

Proceedings

Blockchain Technology: Financial Sector Applications Beyond Cryptocurrencies [†]

Ariana Polyviou ^{1,*}, Pantelis Velanas ² and John Soldatos ²

¹ School of Business, University of Nicosia, 2417, Nicosia, Cyprus

² Innov-Acts Limited, 1101, Nicosia, Cyprus; pvelanas@innov-acts.com (P.V.); jsoldat@innov-acts.com (J.S.)

* Correspondence: polyviou.a@unic.ac.cy

[†] Presented at the 3rd annual Decentralized Conference, Athens, Greece, 30 October–1 November 2019.

Published: 25 October 2019

Abstract: Blockchain technology was initially employed as the public transaction ledger for cryptocurrencies. However, beyond cryptocurrencies, blockchain technology has been recently considered for a plethora of other applications as it encapsulates unique properties including decentralization, security, transparency and anti-tampering. Such properties are particularly advantageous for variety of prominent issues experienced in the financial sector. As a result, blockchain technology holds the potential to revolutionize the financial industry by altering the way in which different services are conducted in the financial industry. In this paper, we outline five different financial industry use cases that are expected to be radically transformed by the use of blockchain technology.

Keywords: blockchain; fintech; customer; decentralization; insurance; security

1. Introduction

Blockchain technology become famous following the introduction of blockbuster cryptocurrencies like BitCoin and Ethereum, which are still the sole applications of blockchains at scale. BitCoin and Ethereum have attracted the interest of the financial services industry, while at the same time giving rise to the introduction of additional cryptocurrencies (AltCoins) such as LightCoin, PrimeCoin, NameCoin and Zcash [1]. Moreover, they have driven the emergence of an entirely new concept for funding innovative ideas and products, namely the Initial Coin Offering (ICO) mechanism. During the last couple of years, there has been a surge of interest in other applications of blockchains beyond cryptocurrencies, notably applications that attempt to exploit the decentralized nature of distributed ledger technologies (DLT), as well as their security, transparency and anti-tampering properties. In many cases applications take advantage of these properties in the scope of permissioned blockchain infrastructures, which offer fine grained authentication and authorization, while at the same time obviating the need for complex and time-consuming Proof-of-Work (PoW) processes. The latter is a key to supporting applications that need to support faster transaction completion than what is supported by conventional public blockchains such as BitCoin and Ethereum. This has given rise to the emergence of platforms destined to support permissioned blockchains such as R3/Corda and Hyperledger Fabric, both of which support hundreds of transactions per second (TPS). Non-cryptocurrencies applications based on permissioned blockchains are currently being explored in many different sectors, such as energy, industry, supply chain management and healthcare. A plethora of such applications are also considered by financial organizations, as part of the wave of FinTech innovations.

The use of blockchain technologies enables financial organizations to dismiss several long-lasting prominent issues. One of the most notable problems associated to bank credit, is lack of information on credit scoring, causing individuals and SMEs to have difficulties in obtaining loans

by financial institutions [2]. Due to lack of sufficient and accurate information, financial institutions are also struggling to conduct accurate customer profiling such that they can efficiently conduct product differentiation and personalization [3]. Along the same lines, insurance products offered by financial institutions encapsulate a complex insurance claims process, requiring the involvement of numerous stakeholders before the finalization and payment of a claim. Finally, existing critical infrastructures that facilitate the majority of the transactions of financial organizations are primary targets for cyber-attacks.

Reflecting in the above-mentioned issues, in this paper, we exhibit five different use cases in which blockchain technology are likely to gain considerable momentum in the years of come, reshaping the financial sector.

2. Five Blockchain Use Cases in the Financial Sector

2.1. Know Your Customer (KYC) and Know Your Business (KYB)

All financial organizations initiate KYC and KYB processes whenever they on-board a customer. As part of these process, the customer is identified and verified against applicable laws and rules set by regulators at national and international level (e.g., Central Banks, Banking Associations, Securities and Futures Commissions). Moreover, an initial profile for the retail or corporate customer is offered, as means of personalizing service offerings. The KYC/KYB process is dynamic, as both customer information and applicable regulations evolve over time, which makes the process of updating profiles and relevant documentation quite challenging. Furthermore, customers are typically required to provide a batch of documents each time they are on-boarded by a financial institution. To alleviate this need, customer documentation can be maintained centrally by an authority (e.g., a regulator or state organization). This is however a solution vulnerable to cyber-attacks and data breaches.

Blockchain solutions can alleviate the above listed challenges, through decentralizing and securing the KYC process. In particular, by keeping customer data in a distributed ledger, blockchain participants will be able to update customer information as needed, while being able to access an up-to-date picture of the customer's profile at all times. In this context, blockchain solutions offer some significant advantages, such as:

- **Decentralization:** Customer records are stored in a decentralized fashion, which reduces the data protection and cyber-crime risks of centralized storage. Apart for increased security, decentralization boosts consistency in the recorded KYC/KYB information.
- **Improved Privacy Control:** Customer information is no longer handled by a single trusted third party. Rather it is processed by decentralized applications such as smart contracts. The latter contracts handle customers' data on behalf of the entire financial ecosystem. Furthermore, access to customer information for KYC (or other) purposes can occur only following the customer's consent, which provides a sound basis for fine-grained privacy control.
- **Immutability:** Once recorded in the blockchain customer information stays forever and cannot be changed. This enables accurate tracking of customer information at all times and based on information available to all financial institutions that participate in the blockchain. However, there may be a needed for erasing customer information following a customer's account closure, in which case customers are entitled to enjoy the "right to be forgotten" one of the core principles of the GDPR (General Data Protection Regulation). Despite an on-going debate about how this principle could be supported on blockchain data, stakeholders seem to be converging on a solution. We will be analyzing ways for ensuring GDPR compliance in a blockchain in future posts.

2.2. Credit Risk Scoring for SMEs

Nowadays, most banks consider Small Medium Enterprises (SMEs) as high-risk customers. This holds not only for very small enterprises (e.g., micro SMEs and startups), but for bigger and wealthier

SMEs as well. It is largely a consequence of stricter regulations (e.g., liquidity rules) that have been introduced following the financial crisis of 2008 (e.g., Basel III), but also a matter of shrinking returns on equity that have made SME lending even more challenging. In this context, banks require novel approaches to credit scoring of SMEs, beyond the use of their conventional finance and accounting data (e.g., P&L balance sheets). Such approaches could leverage the ability to share data across banks, but also the possibility of taking advantage of vast amounts of alternative data (e.g., data from social media, news and other internet sources).

Blockchain technologies enable the secure sharing of credit scoring information from multiple parties (e.g., banks and credit risk assessment organizations). Each participating organization contribute information that can be used for assessing the reliability of SMEs, as a means of facilitating lending decisions. The approach is decentralized, which reduces the information of credit risk scoring information being compromised. Moreover, credit risk scoring is performed without exposing sensitive data. Note that the value of such a blockchain increases with the number of participants to it, but also based on the volume and the value of the information that they contribute. The more banks that collaborate as part of such a blockchain, the more accurate the credit risk assessments.

There are already startups that provide blockchain-based solutions for credit scoring. One example is Bloom, which provide decentralized credit scoring based on Ethereum and the IPFS (InterPlanetary File System), which provides the means for storing hypermedia in a distributed file system. Likewise, PayPie provides a credit risk assessment service based on blockchain accounting, which enables trust and transparency on the basis of a unique Credit Risk Assessment Score.

2.3. Customer Profile Management and Product Personalization

Similar to KYC and credit risk scoring use cases, blockchain technologies can enable much more accurate, secure and privacy friendly profiling of both consumers (i.e., retail customers) and businesses. In most cases customers maintain accounts and other banking products in several banks and financial institutions. Each of these institutions profiles customers based on its own (partial) view of their profile. Data may be held across multiple financial institutions and multiple platforms beyond financial institutions such as social media. Much better profiling is possible by combining profiling data, including data from different account types, relationship data between customers (e.g., family, business), structured and unstructured data (e.g., pictures).

A blockchain infrastructure could enable the secure sharing of such data across institutions, while lowering the trust barriers for them to share their customer data. Moreover, a blockchain infrastructure could facilitate the management of the customers' consent to share this data. Based on a more accurate customer profile, financial institutions will be able to perform customer centric analytics and to tailored products and services to the customers' needs. Some prominent examples include the development of personalized asset management recommendations and the construction of personalized investment portfolios, the individualization of retail banking products and more.

Customer profiling is certainly relevant to the KYC/KYB processes outlined above, as KYC provide the means for bootstrapping the construction of customers' profiles. Nevertheless, it goes beyond KYC, as it can benefit from the provision of more customer data, that the customer opts to provide in order to enjoy more personalized products. In this direction, blockchain infrastructures can serve as a basis for establishing personal data markets, where customers provide access to their data in exchange of proper incentives provided by the financial institutions.

2.4. Insurance Claims Management

The insurance sector is very closely affiliated to the finance sector, as many financial institutions offer insurance services as well. Blockchains provide some compelling value propositions for insurance as use cases. As a prominent example, they are an excellent vehicle for expediting the tedious process of insurance claims management. Indeed, claims processing is nowadays a very lengthy and complicated process, which requires the participation of several stakeholders and intermediaries prior to considering a claim request final and proceeding with its payment. Blockchains can ease this process based on the integration of all stakeholders around a distributed

ledger infrastructure and the implementation of smart contracts for realizing all checks and verifications. Specifically, a smart contract can automatically and securely perform all the steps needed in the claims processing process, including calculation and validation of the amount to be paid. Furthermore, by sharing customer information on the blockchain (e.g., as part of the KYC process) it is also possible to implement smart contracts that perform checks for fraudulent transactions and claims. There are many ways for enriching this process and making it more robust and reliable, such as the inclusion of multimedia information (e.g., photos, videos) taken at the point of an accident, in the case of vehicle insurance. The process might also be enriched by classifying the driver before the insurance contract is released. This might incorporate the communication of driver's performance assessment score that can be achieved through the use of a wide variety of vehicle data including acceleration, steering drive, speed and brake patterns.

2.5. Collaborative Security in the Financial Services Chain

Financial services organizations engage in several collaborative processes across the financial services value chain. For instance, SWIFT transactions involve two or more institutions in their processing and completion. The critical infrastructures that underpin these transactions are primary attack targets for cyber-criminals. Despite the increased investments of financial institutions in security, the critical infrastructures of financial organizations, remain vulnerable. Recent security attacks against financial services critical infrastructures provide a tangible evidence of this. For example, in February 2016, a fraudulent SWIFT transactions cyber-attack resulted in \$81 million being stolen from the Bangladesh Central Bank [4]. Likewise, the famous "Wannacry" ransomware attacked financial institutions and reaffirmed that the financial services industry is a primary target for cyber criminals [5]. To alleviate such attacks financial institutions had better collaborate and share information about the security of their infrastructures that support the collaborative processes of the financial services supply chain. The exchange of security information across collaborating stakeholders of the financial services value chain can be a foundation for security collaboration in the relevant supply chain.

Blockchain technologies facilitates financial organizations in sharing such information, including cyber-security and physical security information [6]. The use of a distributed ledger enables the trustful sharing of data, as means of facilitating security experts' collaboration. In a blockchain all different parties that engage in a supply chain process can participate, which enhances the accuracy and richness of the information, along with the overall credibility of the process. Thus, information about various physical and cyber security systems of financial organizations can be centrally acquired, processed and shared with other financial services parties included in the value chain. Such information is not limited to attacks and threats, but in might encapsulate other relevant forms of security information for the financial sector including assets and services. As a result, beyond facilitating the exchange of information between financial organizations, blockchain technology will also contribute to the implementation of a collaborative risk assessment mechanism across institutions.

3. Conclusions

Blockchain enthusiasts believe that these use cases are likely to become mainstream in the financial sector within the next decade. They also present other use cases in the areas of investment banking and securities, which are already very well served by the Corda/R3 platform. On the other hand, there are also conservative voices that remind us of overhyped technologies and of the fact that cryptocurrencies (such as BitCoin) are up-to-date the only large scale applications of blockchains. What will happen in the medium and long term remains to be seen. For the time being, the listed blockchain use cases provide fertile ground for innovators in the financial sector, including FinTech and InsurTech enterprises.

Acknowledgments: Part of this work has been carried out in the scope of the INFINITECH project (contract number 856632), which is co-funded by the European Commission in the scope of its H2020 program. The authors acknowledge valuable help and contributions from all partners of the project. Moreover, the use case

for exchange of security information is currently under development in the scope of the FINSEC project (contract number 786727), which is co-funded by the European Commission in the scope of its H2020 program.

References

1. Kapoor, S. AltCoins: Cryptocurrencies beyond BitCoin. Available online: <https://www.itexchangeweb.com/blog/altcoins-cryptocurrencies-beyond-bitcoin/> (accessed on 30 July 2019).
2. Guo, Y.; Liang, C. Blockchain application and outlook in the banking industry. *Financ. Innovat.* **2016**, *2*, 24.
3. Rosati, P.; Cuk, T. Blockchain Beyond Cryptocurrencies: FinTech and Strategy in the 21st Century. In *Disrupting Finance*; Lynn, T., Mooney, J.G., Rosati, P., Cummins, M., Eds.; Springer Nature Switzerland AG: Cham, Switzerland, 2016; pp. 149–170.
4. Maurer, T.; Levite, A.; Perkovich, G. Toward a global norm against manipulating the integrity of financial data. *Economics Discussion Papers*, 38, Kiel Institute for the World Economy, Kiel, Germany, 2017. Available online: <https://www.econstor.eu/bitstream/10419/162579/1/890955921.pdf> (accessed on 23 June 2017).
5. Wikipedia. Available online: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (accessed on 30 July 2019).
6. Bosco, F.; Croce, V.; Raveduto, G. Blockchain Technology for Financial Services Facilitation in RES Investments. In Proceedings of the 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), Palermo, Italy, 10–13 September 2018; pp. 1–5.



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).