

A Decentralized Loyalty Program

John Alora, Justin Koh, Hayden Poe

Abstract

Merchants spanning across industries implement loyalty programs to incentivize brand faithfulness among consumers. However, current stand-alone loyalty programs have a flailing success rate retaining customers and fail to take full advantage of network effects that can be gained through cooperative alliances. Though current coalition loyalty programs attempt to solve this issue, they typically conglomerate among large entities in similar industries, alienating smaller businesses that provide complimentary services. These traditional loyalty programs are costly to maintain and the lack of customer participation makes one question if they are even worth while. Koalition addresses the problems found in traditional loyalty programs by leveraging blockchain technology to create an ecosystem that promotes free flow of points for consumers, offer marketing opportunities for merchants, and provide comprehensive data analytics for its users to make better informed decisions. As a stable coin, Koalition's native currency (KOA) allows for convenient accounting and promotes higher transaction rates. Koalition introduces consumers to a vast network of merchants under a unified, fungible, and utilitarian rewards currency through an ergonomic user interface. Koalition is the next-generation rewards currency, providing an agile, industry-grade, and decentralized solution and a frictionless experience to all users.

1 Background

1.1 Introduction

Loyalty programs (LPs) have been implemented across the globe to develop brand loyalty by rewarding returning customers. However, current LPs fail to take full advantage of the network effects that can be gained by leveraging blockchain technology. These advantages include increasing customer loyalty, eliminating third party fees through disintermediation, providing data analytics through customer redemption patterns, and leveraging global integration to develop cooperative alliances that span industries and create a more functional LP for both consumers and merchants.

Koalition is the next generation LP, creating a robust rewards network that integrates existing LPs and adds new opportunities for businesses that previously lacked the resources to deploy their own LP. This network of merchants provides more enticing incentives to customers by allowing them to spend their points when, where and how they want to. Koalition enables customers to accumulate enough points to redeem for meaningful rewards without the hassle of managing separate accounts for dozens of LPs. For businesses, Koalition makes each rewards point transaction more secure and transparent, while removing trusted third party (TTP) services.

The next sections will first focus on the limitations and problems associated with current rewards programs. Then the utility of blockchain technology will be touched upon before describing how it can be used to disrupt the current loyalty industry. Furthermore, the unique aspects of Koalition's decentralized attributes, token stability and added benefits will be described in further detail along with a roadmap for future development.

1.2 Types of Loyalty Programs

1.2.1 Stand-Alone Loyalty Programs

Customer loyalty is an asset that can be leveraged by both small businesses and big brands. Customers loyal to a particular brand are more likely to spread positive word of mouth, less likely to be swayed by competitors, and are less price sensitive. To better compete in a competitive industry, companies in industries ranging from airlines to supermarkets to local coffee shops create incentives using LPs. These programs offer consumers rewards points proportional to their purchases and allow consumers to accumulate points to redeem different types of rewards. Many companies use LPs to increase customer retention as the cost of acquiring new customers is much greater [1]. However, with thousands of programs to choose from, consumers oftentimes are circumscribed by making the most economic travel decisions. According to the 2015 Colloquy Loyalty Census, the average household belongs to nearly 29 different loyalty programs [2]. This perpetuates frustration because customers either pay high costs for similar services to remain loyal to one LP or they have points scattered among a myriad of LPs that they are unable to redeem for anything worthwhile. The end result is account inactivity and low redemption rates. In fact, the 2016 Bond Loyalty Report which queried 12,000 Americans and 7,000 Canadians about their 280 loyalty programs across various industries, found that only 50% of them were active members of their respective programs. Of those 50%, a fifth of them had never redeemed their points. Unredeemed rewards points create accounting liabilities for merchants in the form of unrealized revenues that cannot be absorbed until they are redeemed. Furthermore, customer retention rates diminish for LP members who do not redeem their points. These customers are 2.7 times more likely to join a different program altogether [3].

Many customers have familiarized themselves with LPs through the travel industry, however, travel companies continue to lose market share to Online Travel Agencies (OTAs). OTAs like Priceline and Expedia act as a one-stop shop for consumers by consolidating the experience of individually booking a flight, hotel, and rental car into one platform. OTAs have their own LPs which give customers more choices (so customers can select the cheapest flight with minimal opportunity costs) and make it increasingly difficult for traditional stand-alone LPs to compete. Airlines, hotels, and rental car companies share up to 20% of their revenues with OTAs and OTAs are projected to own 41% of travel industry bookings by 2020 [4]. Despite this fact, merchants still use OTAs because exiting this channel would result in a significant loss of marketing opportunities. It is clear that merchants need an alternative loyalty program that provides enough customer flexibility to compete with OTAs, or continue giving up revenue.

1.2.2 Coalition Loyalty Programs

While the number of stand-alone LPs have grown, the challenges of these programs to consumers and businesses alike have caused many businesses to search for different LP schemes. Businesses have begun to participate in coalition LPs in an effort to provide customers rewards that can be earned and redeemed faster with greater flexibility across businesses. Most coalition LPs are formed through the agglomeration of existing stand-alone LPs and consist of either pairwise partnerships such as Amex-Uber or centralized partnerships like Starwood Hotels and Resorts (U.S.) and SkyTeam (international alliance). These coalitions help split liability among the participating merchants and partially solve some of the customer frustrations while still attempting to increase customer retention and engagement rates. Furthermore, coalition LPs promote the acquisition of new customers more easily than stand-alone LPs due to inter-company cooperation which favors cross-selling. It costs less to join a coalition LP than to establish a stand-alone program, and empirical evidence shows that businesses in coalition LPs achieve higher marketing performance [1].

However, coalitions are often times limited in scope. Coalitions typically form among large entities in similar industries (*i.e.* the many large hotel, airline, and rental car brands within the travel industry). These coalitions alienate small to medium cap businesses providing complimentary services, and hence fail to leverage the additional network benefits provided by adding these businesses. Furthermore, complex exchange rates and liability transfers between various LPs in a coalition require negotiations that consume unnecessary time and resources. While coalition LPs mark a step forward to fixing the problems that plague stand-alone LPs, these programs have a long way to go to improve customer loyalty and enhance the customer experience.

1.3 Centralized Databases

Databases are the primary means by which any digital data and applications are stored. At a high level, these databases consist of a hard drive or series of hard drives whose low level operations (*i.e.* where data is stored) is managed by the operating system (Windows, Mac, Linux, etc). A SQL (Structured Query Language) server runs on top of the operating system and is responsible for how the data is accessed, organized, and used. These digital databases are typically centralized and managed by either the business or a TTP. Centralized databases are easy to maintain and simple to implement, but data stored in these databases can be easily manipulated (mutable) by both external and internal actors due to its centralized nature (*i.e.* there is a single point of failure). Centralized databases also suffer from increased complexity and maintenance cost as the number of users increase. As users increase, the amount

of data stored in the database increases, driving a need for more costly digital space, operational resources, and more IT personnel to manage the database. These problems are significantly magnified for applications that require the interchange and communication of data across different databases. These applications include the formation of consortiums or coalitions in which businesses pool their resources together to achieve a common goal. Generally, centralization introduces a significant amount of friction in these applications because it inhibits modularity (must give control to a central entity, making it difficult to change individual structure), interoperability (different technology, different data structures, etc) and inclusion (difficult, incurs a cost, or slow to add new businesses).

1.4 The Blockchain

1.4.1 Overview

Blockchain is a novel technology that can address many of the pitfalls of centralized databases. Blockchain can provide an open, distributed database of records acting as a public ledger of all transactions or digital events that have occurred between all participating entities. Essentially, it is a shared database that allows multiple users (who do not trust each other) to transparently and securely modify the database directly to reflect a state change or digital event. This is indeed revolutionary because it enables an ecosystem that distributes the cost and resources to manage and operate a database among all the participants, not just the businesses providing a service. Furthermore, due to the decentralization of the data, a blockchain makes it nearly impossible for external or internal actors to manipulate the data. Indeed, one of the key security features of a blockchain is immutability- once data is stored on the blockchain, it cannot be changed.

“If TCP/IP is the standard for secure information transfer, then blockchain is the standard for secure value transfer.”

Bitcoin [5], the world’s first renowned public blockchain, represents the first use case of blockchain technology by generating value through digital scarcity. In the Bitcoin framework, the exchange of the native cryptocurrency, Bitcoin (BTC), represents a unique transaction. More precisely, consider the following example where John sends 1 BTC to Justin, who subsequently sends 0.5 BTC to Hayden. For simplicity, let us assume that John has 1 BTC in his account, while Justin and Hayden have 0 BTC in theirs. If John sends Justin 1 BTC, John signs a new transaction agreement that deducts 1 BTC from John’s account. This transaction agreement is now worth 1 BTC, and can only be spent by Justin. The transaction agreement between John and Justin (call this T_1) is now used to fund this transaction. Justin signs two transaction agreements: one transaction agreement that subtracts 0.5 BTC from T_1 and a second transaction agreement (call this T_2) with Hayden that is worth 0.5 BTC, which Hayden can spend immediately after the transaction is verified. Thus, in the Bitcoin use case, the blockchain is simply a ledger of unique transactions.

The security foundations of blockchains rely on asymmetric cryptography and distributed consensus [6]. Each transaction agreement in the blockchain is protected with a digital signature. John uses his private key to sign the transaction agreement worth 1 BTC with Justin. Justin, using his public key, is then able to independently verify from the digital signature that John authorized the transaction. This prevents a malicious participant from forging a

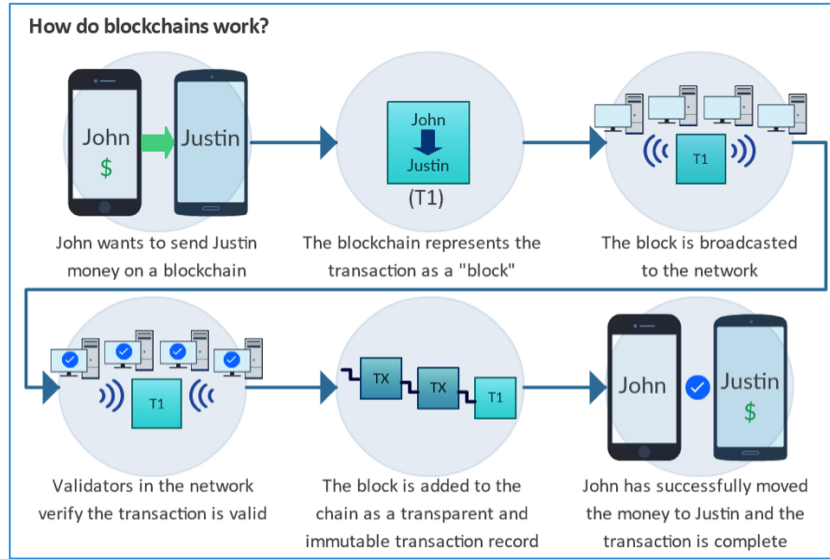


Figure 1: Overview of How Blockchains Work

transaction involving John's assets because (s)he must have John's private key. This transaction (and the transaction between Justin and Hayden) is broadcasted to every participant in the blockchain network in order to be validated and recorded. Transactions are ordered by placing the validated transactions into blocks. These blocks are then linked together to form a chain (hence blockchain) preserving a proper linear, chronological order. For example, the transaction between John and Justin (T_1) will always precede the transaction between Justin and Hayden (T_2) because any attempts to include T_2 in a block where T_1 does not precede T_2 will be rejected during the validation process (since Justin only has enough BTC to send to Hayden, if John sends it to him first). Note that since every participant is able to manage the blockchain, multiple blocks can be generated by different participants at the same time. In the Proof-of-Work (PoW) scheme, the first participant to solve an extremely difficult cryptographic puzzle will be able to submit their block to the blockchain provided that they prove to everyone in the network that they solved the puzzle. The process of validating the block and the participant's proof that (s)he solved the puzzle forms the consensus portion of the blockchain. Since everyone has the same version of the truth (i.e. same blockchain), it is impossible to change the contents of any block of the chain without getting caught. Furthermore, the difficulty of solving the cryptographic puzzle prevents one person from adding a false block to the chain. Figure 1 shows a general overview of how blockchains work.

The advent of Bitcoin has helped spawn more advanced blockchain-based platforms. Ethereum [7] is one of these platforms, which allows the implementation of so called smart contracts—computer programs that control digital assets on the blockchain through a set of arbitrary rules. Smart contracts allow for the complete automation of processes requiring a TTP such as trade agreements, crowdfunding, and redemption of loyalty points. Decentralized applications (Dapps) are client-side applications that allow participants in the blockchain to interact with smart contracts. Dapps and smart contracts enable a dynamic environment for the interaction between participants on the network. Figure 2 illustrates the interaction between Dapps and smart contracts.

Blockchains have seen tremendous growth since the introduction of Bitcoin, and the technology's development has accelerated due to increased adoption by startups and industry alike. For example, the Ethereum project continues to grow as it attempts to solve industry

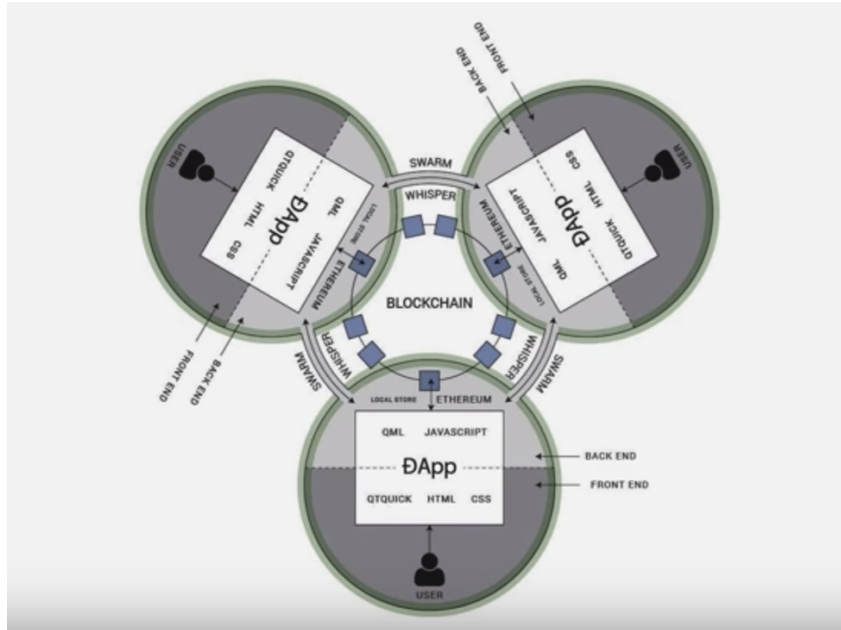


Figure 2: Interaction between Dapps and Smart Contracts

concerns about scaling, customer privacy, and regulation. Alternative blockchain-based platforms such as IBM’s Hyperledger Fabric [8], Microsoft’s Coco Framework [9], Multichain [10], and NEM [11] address the problem of scaling and customer privacy through permissioned or private blockchains. While these platforms handle a narrower range of use cases, they address some of the major problems raised by industry. Projects, such as Cardano [12], aim to solve these problems while preserving the complexity of applications that can be run on the blockchain.

1.4.2 Permissionless vs. Permissioned Blockchains

A Proof of Utility in Equal-level Partnership Model vs Dominant LP Model

Theorem 1. *For any merchant $i \in M$, the individual utility of merchant i , Π_i^* , is greater in the equal-level partnership design than that same merchant i 's utility, Π_i , in the dominant LP design. In other words, $\Pi_i^* > \Pi_i, \forall i \in M$.*

Proof. The following inequality is shown to hold for all $i \in M$.

$$\begin{aligned} \Pi_i^* &> \Pi_i \\ \sum_{k \in M} [\theta_{ki}a_i - \theta_{ik}(a_k c_{ik} - q_i)] &> \sum_{n \in M-N_\ell} [\epsilon \theta_{ni}a_i - \epsilon \theta_{in}(a_n c_{in} - q_i)] + \sum_{j \in N_\ell} [\theta_{ji}a_i - \theta_{ij}(a_j c_{ij} - q_i)] \\ \sum_{k \in M-N_\ell} [\theta_{ki}a_i - \theta_{ik}(a_k c_{ik} - q_i)] &+ \sum_{j \in N_\ell} [\theta_{ji}a_i - \theta_{ij}(a_j c_{ij} - q_i)] \\ &> \epsilon \sum_{n \in M-N_\ell} [\theta_{ni}a_i - \theta_{in}(a_j c_{in} - q_i)] + \sum_{j \in N_\ell} [\theta_{ji}a_i - \theta_{ij}(a_j c_{ij} - q_i)] \end{aligned}$$

Subtracting like terms on both sides, it is clear the the following inequality holds for all $i \in M$ since $\epsilon \in (0, 1)$.

$$\sum_{k \in M-N_\ell} [\theta_{ki}a_i - \theta_{ik}(a_k c_{ik} - q_i)] > \epsilon \sum_{n \in M-N_\ell} [\theta_{ni}a_i - \theta_{in}(a_j c_{in} - q_i)]$$

Note that the above proof is for the special case where there is absolutely no switching cost in the equal-level partnership model. The result above is easily attained for the more general condition where switching costs exists between competitive merchants in the equal-level partnership model. Denote $M_c \subseteq M$ as the set of merchants m that are directly competitive with merchant i such that $c_{im} = c_{mi} = 1, \forall m \in M_c$. The following inequality must then hold.

$$\begin{aligned} \sum_{k \in M-N_\ell-M_c} [\theta_{ki}a_i - \theta_{ik}(a_k c_{ik} - q_i)] &+ \epsilon \sum_{m \in M_c} [\theta_{mi}a_i - \theta_{im}(a_m c_{im} - q_i)] \\ &\geq \epsilon \sum_{n \in M-N_\ell} [\theta_{ni}a_i - \theta_{in}(a_j c_{in} - q_i)] \end{aligned}$$

□

Using the result from Theorem 1, it is now possible to prove the second feature of the equal-level partnership model on the Coalition protocol.

Corollary 1. *Given $\Pi_i^* > \Pi_i, \forall i \in M$, social welfare in the equal-level partnership model is greater than social welfare in a dominant LP protocol. In other words,*

$$\sum_{i \in M} \Pi_i^* > \sum_{j \in N_1} \Pi_j + \sum_{k \in N_2} \Pi_k + \dots + \sum_{\ell \in N_m} \Pi_\ell$$

Proof. Since $\Pi_i^* > \Pi_i, \forall i \in M$, then

$$\begin{aligned} \sum_{i \in N_k} \Pi_i^* &> \sum_{i \in N_k} \Pi_i, \quad \forall k \in \{1, \dots, m\} \\ \sum_{i \in N_1} \Pi_i^* + \sum_{j \in N_2} \Pi_j^* + \dots + \sum_{k \in N_m} \Pi_k^* &> \sum_{i \in N_1} \Pi_i + \sum_{j \in N_2} \Pi_j + \dots + \sum_{k \in N_m} \Pi_k \end{aligned}$$

Since $\langle N_k \rangle_{k \in \{1, \dots, m\}}$ is a partition of M , then $\cup_{i=1}^m = M$. Thus,

$$\sum_{i \in M} \Pi_i^* > \sum_{j \in N_1} \Pi_j + \sum_{k \in N_2} \Pi_k + \dots + \sum_{\ell \in N_m} \Pi_\ell$$

□

B Optimal Seigniorage

Lemma 1. *The maximum seigniorage that the treasury will absorb during any period of time T is as follows.*

$$S^* = p^*(1 - \delta^-)(1 + \alpha^-)Q_0$$

Proof. The treasury initiates a series of absorption tranches causing an incremental depletion of the seigniorage pool as follows.

$$\Delta S_i^- = S_{i+1} - S_i = p^*(1 - \delta^-)(1 + \alpha^-)u_i$$

Since $u_i = Q_i \delta^-$ hence $Q_i = Q_0(1 - \delta^-)^i$, then by induction $\Delta S_i^- = p^*(1 - \delta^-)(1 + \alpha^-)Q_0(1 - \delta^-)^i \delta^-$. Denote $S_{M_T}^-$ as the amount of supply absorbed after some time T , then it is defined as

$$\begin{aligned} S_{M_T}^- &= \sum_{i=0}^{M_T-1} \Delta S_i^- = \sum_{i=0}^{M_T-1} p^*(1 - \delta^-)(1 + \alpha^-)Q_0(1 - \delta^-)^i \delta^- \\ &= p^*(1 - \delta^-)(1 + \alpha^-)Q_0 \sum_{i=0}^{M_T-1} (1 - \delta^-)^i \\ S_{M_T}^- &= p^*(1 - \delta^-)(1 + \alpha^-)Q_0(1 - (1 - \delta^-)^{M_T}) \end{aligned} \tag{1}$$

where the third equality is due to the geometric series $\sum_{i=0}^{M_T-1} (1 - \delta^-)^i = \left(\frac{1 - (1 - \delta^-)^{M_T}}{\delta^-} \right)$. By taking the limit $M_T \rightarrow \infty$ (*i.e.* market behavior is becoming increasingly bearish) of the above equation, the maximum amount of seigniorage required to absorb the whole supply R_0 during a given period T (denoted as S^*) is found.

$$\begin{aligned} \lim_{M_T \rightarrow \infty} S_{M_T}^- &= \lim_{M_T \rightarrow \infty} p^*(1 - \delta^-)(1 + \alpha^-)Q_0 \delta^- (1 - (1 - \delta^-)^{M_T}) \\ &= p^*(1 - \delta^-)(1 + \alpha^-)Q_0 \\ &= S^* \end{aligned}$$

□

C RAA Seigniorage Pool Deplete Probability Bounds

Theorem 2. *If the treasury starts period T with $\hat{S} = \epsilon S^*$ amount of seigniorage, then the probability that the treasury is depleted at the end of period T is as follows, where $\mathbb{P}(\text{deplete}) = \mathbb{P}(S_{M_T} \geq S_0)$.*

$$\begin{aligned} &1 - \Phi(\mathbb{I}(\log_{1-\delta^-}(1 - \epsilon) - \lambda^- + 1) \sqrt{(2H(\lambda^-, \log_{1-\delta^-}(1 - \epsilon) + 1))}) \\ &< \mathbb{P}(\text{deplete}) \\ &< 1 - \Phi(\mathbb{I}(\log_{1-\delta^-}(1 - \epsilon) - \lambda^-) \sqrt{(2H(\lambda^-, \log_{1-\delta^-}(1 - \epsilon)))}) \end{aligned}$$

Proof. In order to determine \hat{S} , it is necessary to determine the probability of any given $S_0 = \hat{S}$ being depleted, *i.e.* $\mathbb{P}(S_{M_T} \geq S_0)$ where $S_{M_T} = S^*(1 - (1 - \delta^-)^{M_T})$ is derived by combining Equations 1 and ???. The first step is to find a condition with respect to M_T such that $S_{M_T} \geq S_0$, and is as follows

$$\begin{aligned}
S_{M_T} &\geq S_0 \\
1 - (1 - \delta^-)^{M_T} &\geq \epsilon \\
1 - \epsilon &\geq (1 - \delta^-)^{M_T} \\
M_T &\geq \log_{1-\delta^-}(1 - \epsilon)
\end{aligned} \tag{2}$$

where the inequality flip in Equation 2 results from $\log_{1-\delta^-}$ being a strictly decreasing function. Since M_T is a Poisson process with parameter, λ^- , probability bounds for Equation 2 can be found using Poisson distribution bounds derived in [13]. Using these bounds and defining the *KL divergence* equation as $H(x, y) = x - y + y \ln \frac{y}{x}$, the probability of the seigniorage pool being deplete during T is derived as follows,

$$\begin{aligned}
&1 - \Phi(\mathbb{I}(\log_{1-\delta^-}(1 - \epsilon) - \lambda^- + 1)\sqrt{(2H(\lambda^-, \log_{1-\delta^-}(1 - \epsilon) + 1)))}) \\
&< \mathbb{P}(M_T \geq \log_{1-\delta^-}(1 - \epsilon)) = \mathbb{P}(S_{M_T} \geq S_0) = \mathbb{P}(\text{deplete}) \\
&< 1 - \Phi(\mathbb{I}(\log_{1-\delta^-}(1 - \epsilon) - \lambda^-)\sqrt{(2H(\lambda^-, \log_{1-\delta^-}(1 - \epsilon)))})
\end{aligned}$$

□

References

- [1] Teresa Villacé-Molinero, Pedro Reinares-Lara, and Eva Reinares-Lara. Multi-vendor loyalty programs: Influencing customer behavioral loyalty. *Frontiers in Psychology* 7, 4, 2016.
- [2] Colloquy loyalty census (2015). <https://www.colloquy.com/latest-news/2015-colloquy-loyalty-census/>.
- [3] Bond loyalty report (2016). <http://info.bondbrandloyalty.com/2016-loyalty-report>.
- [4] Us online travel overview 2017 phocuswright report. <https://www.traveltrends.biz/ttn555-otas-increase-market-share-at-suppliers-expense/>.
- [5] S Nakamoto. Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>, 2008.
- [6] John Prpić. Unpacking blockchains. arXiv preprint arXiv:1703.06117, 2017.
- [7] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151, 2014.
- [8] Ibm hyperledger fabric. <https://www.hyperledger.org/resources/publications>.
- [9] Microsoft coco framework. <https://github.com/Azure/coco-framework/blob/master/docs/Coco%20Framework%20whitepaper.pdf>, 2017.
- [10] Gideon Greenspan. Multichain private blockchain - white paper. <https://www.multichain.com/download/MultiChain-White-Paper.pdf>.
- [11] Nem - distributed ledger technology. <http://docs.nem.io/en>.
- [12] Cardano. <https://cardanodocs.com/>.
- [13] Michael Short. Improved inequalities for the poisson and binomial distribution and upper tail quantile functions. *ISRN Probability and Statistics*, 2013.