append-only technological method. The fervour resulting from this pioneering application – alongside the financial gains accrued by many early crypto adopters – generated well intended interest in the underlying technology.

Evangelical articles and predictions on where blockchain can be applied abound. Over the past few years, several scholarly and practitioner papers have waxed lyrical about the potential of blockchain to disrupt anything from banking to world hunger.

Yet, leaving aside any of the successful or failed implementations discussed above, it remains a fact that blockchain has only achieved real traction for the purpose it was 'originally designed' for: supporting crypto transactions. Any other applications (Non Fungible Tokens included) remain marginal, to say the least. Therefore, before embarking on more experiments, it is important to understand what type of problems blockchain is well suited to support. In other words, we should first define the business requirements and subsequently select the appropriate technology to address them; otherwise, we will keep hitting the wrong nails with the wrong hammer.

The scathing Accenture review of the ASX blockchain project highlights exactly this problem: "there is little value to processing all the business logic on-ledger as ASX maintain data integrity as the market operator and participants receive a point-in-time view via API contracts. [...] ASX is the central source of truth and final arbiter of outcomes, minimising many of the benefits of a DLT architecture". More succinctly, the chosen decentralised architecture offered benefits (trustless verification) that were not important to the problem intended to be solved (settlement processing efficiency).

To evaluate whether blockchain is a candidate technology, one should consider the following non exhaustive checklist of conditions:

- **Data is distributed amongst parties**

  This is the simplest condition to satisfy and a common reason as to why distributed ledger solutions are pursued even though they may not be the most optimal approach. Clearly, several business challenges can be addressed with distributed data, yet data distribution alone is not an adequate reason to opt for blockchain solutions without simultaneously considering other technological options.

- **The transacting parties do not trust each other**

  A genuinely revolutionary contribution of blockchain-like approaches is the achievement of trustless verification. Where transacting parties do not trust each other, proof of work or related approaches can have a great role to play. However, most business problems entail at least some sort of trust between counterparties, regardless of whether such trust is justified or not. After a while, the cost of

trustless verification may outweigh the risks of trusting a potentially untrustworthy central node or authority. Openly verifiable yet centrally managed databases may solve the same problem, without the redundancy and computational intensity embedded in blockchain based distributed ledgers.

- **The data inputs are trusted**

  This is where things start getting more complicated. Even if trustless verification is a desirable attribute, can we trust the veracity of the data inputs? Theoretically speaking, blockchain ledgers are 'immutable' which means that – if fraudulent data enters the chain – fraud cannot be reversed. Do we trust the information provided by the suppliers? Can we validate that the digital signature of a quantitative surveyor has not been compromised by bribing or, simply, incompetence? One needs to evaluate how many business problems can be addressed by (theoretically) preventing the correction of inaccurate inputs.

- **The solution programmers and administrators are trusted**

  More importantly, even where trustless verification is desired, we still need to trust the business analysts, the developers and the administrators of the verification ecosystem. The use of permissioned or private ledgers seems to 'solve' a strangely stated problem: we apply computationally costly verification protocols between a closed group of counterparties that, to some extent, trust each other. Once again, it appears that we strive to tweak the blockchain technology just to apply it on a problem that can be solved otherwise.

- **The data is structured in a time chain (append only)**

  Generally speaking, blockchain-like infrastructures support append only functionality to the ledger chain. In other words, the problem we try to solve should require that the data is primarily structured in a time chain. It becomes obvious that time sequencing may come at the expense of other equally important objectives such as, for example, client centricity. It is also worth noting that the sequencing of data is different from the timing of data. If all you need is a time stamp, a simple SQL-like database with a 'Date' field may be a better, simpler and definitely cheaper solution.

- **Data verification is more important than the data itself (i.e. not a database)**

  Last but definitely not least, blockchain ledgers are best not understood as databases. Holding the same data across all nodes is highly inefficient and therefore costly. Blockchain-like solutions are beneficial when the verification of data is the problem we try to solve, not the storage of the data itself.

Let's accept blockchain for what it is: an excellent niche tool

As mentioned above, system implementation failures cannot be attributed to the choice of technology alone. However, we should always first evaluate the applicability of the technology to a specific business problem in order to reduce the inherent riskiness of any system implementation.

Of course, we may simply be at the very beginning of the diffusion curve and the potential of blockchain remains untapped. We should undoubtedly stand behind innovations that improve people's lives, and be willing to experiment and fail. However, a factual analysis of the conditions outlined above indicates that blockchain will likely remain a niche technology which only addresses a rather narrow set of problems. In other words:

- Blockchain cannot make processes more efficient, even though it has been a useful trigger for rethinking how processes should be redesigned and supported by technology (even if that technology is not DLT based)

- Existing technologies may address our objectives equally well and should be considered as alternatives before we settle on the final approach.

A public letter undersigned by 1500 computer engineers summarises the above in one paragraph.

> "By its very design, blockchain technology is poorly suited for just about every purpose currently touted as a present or potential source of public benefit. From its inception, this technology has been a solution in search of a problem and has now latched onto concepts such as financial inclusion and data transparency to justify its existence, despite far better solutions to these issues already in use. Despite more than thirteen years of development, it has severe limitations and design flaws that preclude almost all applications that deal with public customer data and regulated financial transactions and are not an improvement on existing non-blockchain solutions."

There is nothing wrong with a brilliant technology solving, really well, only a handful of issues. And, we have to continue experimenting in order to learn; failures are welcome, at least for non-financially involved observers! However, we have to base our learning process on the right foundations, rather than hype or media buzz.

Dr Periklis Thivaios CFA, FRM, BTRM is a founding partner of True North Partners LLP, a member of Faculty BTRM®, a founding member of the Hellenic Blockchain Association and (despite appearances to the contrary) a committed technology enthusiast.