Blockchain and Its Role In Your Fund

By Alexandre Miranda

Senior Consultant

MAINSPRING
FUND SERVICES

1. Introductory Remarks

Blockchain has the potential to disrupt countless sectors and its latent impact likened to the introduction of the Internet. This paper is a thought piece on the impact that blockchain can have on the fund management and administration sectors, and whether it should be accepted in the place of currently existing legacy systems or market alternatives. The conclusion of this paper was reached through the amalgamation of outside research sources and the results of a three-month proof of concept, (POC), project conducted by Mainspring Fund Services in 2018 to determine the sustainability of blockchain as a replacement for traditional SQL based systems.

The conclusion of this paper is that although there are some major benefits to the implementation of blockchain, uncertainty and cost considerations rule out firms where blockchain is not determined business critical. The burden for pushing forward lies with: start-ups where the appetite for risk exists, large firms who are willing to assume full risk, or conglomerates of smaller firms where the combination of resources to necessitate the full scope of experimentation are available. However, irrespective of who develops a blockchain solution such an offering must stress utilisation by corporations throughout the supply chain to ensure a lasting, pervasive impact.

2. The Defining Features of the Chain

To understand the information presented; what blockchain is, and some of its core features must be discussed. Blockchain for the function of this paper is defined as a ledger documenting a chronological series of immutable records that has been distributed to all parties within the defined network. Breaking this further apart this paper defines distributed as a source not determined by one, centralised system, but instead by multiple corroborating sources. Records are simply any transaction or other data point stored within the blockchain. This paper discusses a defined network with regards to three potentialities: private, permissioned, and public. A private network is where no system sits above any other, but all parties who participate in the chain exist within a closed system. A permissioned or federated network extends a private network where entry can be granted by a governing or administrative body or rules, who serve an analogous function to a gatekeeper. Finally, a public network is what is commonly imagined with blockchain implementations such as Bitcoin, where any party can gain access and participate in the chain. With these parameters defined attention can turn to the discussion of this paper.

3. Blockchain Potential to Drive Value Added

Mass adoption of blockchain and its replacement of legacy systems has the potential to vastly improve data transparency, auditability, and process efficiency. Santander led a FinTech

analysis of the effect, hypothesizing that distributed ledger technology could quantifiably add between $15 to 20 billion per annum to the banking sector by the year 2022 (Belinky, Rennick, & Veitch, 2015).

3.1 Transparency

One of the major driving forces behind the propulsion of blockchain into the mainstream is trust. With blockchain all parties have access to the same data and as a blockchain is immutable, doubt that one valid party's data somehow differs to another's is removed. Furthermore, all nodes within the blockchain are updated as a transaction is added, allowing connected parties to see the transactions immediately. This structure allows any valid user to employ this immediate transparency in addressing errors that does not match an agreed governance structure.

Increased transparency may also dull some of the need for fund "shadow bookkeeping". Shadow bookkeeping is the practice of maintaining a parallel set of books and records to ensure confidence in reported performance. Immutability means that no user can go back in time and amend transactional workings for a nefarious purpose. As such, having a second set of books to check mistakes due to malicious intent becomes less vital. Blockchain, however cannot guarantee correct initial transactions, so a strong governance system is still necessary, but using blockchain will give valid parties a greater level of transactional transparency.

3.2 Auditability

Working in fund management and administration, blockchain offers a solution to help streamline audit processes and remain compliant, especially concerning a controls audit.

ISAE 3402, like SSAE-16 superseded by SSAE-18 in May 2017, is purposed to assure a client that adequate internal controls are in place at a service organisation. Blockchain can help an organisation meet these criteria in a more effective way compared to reliance on a system of human governance alone. With a structure inherently including controls such: impossibility of block augmentation and multiple records of a sole truth, firms can demonstrate that such a blockchain system includes governance over human malfeasances and accurate transactional documentation. There is nowhere to hide from an audit standpoint. All blockchain transactions employ hashes, which are unique transactional finger prints. By accessing the blockchain directly auditors could use hashes to match transactions and confidently corroborate that appropriate controls have been considered. Furthermore, part of SOC-3 reporting as included in SSAE-18 is documentation of the potential security risk of unauthorized access both physical and logical. Blockchains are immutable meaning that past transactions are tamper proof, but security surrounding any future transactions will

depend on how the blockchain is structured and the network security of access and permissions for inputting updates.

3.3 Efficiency

Blockchain's potential to improve efficiency is immense. For example, consider the adoption of smart contracts, which are automated scripts coded in the blockchain to represent a contractual obligation executed when certain triggers are met. Smart contract automation will increase the speed of transactional action, and assuming valid and appropriate code the frictional costs associated with additional human involvement is minimized. For firms operating in the fund management and administration sectors, the increased level of automation associated with adopting such a technology would allow it to potentially limit the risk for both human input error and issues surrounded with lack of execution. Moreover, human capital freed could be directed towards other value-added tasks. It should be noted that smart contracts would add the greatest value in trading houses or hedge funds with an extremely active trading strategy or where execution time is vital versus a private equity fund, where there are fewer transactions and immediate knowledge of statistical data associated with the transaction is not as imperative.

Having access directly to the blockchain can improve report automation and data entry. As a complete source of all transactional records automated scripts could be built to run using the data stored in the blockchain. As all nodes of the blockchain will synchronise to the new truth as soon as a transaction is added, scripts will run off the most up to date data. There is however a risk with such direct access to data. If a client is granted access to the blockchain any errors that occur, which would have been amended through a review process in a current system become a permanent scar on the chain. Anytime human involvement is required there is a risk for error and this should be taken into consideration when deciding who to allow access to the blockchain.

Blockchain can also offer overall firm efficiency benefits, providing an infrastructure able to be leveraged in filling administrative and communicatory functions. Utilising the blockchain in this way will allow fund managers to divert resources to focus on specialisations and not waste valuable resources completing mundane tasks. With time liberated from such endeavours, parties can allocate a greater focus to the value add of their firm. This benefit will be enhanced the greater the participation along the supply chain from lawyers, auditors, regulators, and fund managers is.

4. Limitations of a Golden Goose

Blockchain is not without its weaknesses. The idea that blockchain is the "be all end all" seems at minimum premature.

4.1 Regulation

One of blockchain's greatest advertised value adds is associated with its inherent principle of immutability, in other words it cannot be edited. The characteristic of immutability in applied cases, such as a transactional accounting ledger, is extremely beneficial, but in other cases can be totally detrimental to the deployment of the blockchain. For example, consider the fund management and administration world where personal information of investors is held by parties. This is done for a whole host of reasons, including know your customer (KYC), anti-money laundering (AML) checks, investor reporting, etc… However, these same investors according to European legislation have an inherent "right to be forgotten":

"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" (The European Parliment And The Council Of The European Union, 2016)

If their personal information is stored within an immutable blockchain, then how can they truly have their data purged from the fund manager's records? This regulatory stumbling block presents a major issue to the adoption of blockchain within an investor focused industry.

4.2 Cost

Another major issue associated with blockchain use is cost. The algorithms necessary to run blockchain have the potential to consume a massive quantity of energy. In his study Alex de Vries stated:

"The Bitcoin network can be estimated to consume at least 2.55 gigawatts of electricity currently, and potentially 7.67 gigawatts in the future, making it comparable with countries such as Ireland (3.1 gigawatts) and Austria (8.2 gigawatts)" (de Vries, 2018).

Although an extreme example of a public blockchain, this example highlights that the energy consumption of blockchain can be sizable. Acknowledging this, it is also important to consider that the energy use could potentially differ depending on the purpose and type of the blockchain. For example, a federated or private blockchain may save on energy costs as the quantity of nodes needed to be updated following an addition is considerably smaller relative to the public Bitcoin blockchain.

In the POC conducted by Mainspring, where a relatively small number of records with less than ten pieces of information per application was stored, energy cost was flagged as a potential

issue. The marginal energy cost may well have shrunk to an acceptable level when a certain threshold of set-ups was passed. Although not definitive the results seem to suggest if many records are not constantly being actioned, such as in the private equity sector where transactions like drawdowns or distributions are done infrequently, the use of a blockchain could be analogues to using a supercar to drive around the corner, unnecessary and costly.

Early stage adopters of technology face the biggest learning curve. In the blockchain environment although multiple sources of the truth offers an improvement on a single source of the truth with regards to perceived security, having so many access points to the data may entice those with nefarious intentions to target this budding technology. Unlike its mature competitor, blockchain is relatively new and thus the security around such a system is relatively untested. Major blockchain based systems have in the past been compromised, such as the approximately $64 million stolen from Slovenian bitcoin platform NiceHash in 2014 (Gibbs, 2017). Beyond this obvious financial cost, such a breach signals a lack of perceived security causing irreputable reputational damage. As the blockchain technology matures such hacks will be better dealt with and prevented, but as a relatively immature technology with multiple access points it currently offers an enticing opportunity for hackers to target.

4.3 Troublemakers

Parallel to the reputational cost of a hack another potential reputational issue with blockchain is concerned with mischief. This is more applicable in public blockchains where accountability is lessened due to its pseudonymous nature. As any person can access and interact with a public blockchain, people can store information that is not only inapplicable, but in extreme cases vulgar and dangerous. The exemplification of such actions can be found throughout the public Bitcoin blockchain as highlighted in analysis conducted by German researchers from RWTH Aachen University and Goethe University:

"Although most data originates from benign extensions to Bitcoin's protocol, our analysis reveals more than 1600 files on the blockchain, over 99 % of which are texts or images. Among these files there is clearly objectionable content such as links to child pornography, which is distributed to all Bitcoin participants" (Matzutt, et al., 2018).

As this chain is immutable these egregious transgressions will remain within the chain in-perpetuity. For an investor facing platform where transparency is deemed a driving force behind adoption, such breaches could have serious and lasting reputational consequences.

5. Blockchain Into the Future

Blockchain is a constantly evolving product and its current rate of growth could be very well expected to accelerate in the future as more research is conducted. In 2016, Accenture argued if a permissioned, editable blockchain made the jump from a theoretical experiment to a real-world application that the fundamental principle of absolute immutability could be reconsidered. (Lumb, Treat, & Jelf, 2016). Parallel to this belief, Accenture applied for a patent for an editable blockchain in 2016 where a central administrator shackled by pre-agreed rules could edit or delete information stored within a permissioned blockchain. An editable, permissioned blockchain in theory helps address the regulatory issues associated with holding personal data within an immutable chain, but the nature of an editable blockchain seems to directly contradict the essence of what blockchain is. If data held must meet stringent regulatory requirements other options should be considered.

5.1 Zero-Knowledge Proofs (ZKP)

The necessity to enhance security of the blockchain following breaches and the occurrence of other nefarious acts has led to a greater focus on cryptographical methodology. One of the methodologies that has garnered a great deal of attention is based on the theory of zero-knowledge proofs (ZKP). Described in the 1989,

"Zero-knowledge proofs are defined as those proofs that convey no additional knowledge other than the correctness of the proposition in question" (Goldwasser, Micali, & Rackoff, 1989)

Applied to an action means one can verify their unique, valid identity without exposing any information besides their statement's validity. Meeting the following criteria the proof can be considered zero-knowledge:

1. *Completeness. If the statement is true, an honest verifier will be convinced by an honest prover.*
2. *Soundness. If the statement is false, no dishonest prover can convince an honest verifier.*
3. *Zero-knowledge. If the statement is true, no dishonest verifier learns anything other than the fact that the statement is true*

   (Koens, Ramaekers, & van Wijk, 2017)

A common example used to explain how a ZKP works is the "colour blind friend". Imagine you have a friend who is unable to tell between a red and a green ball. The friend believes the balls are the same and refutes your statement that they are in fact different. To test you, your friend shows you which ball is in each hand. Next, the balls are put behind their back and interchanged many times. Showing you one ball they ask, which hand that ball originated in. You will get this right

being able to tell the difference with the colours. After a certain threshold of interactions your friend will eventually believe you that there is indeed a difference and you are correct.

ZKP is particularly applicable in transactional documentation. With ZKP valid parties can action transactions without relinquishing sensitive, confidential information. Furthermore, parties within the blockchain environment not deemed valid through the embedded zero-knowledge protocol will see only that a valid transaction has occurred, but not be privy to the information surrounding the transaction. The issue with ZKP was the lack efficiency. To establish validity, large proofs or large numbers of interactions between the parties was required. A further application of ZKP known as zk-SNARKS (zero-knowledge succinct non-interactive arguments of knowledge) was used to address the efficiency limitations that mitigated its practical applicability. zk-SNARKS were created to enhance the efficiency of ZKP by minimising the interaction between the parties. An example called Zcash utilises zk-Snarks to enable users to complete transactions revealing only that transaction has occurred but not the sender, receiver, or amount. However, implementing a ZKP means accepting a trade-off associated with such privacy and cryptographical gains:

"Improved confidentiality and privacy comes at a cost, in the form of a larger transaction size (required to contain the cryptographic proofs required for the various techniques) or, in the case of zk-SNARKs, greater computational cost" (Yang, Gavigan, & Wilcox-O'Hearn, 2016)

The use of a type of ZKP seems to offer a potential for transactional documentation on the blockchain, but for a purpose where client information documentation is the focus, such as investor onboarding as analysed in the Mainspring POC, an alternative solution to ZKP should be considered.

5.2 Off-Chain Storage

Storing an encrypted version of an investor's information off-chain, whilst including a hash reference of any recorded transactions on the blockchain is one potential way of addressing regulatory compliance, especially in relation to GDPR. If an investor exercises their right to erasure, the encrypted data is deleted leaving simply a hash with reference to no personal information stored on the blockchain. This may help address a regulatory concern, but running information on blockchain in parallel to an off-chain system means sacrificing a major benefit of the blockchain, its validity as the sole source of the truth.

Alternatively, storing an encrypted, anonymised version of an individual's person information on a private or federated blockchain with the key to unlocking such information off-chain is a potential solution. Such an approach could allow for the circumvention of the issue discussed in the preceding paragraph. By storing all information in an anonymised form, allows for

the blockchain to still operate as the sole source of the truth, but potentially meet regulatory requirements for personal data storage. The issue here becomes what constitutes true anonymity. GDPR regulation states,

"The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" (The European Parliment And The Council Of The European Union, 2016)

A person has a right to the removal or amendment of their data, but does the simple elimination of their key ensure the anonymity? Simply, no. Using the hashes associated with the public key cryptography that is inherent to blockchain's make up is not sufficient, as this is pseudonymous not anonymous. However, in theory if the cryptographical method used to encrypt the personal information, which was stored on the blockchain is built in such a way that once the decrypting reference key is eliminated no matter the attempt, blunt force or otherwise, the information maintains it's the characteristic that it cannot be linked to any one specific person would seem to meet the criteria of anonymity as defined in legislation by the European Parliament. Using an additional level of cryptography to ensure data anonymity is an interesting potential avenue for future research.

6. Who Needs Blockchain?

Blockchain is in the news constantly and seems very much like the shiny new toy, but there are many other suitable non-blockchain solutions that are more cost effective.

From our analysis of the investor onboarding process where the objectives of transparency and enhanced workplace efficiency were critical it was determined that the desired solution could be achieved leveraging an alternative non-blockchain system. After much research we decided that digital process automation would fill many of those workflow needs. Included in the system was the potential for the process governance we sought with the blockchain, but allowed us the potential to offer a great end user experience. As the technology is relatively new to the business currently, we have focused digital process automation to manage internal process, but have been able to successful POC the ability to allow our clients access to the system providing our clients with operational transparency. Furthermore, instead of hiring an outside blockchain developer with a unique and expensive set of skills the building and administration of the platform could be handled with in house resources and conventional development expertise. The choice of a workflow automation system allowed Mainspring Fund Services to save cost without sacrificing an elevated

level of service offering. Additionally, there are ways to ensure secure and compliant information transfer such as a customisable SFTP site, which is a less costly alternative. By employing these product offerings amongst others in conjunction, we feel that we cannot only meet all our client needs, but match all those efficiency, transparency, and auditability benefits that have been attributed to blockchain.

7. Concluding Discussion

Building a suitable, customised blockchain infrastructure to replace currently implemented systems requires a vast amount of devoted capital. Unless a supply chain including regulators, auditors, lawyers, and fund administrators is created such an undertaking would be limited in potential value addition. Furthermore, the associated risk with such an initial outlay of capital necessary to such an endeavour seems to rule out firms where a blockchain is not deemed critical for continued business functionality. Instead, if a smaller firm wished to build a blockchain it seems more suitable to form partnerships and combine talent, resource, and knowledge wealth in the pursuit of a common goal. Alternatively, this developmental opportunity can be seized upon by large firms with the necessary capital to fully assume the risk or start-ups where risk appetite is far larger.

Future research is necessary for the widespread adoption of blockchain, but in this sector where both transactional and sensitive client information is held, a blockchain leveraging the transactional anonymity of a methodology such as ZKP with a new cryptographical method ensuring that legislative directives are met, would streamline the business and enhance profit margins. If such a solution could sufficiently address these regulatory and practical issues the corresponding firm would be able to seize upon an extremely large opportunity both by furthering the evolution of the financial fund management and administration industries and establishing an early market presence within an emerging, growth sector. However, until such a solution exists, and a business can be confident that it offers a level of service to such a standard that exceeds current alternative legacy systems, firms will be hesitant to adopt blockchain technology. It is possible such a suitable technology offering may exist in the near to medium term as an endeavour by a Northern Trust fronted partnership with IBM used a blockchain based system for a live capital call at the end of 2018, which represents a preliminary step towards greater adoption (Ledger Insights, 2018). However, irrespective of when the technology become widely available the key for lasting success is the collaborative adoption by corporations throughout the supply chain.

Works Cited

Belinky, M., Rennick, E., & Veitch, A. (2015, June 15). *The Fintech 2.0 Paper.* Retrieved from http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. (2015, May 19). *Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture*. Retrieved from https://eprint.iacr.org/2013/879.pdf

Christidis, K., & Devetsikiotis, M. (2016, May 10). *Blockchains and Smart Contracts for the Internet of Things.* Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408

de Vries, A. (2018, May 16). Bitcoin's Growing Energy Problem. *Joule, 2*(5), 801-805. Retrieved from https://www.cell.com/action/showPdf?pii=S2542-4351%2818%2930177-6

Di Gregorio, M. (2017, February). *Blockchain: A New Tool to Cut Costs*. Retrieved from https://www.pwc.com/m1/en/media-centre/2017/articles/max-di-gregorio-me-insurance-review-feb2017.pdf

Ernst & Young Accountants LLP. (2013). *Implementing and Maintaining ISAE 3402*. Retrieved from https://www.ey.com/Publication/vwLUAssets/Broszura_EY_ISAE_3402/%24FILE/ISAE_3402.pdf

Fauvel, W. (2017, August 11). *Blockchain Advantage and Disadvantages*. Retrieved from https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0

Gibbs, S. (2017, December 07). *Bitcoin: $64m in cryptocurrency stolen in 'sophisticated' hack, exchange says*. Retrieved from The Guardian: https://www.theguardian.com/technology/2017/dec/07/bitcoin-64m-cryptocurrency-stolen-hack-attack-marketplace-nicehash-passwords

Goldwasser, S., Micali, S., & Rackoff, C. (1989, February). The Knowledge Complexity of Interactive Proof-Systems. *SIAM Journal on Computing, 18*(1), 186-208. Retrieved from http://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf

Hearn, M. (2016, November 2016). *Corda: A Distributed Ledger*. Retrieved from https://www.corda.net/content/corda-technical-whitepaper.pdf

Ibanez, L.-D., O'Hara, K., & Simperl, E. (2018). *On Blockchains and the General Data Protection Regulation.* Retrieved from https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf

Koens, T., Ramaekers, C., & van Wijk, C. (2017, November 16). *Efficient Zero-Knowledge Range Proofs in Ethereum*. Retrieved from https://www.ingwb.com/media/2122048/zero-knowledge-range-proof-whitepaper.pdf

Ledger Insights. (2018, November). *Northern Trust expands private equity blockchain*. Retrieved from Ledger Insights: https://www.ledgerinsights.com/northern-trust-private-equity-blockchain/

Lumb, R., Treat, D., & Jelf, O. (2016, September 26). *Editing The Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt To An Imperfect World*. Retrieved from

https://www.accenture.com/t20160927T033514Z__w__/us-en/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf#zoom=50

Matzutt, R., Hiller, J., Henze, M., Ziegeldorf, J. H., Mullmann, D., Hohlfeld, O., & Wehrle, K. (2018). *A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin.* Retrieved from https://fc18.ifca.ai/preproceedings/6.pdf

Maxwell, Winston; Salmon, John; Hogan Lovells. (2017, September). *A Guide to Blockchain and Data Protection.* Retrieved from https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf

Mercieca, J. (2018, April 19). *Blockchain UX: Challenges, Principles and Heuristics*. Retrieved from https://medium.com/@jmer.ux/blockchain-ux-design-challenges-principles-and-heuristics-903f8e0aa370

Moser, J. (2017, February 2017). *The Application and Impact of the European General Data Protection Regulation on Blockchains*. Retrieved from https://www.r3.com/wp-content/uploads/2018/04/GDPR_Blockchains_R3.pdf

The European Parliment And The Council Of The European Union. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliment and of the council.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Yang, D., Gavigan, J., & Wilcox-O'Hearn, Z. (2016, November 14). *Survey of Confidentiality and Privacy Preserving Technologies for Blockchains*. Retrieved from https://www.r3.com/wp-content/uploads/2017/06/survey_confidentiality_privacy_R3.pdf