Crossing the Chasm: Enhancing Cryptocurrency Adoption by Leveraging a Transaction and Trading Layer for the Points Economy and Other Digital Assets

-

Whitepaper - Version 2.2
November 30, 2018

Al Burgio

Founder of DigitalBits Foundation
aburgio@digitalbits.io

Abstract. Blockchain technology is promoted as one of the great technological advances of our time and considered as a solution to many of the technical problems faced by industries in sectors such as finance, automobile, and retail. Despite growing attention and utilization, mass adoptions of cryptocurrencies has not happened yet. So how do we cross the chasm from the vision phase to the actual use phase? To do so, blockchain technology has to target a pre-existing legacy market that already posses billions of user accounts globally in a digital asset category; Not to create a competing tokenize digital asset, but instead to transform these legacy digital assets into tokens on a public blockchain with key functionality that benefits both consumers and the enterprise-issuers of these digital assets.
This whitepaper fills the gap in the state of the art by presenting the DigitalBits blockchain powered infrastructure that builds a bridge facilitating the implementation of new technologies to support and enhance our every day life interactions as well as foster blockchain mass adoption. The DigitalBits blockchain allows for easy asset-tokenization using a transaction and trading layer for the point economy. We present a loyalty- and reward points focused running case, detail the advantages of the system, outline the requirements and goals, as well as the architecture of the DigitalBits network and ecosystem. In addition, we present the on-boarding process of digital assets and the asset tokenization which is an indispensable functionality of our platform. Furthermore, we introduce the novel idea of the token name certification service (TNCS) that prevents malicious network entities from issuing and distributing illegitimate tokens of assets that they are not associated with. Finally, we present the XDB token value proposition and the surrounding token economy ecosystem that fuels the platform.

Keywords: Loyalty Programs, Digital Assets, Tokenization, Payment, Remittance, Blockchain, Smart Contract, Point Economy, DigitalBits, Liquified Assets

1 Introduction

The vision for cryptocurrencies has been embraced by many people around the world. In 2017, the world saw a surge in Initial Coin Offerings (ICOs) with associated whitepapers that has driven tremendous enthusiasm for the futurist possibilities of blockchain technology and utility tokens [3][43]. However, as the end of 2018 is near, many people are beginning to wonder: When will many of these cryptocurrencies and utility tokens begin to gain wide real world use and adoption? How do we cross the chasm from the vision phase to the actual use phase? To do so, blockchain technology has to target a pre-existing legacy market that already posses billions of user accounts globally in a digital asset category; Not to create a competing tokenize digital asset, but instead to transform these legacy digital assets into tokens on a public blockchain with key functionality that benefits both consumers and the enterprise-issuers of these digital assets.

Loyalty and rewards points (LRPs) presents a unique opportunity as the first digital asset category to leverage the DigitalBits blockchain and help drive mass growth of cryptocurrency adoption. Such programs are established means to improve customer engagement and brand awareness. Needless to say, due to their recognized and tremendous potential, these membership programs spread across several industries, as for example, travel, retail, financial services, and so on. A successful loyalty and reward program ensures that a customer keeps returning to a specific brand in order to make purchases and subsequently earn reward points thereby building *loyalty* and retaining customers over the years. At the same time, companies that effectively create, launch and run loyalty programs underline their commitment to long term relationships with their customers [29]. A 2014 report suggests that 91% of companies employ some form of customer engagement or loyalty program [18], resulting in 3.8 billion individual loyalty program memberships just in the United States [12]. The average U.S. household participates in 29 different loyalty programs [11], whereas in the UK the average customer is a member of more than 14 different loyalty programs [14]. According to a report from 2017, the estimated overall corporate liability for loyalty points exceeded $100 billion, thereby representing a new unsurpassed high and an enormous business potential [6].

However, despite the widespread availability of these programs, only a small fraction of their potential is used. Consumers are generally discouraged by unnecessary barriers to accumulate and redeem their points and by changes to program rules or rewards. Hence, users get easily frustrated and millions of points are unredeemed. Furthermore, the lack of transferability and portability of most LRP programs affects their perceived value by customers, since they are unable to transfer or trade those points at any time for other points they desire. Of the $48 billion in total perceived value of points and miles issued in 2010 in the U.S., about $16 billion worth of LRPs were left unused [20]. It is important to note, that it is not just the customers putting up with the downsides of current state of the art solutions. Loyalty program providers have high entry barriers to set up their own reward program. Once they have created their own program, providers suffer from high costs of maintenance. Moreover, even if they wish

to achieve a certain level of compatibility with another membership program, the underlying infrastructure is often incompatible. Hence, a more holistic and interoperable solution is required.

Blockchain technology, also referred to as distributed ledger system, is most noticeably known for providing the foundation of the peer-to-peer (P2P) cryptocurrency and payment system Bitcoin [34], but nowadays there a various different platforms out there, e.g., [25][39][48]. In the context of LRP programs, blockchains have the potential to enable interoperable and holistic platforms for the next generation of loyalty programs. Blockchain-based LRPs can be easily transferred and redeemed - even across other businesses or services. In addition, LRPs become interchangeable and can be exchanged for other loyalty points or even fiat currencies. Finally, a blockchain-based solution significantly reduce development, integration, reconciliation, and security costs for the program providers.

In recent times, nearly a dozen companies announced their intent to launch blockchain based LRP programs to encourage customer engagement [38]. However, most of them merely translate the legacy LRP programs into a blockchain based solution with separated data silos and a lack of interoperability. Others are built on first generation blockchains, such as Bitcoin and therefore, suffer technological downsides such as high transaction fees, limited scripting languages or missing scalability. In contrast, we envision a solution that is not only limited to ease the creation, transfer and exchange of LRPs on a blockchain but also offer an easy-to-use platform which allows the tokenization of all kinds of assets at the mere click of a button. This, as a result, fosters the mass market adoption of blockchain technology.

This whitepaper addresses the detected gap by introducing the DigitalBits blockchain, thereby answering the question of how to enable easy asset-tokenization using a transaction and trading layer for the point economy? In order to answer this question with a separation of concerns, we pose the following sub-questions: What are the goals and requirements of such a system? What is the architecture of the DigitalBits asset tokenization platform? What are the system-engagement processes for the stakeholders? What is the long term vision of DigitalBits?

The remainder of this paper is structured as follows: Section 2 introduces background information, a running case as well as related work. Section 3 focuses on defining functional as well as quality goals and the requirements of the DigitalBits system, together with the positioning of stakeholders. Next, Section 4 analyses and outlines the resulting system architecture that we derive from the requirements. Section 5 expands on the system engagement processes for the stakeholders. Finally, Section 6 concludes this work.

2 Technical Background and Running Case

In Section 2.1 we provide an introduction into LRP programs. Afterwards, Section 2.2 presents an exemplary use-case – HotelBrand –, that we use as a running case to detail the DigitalBits framework and solution throughout the rest of the

paper. Next, the state of the art on blockchain-based LRP solutions is presented in Section 2.3.

2.1 Loyalty and Reward Points Programs

LRPs are a means adopted by companies and brands to engage the consumer repeatedly, develop a long standing relationship with the consumer and encourage the consumer to choose a particular set of products offered by a brand (or a group of brands) over other brands offering similar products. In the current landscape, there are two types of LRP programs. One is a single business program in which the points are issued by the same business, such as the *Advantage program* of American Airlines and *Starbucks Rewards* or Starbucks. The second type is a multi-business program, in which the points issuer is a third party. For example, LoyaltyOne and its Air Miles program or *Payback* in Germany.

A variety of companies and brands have applied these LRP programs. Studies show that roughly 80% of Americans belong to some type of reward program [47]. The average US household belongs to 29 loyalty programs [5] and 71% of loyalty program members say that they are open to joining more programs [42]. There were 3.8 billion individual loyalty memberships in the US in 2017 and 175 million loyalty memberships in Canada in 2016 [19]. These figures reflect a 15% growth in the U.S. and 35% growth in Canada since 2014.

2.2 Running Case

HotelBrand is a fictional flourishing chain of hotels with a global presence. Similar to other hotel chains, HotelBrand has an ongoing loyalty program with roughly 30 million customers and approximately 40 billion points in circulation. However, owing to the fiercely competitive hospitality market, HotelBrand is currently languishing at the 10th place. Moreover, it is facing heavy competition from a variety of innovative startups that are primarily focused on a sharing economy. In order to enhance their market share in the upcoming years, HotelBrand has identified that a key solution to strive in the market should be the overhauling of their LRP program with the objective to make it more customer-centric. A customer-centric LRP program has features such as ease of sign-up and use, and more importantly, facilitate high liquidity, i.e., allow the customer to easily collect, monitor, share and utilize the accumulated points. High liquidity results in higher customer engagement and an increase of the perceived value of the LRP program. This encourages new customers, in addition to their current clientele, to avail their services over their competitors. HotelBrand is naturally looking to expand and increase their worldwide reach and aspires to be the market leader. Therefore, they are interested in creating a platform that can dynamically and easily scale up with their ever ambitious goals. However, HotelBrand realizes that the following factors could the revamp of their LRP program:

– Infrastructure (including maintenance, scale & security): High liquidity results in a significant increase in the number of transactions that need to

be performed on a daily basis. They have to further take into account that there could be spikes in the amount of transactions during the day, based on consumer behavior patterns. A large part of the transactions are expected to be performed online. Their infrastructure has to be upgraded in order to cater these demands. A cloud-based system is appealing, however, in addition to the huge cost, this requires in-house expertise in maintenance, dynamic scaling, and security.

– Consumer experience: In order to accommodate the current trends to operate via mobile Apps, an App rich in features and appeal, has to be developed. The major concern though, is of consumer engagement. Although Apps are easy to install, the large number of them on a consumer's phone tends to suffer the same issues as that of multiple loyalty cards with a consumer – a lack of enticement for the customer. The App might be yet another App on the consumers' phone and thus not used frequently.
– Costs & Time: Regardless of prioritizing and choosing an in-house or a cloud-based version, the costs of creating and then maintaining such a program would be huge. Moreover, the launch of an overhauled LRP program also requires a lot of development time.

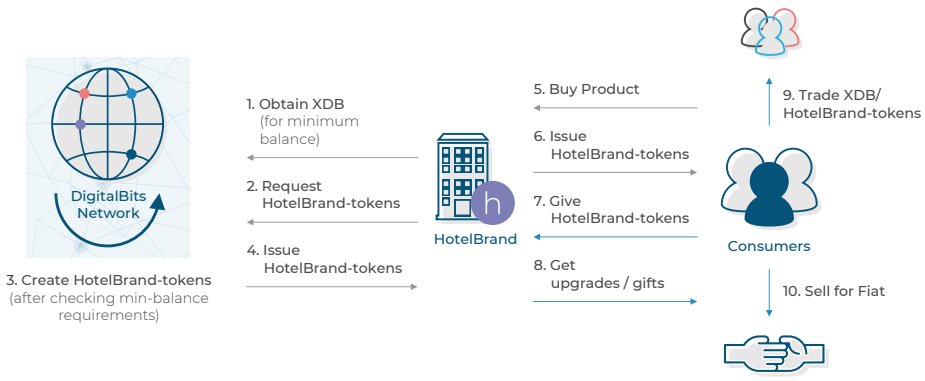


Fig. 1: Use-case of HotelBrand creating and using HotelBrand-Tokens on the DigitalBits network: 1.) HotelBrand obtains the minimum XDB-tokens required for participation in the DigitalBits network; 2.) Create HotelBrand-Tokens; 3.) HotelBrand-Tokens being created by DigitalBits network; 4.) HotelBrand-Tokens issued to HotelBrand; 5.) Consumer-Tom booking a room offered by HotelBrand; 6.) HotelBrand issuing the corresponding HotelBrand-Tokens; 7.-8.) Consumer-Tom choosing to trade the tokens for a free room at HotelBrand; 9.) Consumer-Tom choosing to trade some of her HotelBrand-Tokens or XDB-tokens with other consumers; and 10.) Consumer-Tom choosing to sell her HotelBrand-Tokens or XDB-tokens for fiat currency or other cryptocurrency.

HotelBrand is monitoring the hype behind blockchain, championed as the solution to many prevalent technological problems. Nonetheless, early prototypes investigated by their teams revealed that blockchain based solutions have pitfalls such as huge transaction fees and time. Recently, HotelBrand is intrigued by the blockchain based solution offered by DigitalBits, especially the manner in which it overcomes many of the limitations of the earlier generations of blockchain.

A key feature provided by DigitalBits is that the offered tokens have high liquidity, in alignment with HotelBrand's customer-centric focus. They appreciate that DigitalBits allows them to create a new LRP program at virtually no cost[1]. They also realize that the system can dynamically scale in order to handle their global consumers. Moreover, they realize that they can start off by using the basic app provided by DigitalBits and later invest on developing a brand-specific app on top of the basic app by making use of its APIs and SDK. The only cost they incur is a very low transaction fee[2], a cost that is required to ensure the integrity of the transaction. The fee is used to sustain the ecosystem. HotelBrand, therefore, uses the money saved to pass on more benefits to the consumers and also increase their marketing and consumer engagement activities, and more importantly, focuses on their core product.

As depicted in Figure 1, HotelBrand obtains the minimum XDB-tokens . They then proceed to create a new token, HotelBrand-Tokens for their brand and specify the maximum tokens that they would like to have. When Consumer-Tom books a room at one of their hotels, they transfer some tokens to Consumer-Tom based on their own internal algorithm. Consumer-Tom is immediately able to see the increase in HotelBrand-Tokens in her DigitalBits-enabled App which she regularly uses with other brands. Moreover, she is glad not having to install yet another app or fill up a form for another loyalty card. At a later point in time, Consumer-Tom would like to use some of her HotelBrand-Tokens to avail a free room from HotelBrand and also convert the rest into tokens to avail a discount on her next flight. Consumer-Tom also periodically chooses to convert some of her tokens into XDB-tokens to benefit from the growing value of the DigitalBits network.

2.3 Related Work

Currently, most LRP programs exist in silos, i.e., belong to a certain brand (or group of brands) and cannot be easily transferred or traded with. Since each of them exists in custom-built infrastructure, it is practically impossible to merge or facilitate real-time interworking among two different LRP program, even when the brands wish to do so. Moreover, a peer-to-peer based platform that facilitates the transfer and trade between different LRP programs has not historically existed. This problem does not merely arise from businesses desiring

[1] they will have to obtain the minimum XDB-tokens (DigitalBits native token) required to maintain the account, which is currently set at 10 XDB-tokens

[2] currently set at 1 XDB-tokens for 100,000 transactions and can be changed only with consensus

to hold on to their customers, but also that the barrier to facilitate such a system is high. Businesses that are keen on making their platform more open face hurdles of scale, cost and time. As a result, customers are forced to carry different cards for each of the loyalty programs or install a new app for each of them on their phone. Apart from the issue of overloading a wallet/phone, one also has to weigh in the chances of a customer remembering if he or she is a member of the loyalty program or not. The entry barrier for new players is also high when we consider the high costs, time to launch, maintenance/scaling efforts, security and the need for skilled personnel.

	DigitalBits	**Stellar**	**Ethereum**
Blocktime (w/ Confirmations)	2-5s	2-5s	5m to 1h+
# of Confirmations	1	1	30
Processing Method	Validation	Validation	Confirmations via Mining / PoW
Transaction Costs	Very Low	Very Low	High
Multi-Asset	Built-in	Built-in	Custom App via Smart Contracts
Distributed Exchange	Built-in	Built-in	Custom App via Smart Contracts
Compliance Mechanism	Built-in via compliance server	Built-in	No
Inflation	No	Yes	Yes
Mining	Pre-mining	Pre-mining	PoW & PoS
Certified Token Issuer	Yes	No	No
TNCS	Yes	No	No
Automatic Algorithmic Native Token Distribution	Yes	No	Yes

Fig. 2: Platform Comparison of DigitalBits, Stellar and Ethereum.

Blockchain has the potential to ease many of the aforementioned problems. However, many of the blockchain based solutions are in fact Decentralized Apps (Dapps) built on Ethereum [48]. This subjects them to issues such as high trans-

action costs, verification time and low transaction processing rate. Moreover, since *ETH*[3] continue to be created every day, they are also subjected to inflation. Solutions such as Qiibee [40], have a huge entry cost by binding the value of tokens to their native currency, similar to how certain monetary systems used the gold standard [17]. A key issue with Dapps is that they can support only one native token, similar to many of the legacy LRP programs. Therefore, all participating brands have the same native coin with the same features and confinement to a silo. Alternatively, blockchain platforms such as Ethereum[4] [48], Waves[5] [23] and Stellar[6] [31][45] allow users to create their own tokens. DigitalBits, a fork of Stellar, shares many of the benefits of Stellar, but differs in key aspects such as not subjecting its tokens to inflation, and is developing a token name certification service and an automatic algorithmic token distribution. Figure 2 presents a high level comparison between DigitalBits, Stellar and Ethereum. Waves, which relies on Proof-of-Stake (PoS), provides similar features like Ethereum and is comparable in performance to Ethereum. DigitalBits, outperforms both Ethereum and Waves in terms of the number of transactions per second (10,000 transactions per second [7]) and the time to verify transactions (approximately 3-5 seconds [45]). Additionally, it provides features such as legal compliance, multi-asset support and a distributed exchange.

3 Goal Modeling and Requirement Engineering

The previous section introduced the DigitalBits running case, that we now use to deduce the functional- and non-functional requirements that our system must adhere to, in order to address the drawbacks and limitations of current LRP programs. To systematically capture the necessary requirements, we use one part an Agent-Oriented Modelling (AOM) methodology [46], i.e., goal models. In the context of system development and software engineering, good requirements follow certain characteristics, e.g., requirements address one issue only and are completely specified without missing information and they must be atomic as well as without conjunctions [13][22][36]. In addition, the requirements have to be consistent and do not contradict itself, or in correlation with other requirements.

The AOM methodology [46] is a socio-technical requirements-engineering approach. It is used to model complex systems that consist of humans, hardware agents, and software agents in a changing environment (also referred to as distributed socio-technical system). Essentially, an AOM goal model presents the software and the tasks it can perform from an agent-oriented view. It therefore enables both, technical and non-technical stakeholders, to capture and understand the functional and non-functional requirements of a complex system. As depicted in Figure 3, *Role*, *Goal* and *Quality Goal* are the three key elements of an AOM goal model. *Roles* of involved entities, i.e., stakeholders, are represented

[3] Ethereums native token
[4] `https://www.ethereum.org/`
[5] `https://wavesplatform.com/`
[6] `https://www.stellar.org/`

in the form of sticky men. Sticky men represent both human entities as well as entities such as apps on their phones that act on behalf of the human entity. The functional requirements are depicted as parallelograms and refer to *goals* of the modeled software system. The non-functional requirements are depicted as clouds and refer to *quality goals* of the modeled software system. The AOM goal model follows a tree-like hierarchy. The root value proposition, i.e., the main *goal*, of the modeled system is at the top. This root goal is decomposed into sub-goals where each sub-goal represents an aspect for achieving its parent goal [30]. These sub-goals are further decomposed into multi-layered sub-goals until the lowest atomic level is reached. *Roles* and *quality goals* may be assigned to either the key goal or the sub-goals and are inherited by all the lower-level goals.

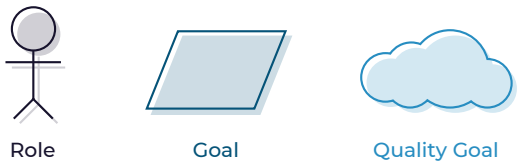


Fig. 3: Selection of AOM notation elements.

This section presents our AOM goal model to define the requirements of the DigitalBits system thereby highlighting the functional and non-functional goals of the platform. In Section 3.1, we first address the top-level goal model comprising the value proposition and the directly linked functional and quality goals along with the relevant stakeholders. Later, Section 3.2 focuses on the lower-level refinements of the model.

3.1 Top-Level Goal Model

Figure 4 presents the top-level AOM goal model of the system using the modeling method described above. The main value proposition is to provide easy asset-tokenization using a transaction and trading layer for the points economy and other digital assets, thereby representing the root of the goal model. The complex main value proposition is split into four sub-goals representing the four main functionalities of the DigitalBits system. The refining functional goals are *enact plugins and Apps*, *tokenize assets*, *trade assets* and *pay and remit*. Furthermore, relevant stakeholders pertaining to these high-level functional goals are also highlighted in Figure 4. These high-level functional goals are refined further in subsequent sections.

Besides the four sub-goals of the top-level AOM goal model, we further identify thirteen quality goals. Nine of these quality goals belong to the main value

proposition and are inherited by all its sub-goals. The remaining quality goals belong to a sub-set of the sub-goals and are inherited by its child-goals.

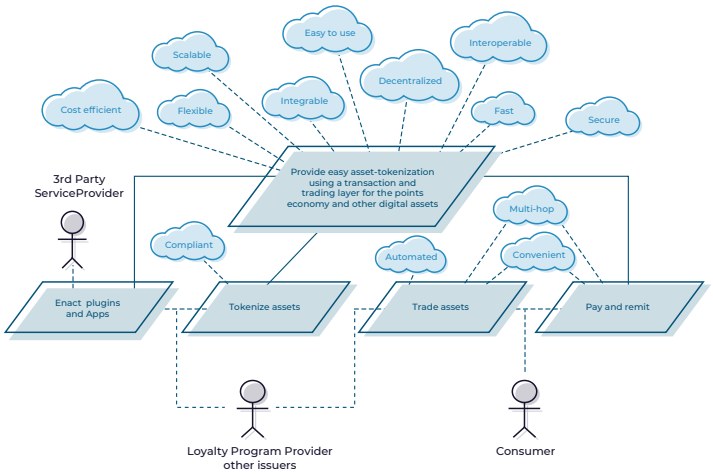


Fig. 4: Value proposition and first level refinement of the DigitalBits goal model.

A *scalable* and *decentralized* system design is necessary for the envisioned platform to handle the large number of LRP program, consumers and the resulting transactions. The LRP program providers have a large consumer base with a worldwide presence and therefore the platform must be able to handle the verification of transactions in a *fast* and *secure* manner. A secure service provision is crucial in terms of operational security, e.g., protect provider as well as consumer accounts and personal data from unauthorized access, secure data transfer within the system between entities or preventing data and information leaks.

The DigitalBits network is expected to support a large variety of LRP programs (and other digital assets) and must therefore be agnostic to the specific needs of an individual provider. The ecosystem is also expected to include a large number of plugins and apps developed by third party developers and therefore must be designed to be *interoperable* and *integrable* in terms of hardware and software design. It is also crucial to *interoperate* at runtime with information systems supporting other business functions.

Since the users of the platform are consumers who are not necessarily tech-savvy, it is important for the platform to be easy-to-use. The consumers must be able to interact with the platform, the plugins and apps easily in order to perform actions such as register for points, collect points, get an overview of their points and trade/sell points. According to [36], easy usability also includes the support of proper error avoidance in order to "anticipate and prevent common errors that occur during a collaboration configuration".

A *reliable* enactment of all transactions and trades is mandatory to facilitate the previous goals. The system must also strive to provide these benefits in a *reliable* and *cost efficient* manner. Last, but not the least, the system must be designed in a *flexible* manner in order to facilitate a highly dynamic process that involves the enactment of diverse activities, the participation of diverse partners, and the exchange of diverse data [35].

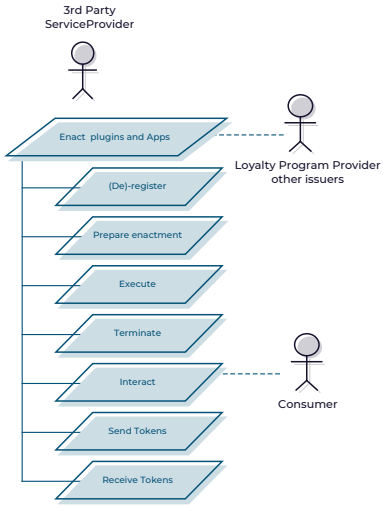


Fig. 5: Lower-level refinements of the *Enact plugins and Apps* functional goal.

3.2 Refined Goal Model

The lower-level refinements of the four sub-goals are detailed below. First, Figure 5 presents the *enact plugins and apps* goal. Applications and plugins have to be registered, prepared for enactment, executed and terminated. Moreover, they have to interact with various entities of the ecosystem depending on the use case, e.g., receiving and sending tokens, or other kind of data. Since nowadays most blockchains offer Turing-complete smart contract languages, the variety of applications and plugins in our ecosystem is quite vast. In the context of DigitalBits, a variety of such services is developed and offered by 3rd party providers and might include services such as wallets or LRP programs. While these are pretty standard apps, more sophisticated applications will be offered as well, e.g., the federation server and the token name service (see Section 4). The DigitalBits federation server are similar to the DNS system of the Internet but instead of resolving website urls to IP-addresses, the federation servers resolve token aliases to the specific smart contract token addresses. The token name certification service (see Section 5) represents a certification service that will map token

names to an entity and ensures a correct binding, e.g., certify that the *Company A*-token actually belongs to Company A and was not created by a malicious entity.

Figure 6 illustrates the refinements of the goal *tokenize assets*. In order to tokenize an asset, it is bind to a token that is created and subsequently issued on the DigitalBits platform. As mentioned previously, the token name certification service being developed can be used to certify issued tokens. Finally, the new digitalized asset has to be managed and be able to be integrated in applications and plugins of the platform. A key quality goal of the requirement *tokenize assets* is legal compliance in terms of who can view and validate transactions.

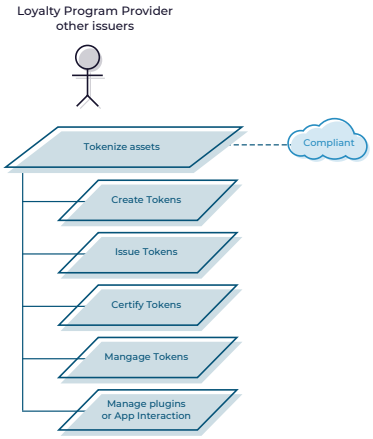


Fig. 6: Lower-level refinements of the *Tokenize assets* functional goal.

The third functional requirement *trade assets*, is shown in Figure 7. The tokenized assets of Figure 6 are worthless if it is not possible to trade and exchange them with other parties. Hence, this functional goal covers on- and off-chain supply and demand administration as well as trade of tokenized assets. Entities may register offers or requests on-chain in order to attract business partners. For other use cases a local supply demand management off-chain is more suitable. In today's highly digital world, *automation* in trading assets is expected by the platform users. *Multi-hop*, i.e., the ability to trade tokens by first converting them to a common token or fiat currency is a feature that adds value to the platform. *Convenience* while making payments, remittance and trading is an expected goal to enhance consumer experience.

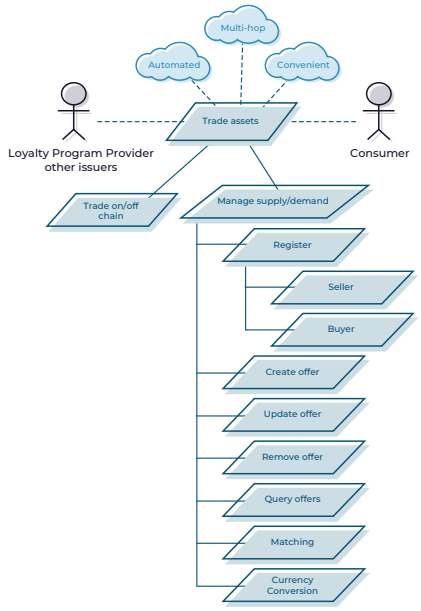


Fig. 7: Lower-level refinements of the *Trade assets* functional goal.

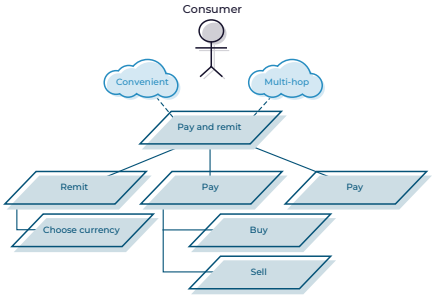


Fig. 8: Lower-level refinements of the *Pay and remit* functional goal.

Finally, the fourth functional requirement *pay and remit* (Figure 8) focuses on the payment and remittance functionalities of our solution. The sub-goal pay is further refined into selling and buying from, or to merchants. In the context of this model, a merchant can also be another user offering a service, or good. The remit sub-goal consists of selecting a currency and recipient for the remittance process. The final functionality is the transaction itself and pertains the payment as well as the remittance process. Again, the quality goals of *multi-hop* and *convenience* apply.

The presented goal model is used in the following Section 4 to derive our system architecture. We do not list all details of the further refined AOM goal model in this whitepaper due to space constraints and in order to focus on the most relevant system components and features.

4 DigitalBits System Design and Architecture

The DigitalBits network consists of entities that perform different but complimentary roles in order to maintain the health of the network. The key role is played by the nodes that run the DigitalBits blockchain-based software and connect to one another. These nodes are well supported by nodes that provide services such as compliance verification, mapping and RESTful APIs. Additionally, APIs, SDKs and wallets provided by DigitalBits facilitate businesses and third party developers to easily develop and deploy their custom apps and wallets. Below, Section 4.1 presents the high level network overview that consists of the various entities that play a vital role. Next, Section 4.2 presents the technology stack and finally Section 4.3 focuses on the system architecture itself.

4.1 DigitalBits Network Overview

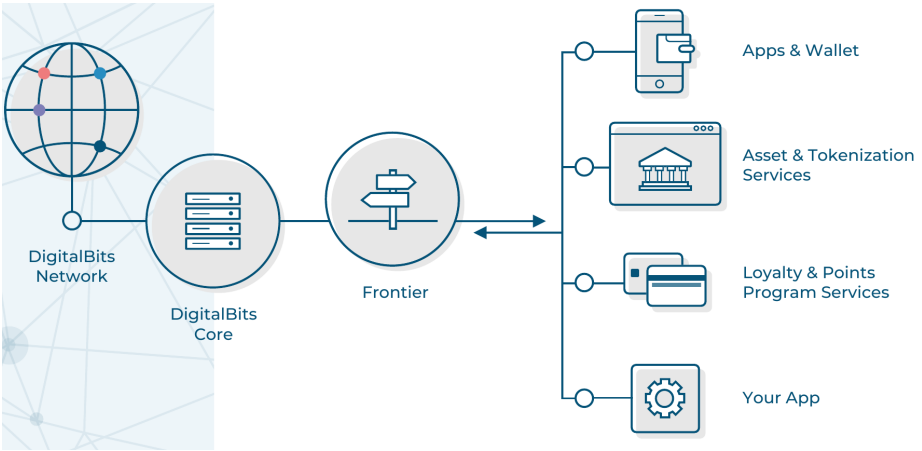


Fig. 9: High Level DigitalBits Architecture Overview

Figure 9 illustrates an overview of the Digitalbits architecture. The DigitalBits architecture consists of the key components described below.

4.1.1 Frontier

Frontier provides a RESTful API for the DigitalBits ecosystem. It acts as the interface to applications that wish to access the DigitalBits network. Frontier

facilitates actions such as the submission of transactions to the network, checking the status of accounts and subscribing to event streams. It also ingests and re-serves the data produced by the Digitalbits network in a form that is easier to consume than the performance-oriented data representations used in the network.

Application developers interact with Frontier's Restful API via the web browser, simple command line tools like cURL, or the DigitalBits SDK. DigitalBits maintains JavaScript, Java, and Go-based SDKs for communicating with Frontier. There are also community-maintained SDKs for Ruby, Python, and C#. The Frontier APIs and SDKs can also be used to build or enhance custom brand specific Apps and clients.

4.1.2 Network Backbone: DigitalBits Core

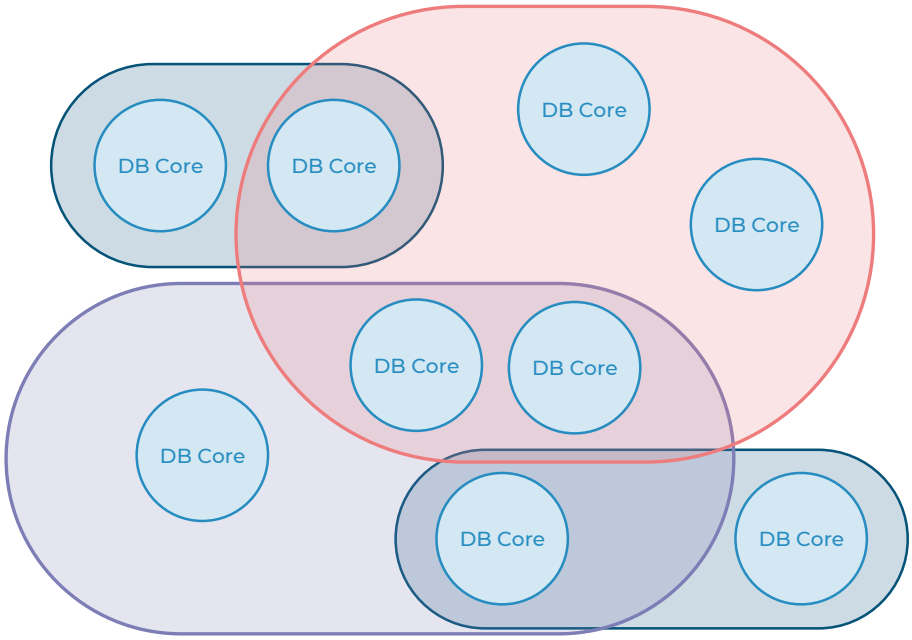


Fig. 10: Quorums, i.e., circles of trust formed among DigitalBits core instances (represented as DB core) of various partner institutes and individuals. The DigitalBits core instances can choose to belong to one or more quorums and utilize them in a hierarchical manner or based on the type of transaction that needs to be verified. The nodes belonging to a quorum need not be located close to one another as can be observed in the blue quorum set.

The DigitalBits core is the backbone of the DigitalBits network. The DigitalBits Core software interacts with a chosen subset of other instances of cores in order to validate and agree on the status of every transaction through the DigitalBits Consensus Protocol (DCP) which is based on the Stellar Consensus Protocol (SCP) [4]. Similar to Stellar's SCP, DCP relies on a Federated Byzantine Agreement (FBA). Unlike the Byzantine Algorithm [9], the FBA does not have a single list of trusted validators, i.e., a centralized list of trusted validators. Instead, an FBA allows for different quorums or sets of validators to co-exist. The nodes can determine the composition of the quorum in a decentralized manner. As shown in Figure 10, DigitalBits core instances of different institutions can choose to participate in one or more quorums subject to the existing quorum members agreeing to grant it access. The quorums facilitates the compliance process based on legal requirements. Organizations may choose one or more quorums that satisfy their requirements. Nodes or organizations could also choose to have a hierarchy of trust with the parameters that define the level of trust that a node accepts for each transaction. In other words, quorum composition and aspects such as simple majority vs. 2/3 majority are defined for different classes of transactions, similar to parliamentary systems in many parts of the world.

The benefit of hosting an own instance of DigitalBits core as compared to just running an App or client is many-fold. Transactions can be submitted without having to rely on a third-party and the DigitalBits core can select its own instance of who to trust, i.e., the quorum. The more organizations and partners contribute instances of DigitalBits core to the network, the more reliable and robust the network becomes. Each organization can choose to run one or more DigitalBits core nodes, which also participate as validators.

4.1.3 The DigitalBits Network

The DigitalBits network itself is a collection of connected DigitalBit cores run by various individuals and entities around the world. Instances of DigitalBits core add reliability to the overall network. Additionally, they may choose to have a Frontier server for communication in order to access the DigitalBits Network. The distributed nature of the network makes it reliable and safe. All these DigitalBit cores within the network eventually agree on sets of transactions. Each transaction on the network costs a small fee: 100 nibbs (0.00001 XDB). This fee helps to prevent bad actors from spamming the network. The DigitalBits Foundation also maintains archive servers with live backups of the current state in the network in order to facilitate new DigitalBits cores to come in sync with the current status of the network.

4.2 Technology Stack

Figure 11 illustrates the key components of the DigitalBits architecture, namely the application server, the bridge server, the federation server and the compliance server. Below, we describe each of these key components. In Section 4.3

we provide the overall architecture and a flowchart based description of how transactions are performed in the DigitalBits network.

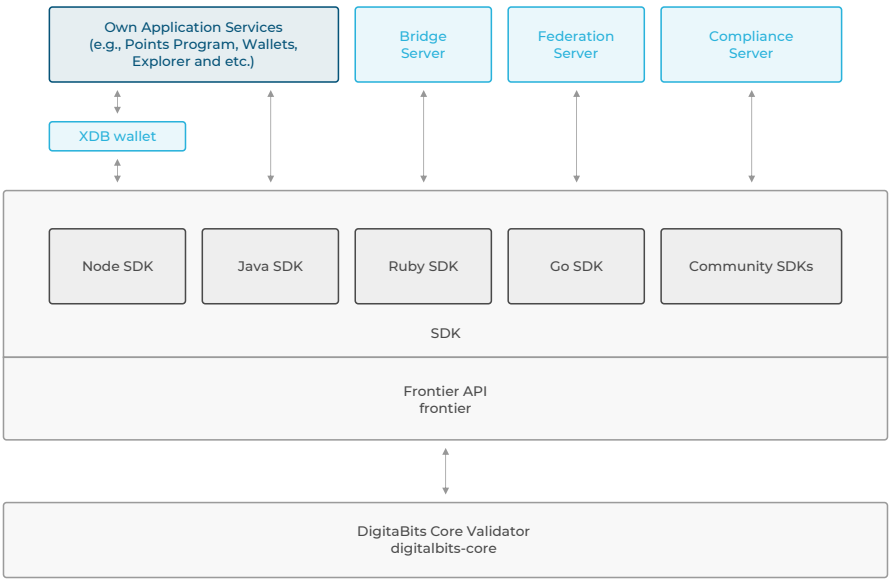


Fig. 11: Technology Stack

4.2.1 Bridge Server

The Bridge server is designed to support applications in easily performing transactions on the DigitalBits network. The bridge server enables applications to use the federation and compliance servers to send and receive payments. As shown later in Figure 15, when a sender wishes to perform a transaction, the sender's client contacts its bridge server in order to initiate the transaction. If required, the bridge server then connects the federation server of the receiver and its own compliance server. If all verifications are successfully completed, the transaction is recorded in the DigitalBits network. The bridge server on the receiver's side periodically monitors the DigitalBits network and spots transactions destined for its end-point and then connects to the required federation and compliance servers as well as finally accepts the transaction. The bridge servers then inform the respective end-points about the result of the transaction.

4.2.2 Federation Server

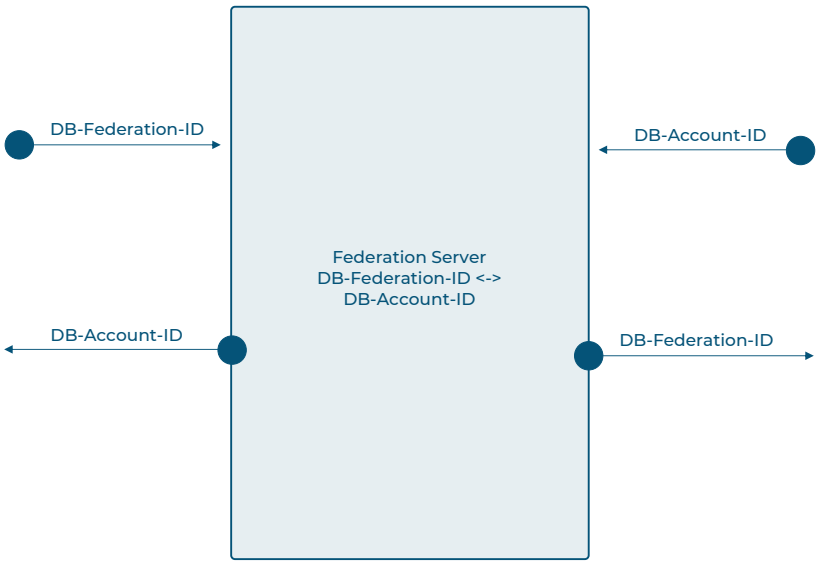


Fig. 12: Federation Server Overview: The federation server holds the mapping between the DigitalBits Account-ID and the Federation-ID and support lookup or reverse-lookup to map from one type of ID to another.

In order to enhance the consumer experience and ease adoption by consumers, DigitalBits associates an account with an email-like human readable identification in addition to the standard public key based identification prevalent in blockchain [34][48]. The human readable email-like address allows consumers to easily use the Apps and clients without having to familiarize themselves with public-key cryptography [15][41].

The role of the federation server is therefore to provide a mapping service between the email-like human readable address and the public key based address. Figure 12 illustrates how an entity interacts with the *federation server* in order to either map a DB-Federation-ID (the email-like address) to a DB-Account-ID (the public key based address) or vice-versa. The DB-Federation-ID is of the form usernameyourdomain.com. For example, a consumer named "Joe" could have a DB-Federation-ID "Joedigitalbits.io", wherein "Joe" is his username and "digitalbits.io" is the domain name. The username could also be an email id. The domain can be any valid RFC 1035 [32] domain name. The Apps or clients automatically perform the federation lookup (DB-Account-ID $->$ DB-Federation-ID), or reverse-lookup (DB-Federation-ID $->$ DB-Account-ID)

and thereby allow the users to perform transactions by making use of just the DB-Federation-ID.

4.2.3 Compliance Server

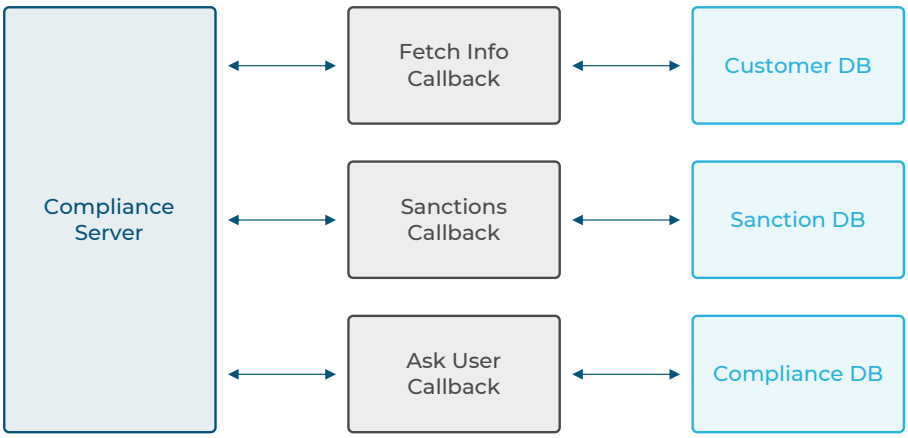


Fig. 13: Callbacks performed by the compliance server to the various databases at the sender as well as receiver side in order to obtain the necessary information to perform a compliance verification.

It is the responsibility of the anchor to handle regulatory compliance, especially to adhere to Anti-Money Laundering (AML) regulations. Complying with AML laws requires certaion enterprises and institutions (EIs) to know not only who their customers are sending value to, but also who their customers are receiving value from. However, in some jurisdictions certain EIs are able to trust the AML procedures of other EIs. In other jurisdictions each EIs must do its own background check of both the sender and the receiver. The DigitalBits compliance protocol supports the exchange of compliance information to pre-approve a transaction with another EI. The customer information that is exchanged between EIs via the compliance protocol is quite flexible and typically consists of the full name, date of birth and physical address.

Figure 13 illustrates the callbacks that are used to obtain information at the sender side and also to verify compliance in case a sender's compliance server contacts a receiver's compliance server to verify compliance before clearing a transaction. The following callbacks are performed:

- **Fetch_info callback:** This callback returns all the information about a particular consumer on receiving the consumer's federation address.
- **sanctions callback:** This callback is used to identify if any sanctions exist in order to receive money from the sender. The HTTP response code it

produces indicates whether the payment is accepted (status 200), denied (status 403), or if additional time for processing is required (status 202).

- **Ask_user callback:** This callback is called in case a sender has requested information about the receiver. The HTTP response code it produces indicates whether the information can be sent. If the callback is a success, the *fetch_info* callback is called to obtain the information.

4.2.4 Wallets and Apps

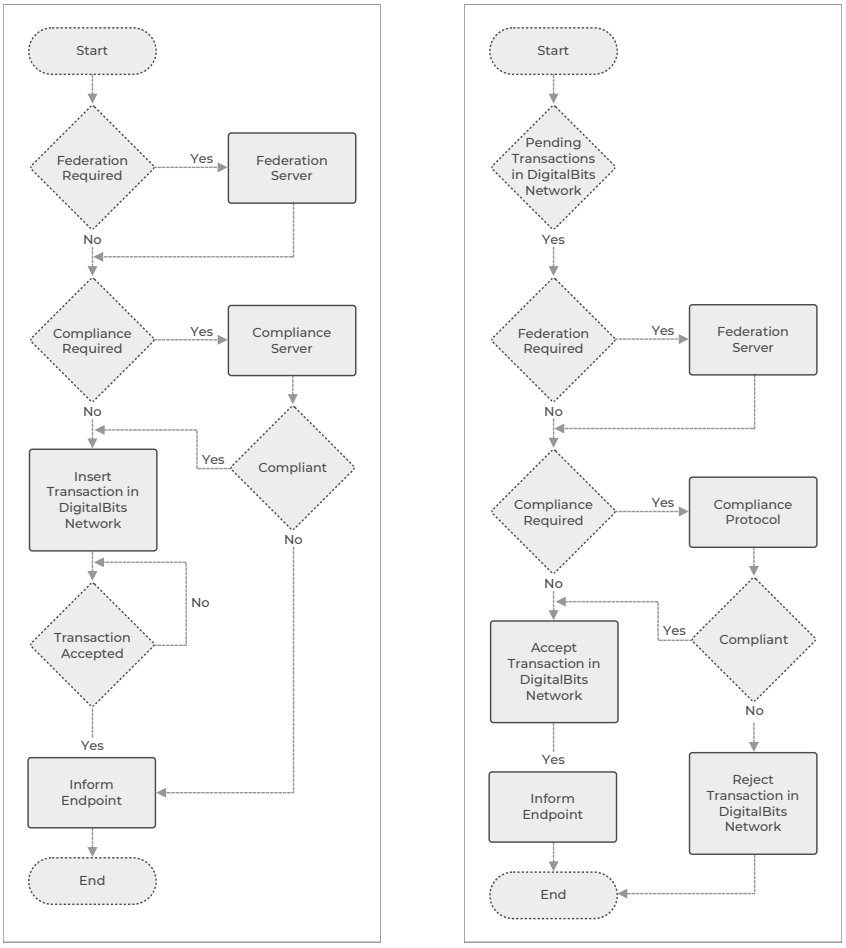
Businesses and third-party developers could easily develop custom Apps by leveraging the Frontier API and DigitalBits SDK. DigitalBits also provides a native XDB wallet source code that can be directly used or easily adapted to create a brand specific wallet. The bridge server facilitates easy access for the end points to the federation and compliance server.

4.3 System Architecture

Figure 14a presents a flowchart depicting the decision making process of a bridge server when it receives a request for a new transfer. The bridge server would contact the federation server of the receiver in case a mapping from a DB-Account-Id to a DB-Federation-Id for the receiver is required. It then verifies whether compliance is required for the transaction to be validated. If compliance is required, the bridge server contacts the compliance server to initiate the compliance protocol. The bridge server then places the transaction as a pending transaction in the DigitalBits network. Once the receiver accepts the transaction (see Figure 14b), the bridge server informs its endpoint. The endpoint then modifies its account balances accordingly.

Figure 14b presents a flowchart depicting the decision making process of a bridge server on the receiver side. The bridge server continuously monitors the DigitalBits network for any new pending transactions destined towards it. On observing such a transaction, the bridge server contacts the federation server of the sender in case a mapping from a DB-Account-Id to a DB-Federation-Id for the sender is required. It then verifies whether compliance is required for the transaction to be validated. If compliance is required, the bridge server contacts the compliance server to verify if compliance was already obtained. Accordingly, the bridge server either accepts or rejects the transaction in the DigitalBits network. If the transaction was positively verified and accepted, the receiver endpoint modify its account balances accordingly.

(a).pdf (b).pdf



(a) Bridge Server at the sender side (b) Bridge Server at the receiver side

Fig. 14: Flowcharts depicting the decision making process of a bridge server on receiving a request for sending or receiving tokens.

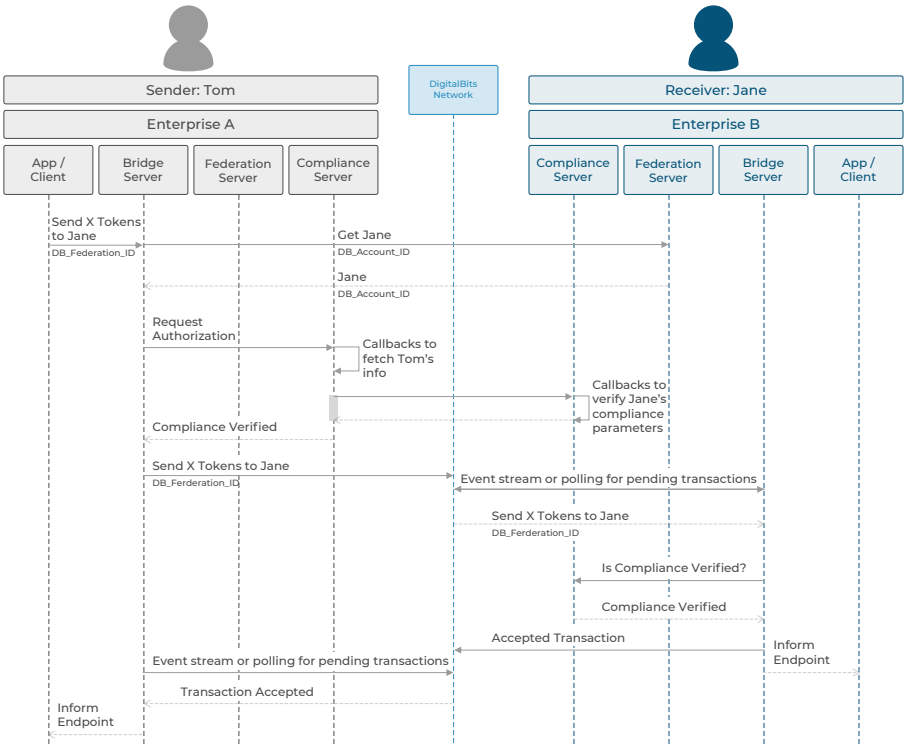


Fig. 15: A sequence diagram to describe how a sender (Tom) sends tokens to a receiver (Jane).

Figure 15 presents an overview of the processes at both the sender and the receiver side to perform a transfer. Let us assume that Tom wants to transfer tokens to Jane. Tom's App contacts its bridge server in order to initiate the transfer. The bridge server then contact the receiver's federation server to obtain Jane's DB-Account-ID. Afterwards it requests authorization from its compliance server. The compliance server makes use of the DigitalBits compliance protocol to clear the transaction with the recipients compliance server and accordingly informs its bridge server. The bridge server places this transaction in the DigitalBits network and wait for the transaction to be accepted. Meanwhile, the bridge server on the receiver side observes this pending transfer via a periodic polling mechanism. Jane's bridge server verifies with its compliance server whether compliance verification has been performed for the transaction. Accordingly, the bridge server accepts or rejects the pending transfer on the DigitalBits network. Both Tom's and Jane's bridge servers inform their respective endpoints of the validity of the transaction.

5 Stakeholders Engagement and Services Interaction

DigitalBits blockchain powered infrastructure builds a bridge that facilitates the implementation of new technologies to support and enhance our every day life interactions as well as foster blockchain mass adoption. Hence, stakeholder engagements and service interactions are essential to the DigitalBits platform. The underlying processes that enable engagement and interaction are the result of collaborating tasks and sub-processes. Based on the chosen LRP program running case from Section 2, we outline the exemplary detailed processes and benefits of involved stakeholder, e.g, for tokenizing assets, trading assets as well as validating and authenticating tokenized assets via certification service.

Consequently, Section 5.1 details the on-boarding process of digital assets, followed by Section 5.2 that details the digital asset validation and authentication service. Afterwards, Section 5.3 outlines the built-in decentralized multi-hop exchange of DigitalBits, followed by Section 5.4 that covers the token value proposition. Finally, Section 5.5 focuses on incentives that foster the DigitalBits community.

5.1 On-Boarding Process of Digital Assets

In previous sections we briefly outlined the general workflow of tokenizing an asset on the DigitalBits blockchain. Even though this paper focuses specifically on the tokenization of LRP programs, the underlying concept is more diverse and can be applied to commodities such as diamonds [37] and gold [2], or securities [24]. In general, tokenization is a method that converts the rights to an asset into a digital token that resides on a blockchain [8][21] and DigitalBits supports the tokenization of all types of assets.

In the context of our LRP program running case, we may face two different scenarios when it comes to tokenizing those programs. First, the asset provider (or issuer) wants to set up a brand new program without any legacy dependencies. Second, the assets provider already has an existing legacy (non-blockchain) LRP program that has to be migrated into the DigitalBits system. While the first case is rather straight forward, the second case is more complex.

In either case, the asset provider (or issuer) is to choose an identification code for the new asset - a combination of up to 12 letters or numbers that identify the asset in a human-readable form. Afterwards, the asset is ready to be used on the network. However, before other users are able to receive the loyalty tokens of fictional HotelBrand company from the running case of Section 2.2, the users have to choose to trust it (or the fictional company may do this in batch for all its users, if it is electing to initially hold custody of its members' accounts), since a DigitalBits asset is actually a credit. Therefore, users have to trust that HotelBrand can redeem that credit if necessary later on. In the context of a LRP program, the user usually trusts the asset provider, e.g., a retail company. Each account can create a trustline, or a declaration that it trusts a particular asset. In addition, users can also limit the trust to a particular amount of tokens. This security feature ensures that small asset providers with limited credibility do not

hand out excessive amounts of tokens. In the context of our running case, such details will be dealt with when a new user decided to join the loyalty program. By default, users have to trust the issuer to participate in the program.

The loyalty and reward industry uses so called reward engines to manage the mapping between purchases and allocated reward points (e.g., staying in a hotel for five nights results in a reward of 25 loyalty points). Those mappings as well as the terms and conditions that apply when redeeming the points are managed by the reward engine and the assets' providers IT system. As mentioned previously in Section 4, the asset providers bridge server facilitates the interactions between the DigitalBits network and the application-services on the asset provider side.

Finally, going back to the second scenario - that we outlined in the beginning of this section - assuming that HotelBrand wishes to migrate its existing program to the DigitalBits infrastructure. The workflow is mainly the same; a new asset is initially created on the blockchain and then the respective trust settings are performed. However, further application logic on the provider side is necessary to manage the migration process from the legacy platform to the blockchain solution. There are three approaches to that issue: First, HotelBrand may create accounts (consisting of public and private keys) for each legacy user and equips the corresponding accounts with a number of tokens that is equal to the number of loyalty points in the legacy system. The issuer can then create the keys and manage those accounts directly via the DigitalBits SDK, or the frontier server. A second solution could rely on the loyalty program bridging their existing database via their bridge server to handle any on-chain actions. In this case, the LRP program continues to rely on the existing accounting database of the legacy system while handling blockchain events via the bridge server, e.g., send and receive tokens. Finally, the third option is that in order to issue a new blockchain-based loyalty and reward tokens to customers with legacy tokens, these customers need to register with a DigitalBits account ID (as presented earlier in Section 4). As soon as an account has been registered, the issuer transfers tokens equivalent, or proportional to the points that the customer possessed in the legacy program. The migration process may consist of different stages, e.g., early access program, proof-of-concept and cut-over. Point-holders that wish to further use their accumulated points have to migrate before the cut-over in order to ensure that they do not loose their points.

5.2 Token Name Certification Service (TNCS) - Validation and Authentication of Asset Providers

In the previous section we elaborated on the process of on-boarding a new asset to the blockchain and tokenizing the asset. However, whether a specific tokenized asset actually represents the analogue asset of the real world is unclear. Ensuring a binding of the analogue value and its digital representation is a common problem in computer science and most thoroughly studied in the context of digital identities, e.g., [1][33]. How can Jane digitally prove to Tom that she is fact the owner as well as analogue representative of a specific digital identity? An equivalent problem, even though less complex than the human identity issue, arises

in the context of certificates for websites [16]. Most common solution for website certificates and digital identities are so called public key infrastructures (PKIs) that are either organized in a centralized and hierarchical manner (so called certificate authorities - CAs), or in a decentralized manner such as the PGP Web of Trust [49]. Both concepts have different advantages and disadvantages that have been partially solved by moving the underlying ideas to a blockchain-based platform [10][27][44].

In order to prevent malicious entities from issuing tokens that represent a brand or company that they are not associated with, we suggest a so called Token Name Certification Service (TNCS) be developed for validation and authentication of asset providers. Service providers within the DigitalBits network might then offer services similar to SSL certificate authorities that maintain a mapping between token smart contract addresses and the identities of token issuers. As a result, it becomes difficult for a malicious attacker to impersonate a legitimate company or issuer and issue a counterfeit asset on their behalf. The advantage for users and consumers is, that they do not have to worry about buying/trading worthless counterfeit tokens that have the same name as the original, but a different token address. Hence, it fosters security and convenience for users. A blockchain-based protocol that was designed to provide such services is the

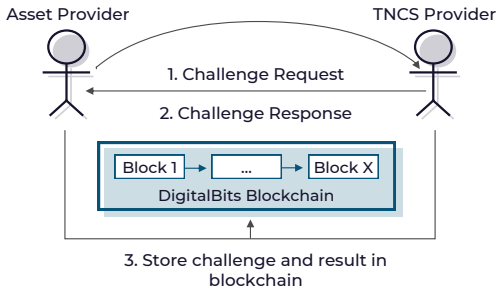


Fig. 16: Challenge response-based validation and authentication process on a blockchain (Adapted from [27]).

Authcoin protocol [26][27][28] that can easily be adapted to enable the TNCS on the DigitalBits network. The protocol provides validation and authentication for secure identity assurance on the blockchain via a challenge-response mechanism. In general, validation aims to prove that an entity has access to a certain resource (in our case access to a DigitalBits account that issued a specific token), while authentication continues the validation procedure by verifying the identity of the issuer and aims to confirm that the entity with access to the account is also the actual representative of the company. Figure 16 illustrates the idea in the context of DigitalBits TNCS. An asset provider (token issuer) wants the TNCS provider to approve the authenticity of their digital assets. To do so, the issuer requests

a challenge that is then created by the TNCS provider. Afterwards, the issuer fulfils the challenge and sends the response back. Challenge as well as response are transparently stored in the blockchain. The chosen challenge depends on the use-case scenario, the required level of security and the given threat level of the involved entities. In the context of a LRP program provider the challenge might ask the issuer to provide a company statement that proves that they issued the token and that they are in fact the company they claim to be.

5.3 Decentralized Multi-Hop Exchange

Besides the tokenization and transfer of digital assets such as LRPs, it also enables seamless transfer or trade of those assets on-chain with others entities interested in receiving those assets. This helps to solve many of the existing issues of non-tokenized assets that often suffer from missing market liquidity. In some cases, it is possible to seamlessly trade these assets even if no direct market exists between two assets. As a Stellar [31] fork, this decentralized multi-hop exchange works similar to the original.

5.3.1 Matchmaking

Users interested in trading LRPs or any other asset can create an offer to buy or sell an asset. In order to make an offer, the account must hold the asset it wants to sell. Moreover, the user is required to trust the issuer of the asset it is trying to purchase. When an account creates an offer, the offer is checked against the existing orderbook for that asset pair. If the offer crosses an existing offer, it is filled at the price of the existing offer. If not, the offer is saved in the orderbook until it is either taken by another offer, taken by a payment, canceled by the account that created the offer, or invalidated because the account making the offer no longer has the asset for sale.

5.3.2 Cross-Asset Multi-Hop Payments

Let us assume that Jane owns points from Company A and wants to buy an item or a service from a merchant that only accepts points from Company B. In this scenario, Jane can create a payment in Digitalbits that automatically converts her points from Company A into points of Company B by querying the orderbook and converting among the points at the best available rate. In case the orderbook does not contain any offers for such a conversion, it is also possible to first convert it into another asset, e.g., points from Company C, and afterwards converting those points to the target asset class. The number of intermediate steps before the final conversion is limited to a maximum of 6 hops and atomic[7].

Since cross-asset payments and conversions are simple and seamlessly, users are not required to hold any unwanted assets just for payment purposes. Instead,

[7] It will either succeed or fail and the payment sender will never be left holding an unwanted asset.

they keep their preferred LRPs of their favorite brand (or any other asset), only converting them if necessary. As a result, the DigitalBits system can offer and ensure liquidity in previously illiquid markets, thereby enabling a world where users never have to exchange currency except at the point of sale. Moreover, users could choose to keep all their assets in, for example stocks, only cashing out small amounts as they need to pay for things.

5.4 Token Value Proposition

While previous sections focused on the architecture, services and processes of the DigitalBits blockchain and ecosystem, the following section details the value proposition of its native token - the XDB token. XDB serves three main objectives: Firstly, as a protective security feature. Each account on the DigitalBits blockchain is required to stake a minimum of 10 XDB tokens to ensure an account is authentic and for the *send*-function to be enabled on the network. For example, if Jane wants to send 20 Tokens to Tom, her account must have a minimum of 30 Tokens to do so. Moreover, each transaction results in a minor transaction fee of 0.00001 XDB. Both requirements serve as protective security features and prevent users with malicious intentions from flooding the network. Secondly, XDB enables transaction among non-native tokens, by acting as a bridge to facilitate trades between pairs of other digital assets, which may not have a large direct market. Finally, DigitalBits XDB token can also be used for fast and low-cost micro-payments and remittances.

5.5 Community Engagement

The DigitalBits platform and the surrounding ecosystem aim to support mass adoption of blockchain technology. Hence, a community of various partners and users is crucial for the further development of DigitalBits. The following section introduces plans for token allocations, scholarships, grants and donations that will facilitate the community engagement of the DigitalBits ecosystem.

As illustrated in Figure 17, at the launch of the network, 32% of the XDB tokens will be reserved for an initial token sale and any that are unsold we will reserved for future use. 53% of the XDB tokens will be reserved for rewards to users, grants, airdrops and donations to charity. Lastly, another 15% are held by Fusechain Group Ltd. and its subsidiary, the founding contributor to the DigitalBits network, reserved for the Team and advisors. The initial allocation of 40.0% designated for rewards to users as well as donations to charities is separated into two pools: The DigitalBits Algorithmic Pool (39.60%) and the Charity Pool (0.40%). The XDB reserved for the DigitalBits Algorithmic Pool (DBAP) is designated for give away based on DigitalBits blockchain use and determined by DBAP's algorithms and system currently under development. This DBAP pool will be restricted and remain in reserve until this development is complete. Transaction fees are also used to refill the pool. XDB within the DBAP is released directly to users via their respective accounts on the blockchain when the rewards are earned.

40.0%	Algorithmic Pool (39.6%) and Charity Pool (0.40%). Restricted until algo launch within 24months.
5.0% 5.0%	Distributed via partnership development program, specifically driving benefit to DigitalBits; Distributed via R&D grants;
3.0%	Distributed via airdrops and bounties;
15.0%	12.5% distributed to founders, team, and contractors and 2.5% to advisors ("Team")
32.0%	Up to 32% to be sold in a token sale and the balance to be held for future use.

Fig. 17: XDB Token distribution at the launch of the DigitalBits network.

Donations from the Charity Pool are given to designated charities at a ratio of 1-to-99 with the DBAP, until the Charity Pool supply is exhausted. For example, if 990 XDB are released by the DBAP, then 10 XDB are released from the Charity Pool. The Foundation plans to identify, designate and monitor charities to be recipients of the XDB released from the Charity Pool. The Charity Pool will restricted and remain in reserve until the DBAP system is developed.

Finally, we plan to give away a 5% allocation through the DigitalBits Research and Development Grant Program and 5% Partner Ecosystem Development Program from time to time. The Partner Grant Program and Partner Ecosystem Development Program are focused on encouraging prospective partners to develop and operate products, services, or solutions that are important to the DigitalBits network.

6 Conclusion

This whitepaper presents the DigitalBits blockchain powered infrastructure that facilitates the implementation of new technologies to support and enhance our every day life interactions as well as foster the mass adoption of blockchain. Moreover, our solution facilitates easy asset-tokenization using a transaction and trading layer for the point-to-point economy.

Based on the use cases and scenarios, we identify the requirements and criteria that the DigitalBits blockchain infrastructure must satisfy. With respect to functional and non-functional requirements, the DigitalBits network has to be easy to use, flexible and convenient in order to reach the goal of mass-adoption. Furthermore, interoperability and scalability as well as security and compliance are further mandatory properties of our solution. Moreover, easy integration

into other services and a plugin interface for external applications are essential to DigitalBits.

Subsequently, we derive and outline the DigitalBits network and system architecture based on the identified requirements and goals. We present the overall architecture and detail on the key network components that enable the DigitalBits platform. Moreover, we outline the communication interfaces, the network topology and describe the interplay of services and entities within the network. In order to ensure widespread adoption, DigitalBits offers a variety of SDKs and easy to use APIs for developers, partners and the community.

Next, we deal with the exemplary stakeholder engagement and service interaction processes that are essential to the DigitalBits platform. First, the onboarding process of digital assets and the asset tokenization which is an indispensable functionality of our platform. Afterwards, present the novel idea of the token name certification service (TNCS) that prevents malicious network entities from issuing and distributing illegitimate tokens of assets that they are not associated with. In order to trade and exchange tokenized assets in a proper manner, DigitalBits provides a built-in decentralized multi-hop exchange for cross-asset payments. Finally, we present the XDB token value proposition and the surrounding token economy ecosystem that fuels the DigitalBits platform.

References

1. Alsarkal, Y., Zhang, N., Zhou, Y.: Linking Virtual and Real-World Identities. In: Intelligence and Security Informatics (ISI), 2015 IEEE International Conference on. pp. 49–54. IEEE (2015)
2. Aurus.io: Aurus: Tokenized Physical Assets - Whitepaper. URL: `https://aurus.io/wp-content/uploads/2018/08/Aurus-Whitepaper-V2.1.pdf` (2018), (Accessed August 29, 2018)
3. Barnett, C.: Inside the Meteoric Rise of ICOs. URL: `https://www.forbes.com/sites/chancebarnett/2017/09/23/inside-the-meteoric-rise-of-icos/#f5de0bf5670c` (2017), (Accessed September 01, 2018)
4. Barry, N., Losa, G., Mazieres, D., McCaleb, J., Polu, S.: The Stellar Consensus Protocol (SCP) (2015), (Accessed September 02, 2018)
5. Berry, J.: The 2015 COLLOQUY Loyalty Census: Big Numbers, Big hurdles. URL: `https://www.colloquy.com/latest-news/2015-colloquy-loyalty-census/` (2015), (Accessed August 17, 2018)
6. Bond Brand Loyalty: The Loyalty Report 2017. URL: `http://info.bondbrandloyalty.com/2017-loyalty-report` (2017), (Accessed August 15, 2018)
7. Brian Patrick Eha, American Banker: How Barclays Aims to Bring a Billion Unbanked into the Fold. URL: `https://www.americanbanker.com/news/how-barclays-aims-to-bring-a-billion-unbanked-into-the-fold` (2016), (Accessed August 17, 2018)
8. Cameron-Huff, A.: How Tokenization Is Putting Real-World Assets on Blockchains (2017), (Accessed August 29, 2018)
9. Castro, M., Liskov, B., et al.: Practical byzantine fault tolerance. In: OSDI. vol. 99, pp. 173–186 (1999)

10. Civic Technologies, Inc.: CIVIC - Whitepaper. URL: https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf (2017), (Accessed August 29, 2018)
11. COLLOQUY: 2015 COLLOQUY Loyalty Census Report. URL: https://www.colloquy.com/reports/ (2015), (Accessed August 14, 2018)
12. COLLOQUY: 2017 COLLOQUY Loyalty Census Report - An In-depth Analysis of Where Loyalty Is Now ... and Where It's Headed. URL: https://www.colloquy.com/reports/ (2017), (Accessed August 14, 2018)
13. Davis, A.M.: Software Requirements: Objects, Functions, and States. Prentice-Hall, Inc. (1993)
14. Deloitte: The Deloitte Consumer Review - Customer Loyalty: A Relationship not just a Scheme. URL: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-customer-loyalty.pdf (2017), (Accessed August 15, 2018)
15. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory 31(4), 469–472 (1985)
16. Ellison, C., Schneier, B.: Ten Risks of PKI: What you're not Being Told About Public Key Infrastructure. Comput Security Journal 16(1), 1–7 (2000)
17. Encyclopedia.com: Gold Standard. URL: https://www.encyclopedia.com/social-sciences-and-law/economics-business-and-labor/money-banking-and-investment/gold-standard, (Accessed August 17, 2018)
18. Experian: Driving customer loyalty - Maximize loyalty program data collection to drive insight and revenue. URL: http://cdn.qas.com/us-marketing/whitepapers/driving-customer-loyalty.pdf (2014), (Accessed August 15, 2018)
19. Fruend, M.: The 2017 COLLOQUY Loyalty Census. URL: https://www.colloquy.com/latest-news/u-s-customer-loyalty-program-memberships-reach-double-digit-growth-at-3-8-billion-2017-colloquy-loyalty-census-reports/ (2017), (Accessed August 17, 2018)
20. Gordon, N., Hlavinka, K.: The 2011 Forecast of U.S. Consumer Loyalty Program Points Value. URL: http://www.swiftexchange.com/Content/Documents/2011-COLLOQUY-Liability-Talk-White-Paper.pdf (2011), (Accessed August 14, 2018)
21. Hargrave, J., Sahdev, N.K., Feldmeier, O.: How Value is Created in Tokenized Assets (2018), (Accessed August 29, 2018)
22. IEEE Computer Society. Software Engineering Technology Committee and Institute of Electrical and Electronics Engineers: IEEE Recommended Practice for Software Requirements Specifications. IEEE Std, Institute of Electrical and Electronics Engineers (1994)
23. Ivanov, S.: WAVES Platform - Whitepaper. URL: https://wavesplatform.com/files/images/whitepaper_v0.pdf, (Accessed August 26, 2018)
24. Koverko, T., Housser, C.: Polymath: The Securities Token Platform - Whitepaper. URL: https://polymath.network/whitepaper.html (2018), (Accessed August 29, 2018)
25. L. M. Goodman: Tezos - A Self-Amending Crypto-Ledger (White paper). URL: https://www.tezos.com/static/papers/white_paper.pdf (2014), (Accessed August 20, 2018)
26. Leiding, B.: Securing the Authcoin Protocol Using Security Risk-oriented Patterns
27. Leiding, B., Cap, C.H., Mundt, T., Rashidibajgan, S.: Authcoin: Validation and Authentication in Decentralized Networks. In: The 10th Mediterranean Conference on Information Systems - MCIS 2016. Cyprus, CY (September 2016)

28. Leiding, B., Norta, A.: Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance. In: International Conference on Future Data and Security Engineering. pp. 181–196. Springer (2017)
29. Liu, Y.: The Long-Term Impact of Loyalty Programs on Consumer Purchase Behavior and Loyalty. Journal of marketing 71(4), 19–35 (2007)
30. Marshall, J.: Agent-Based Modelling of Emotional Goals in Digital Media Design Projects. International Journal of People-Oriented Programming (IJPOP) 3(1), 44–59 (2014)
31. Mazieres, D.: The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus - Whitepaper. URL: https://www.stellar.org/papers/stellar-consensus-protocol.pdf (2016), (Accessed August 26, 2018)
32. Mockapetris, P.: Domain names - implementation and specification. URL: http://tools.ietf.org/rfc/rfc1035.txt (November 1987), (Accessed August 29, 2018)
33. Mordini, E., Massari, S.: Body, Biometrics and Identity. Bioethics 22(9), 488–498 (2008)
34. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf (2008), (Accessed August 01, 2018)
35. Norta, A.: Exploring Dynamic Inter-Organizational BusinessProcess Collaboration: Privacy Protecting Concepts for ChoreographingeSourcing in B2B with Service-Oriented Computing. VDM Verlag (2008)
36. Norta, A., Grefen, P., Narendra, N.C.: A Reference Architecture for Managing Dynamic Inter-Organizational Business Processes. Data & Knowledge Engineering 91, 52–89 (2014)
37. Norta, A., Levi, S., Priewer, R., Kif, E.: CEDEX: Certified Blockchain Based Diamond Exchange - Whitepaper. URL: https://cedex.com/img/Whitepaper.pdf (2017), (Accessed August 29, 2018)
38. Owyang, J., Groopman, J., Szymanski, J., Rebecca, L.: Analysis: Should Blockchain Power Your Customer Loyalty Program? URL: http://www.web-strategist.com/blog/2018/03/09/analysis-should-blockchain-power-your-customer-loyalty-program/ (2018), (Accessed August 13, 2018)
39. Popov, S.: The Tangle - Version 1.4.2. URL: https://iota.org/IOTA_Whitepaper.pdf (2018), (Accessed August 22, 2018)
40. Qiibee Foundation: Qiibee: Loyalty on The Blockchain - Whitepaper 2.4. URL: https://static.qiibee.com/qiibee-White-Paper.pdf (2018), (Accessed August 17, 2018)
41. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(2), 120–126 (1978)
42. Robinson, S.: The 2013 Maritz Loyalty Report. URL: https://nrf.com/resources/retail-library/the-2013-maritz-loyalty-report-benchmarks-trends-and-lessons-brand-loyalty (2013), (Accessed August 17, 2018)
43. Russolillo, S.: Initial Coin Offerings Surge Past $4 Billionand Regulators Are Worried. URL: https://www.wsj.com/articles/initial-coin-offerings-surge-past-4-billionand-regulators-are-worried-1513235196 (2017), (Accessed September 01, 2018)
44. SelfKey Foundation: SelfKey - Whitepaper. URL: https://selfkey.org/whitepaper/ (2017), (Accessed August 30, 2018)
45. Stellar Development Foundation: Stellar Basics - Website. URL: https://www.stellar.org/how-it-works/stellar-basics/, (Accessed August 17, 2018)
46. Sterling, L., Taveter, K.: The Art of Agent-Oriented Modeling. MIT Press (2009)

47. Synchrony Financial and Reuters Content Solutions: Much Love for Loyalty Programs. URL: https://www.reuters.com/brandfeatures/synchrony/inside-retail/much-love-for-loyalty-programs (2015), (Accessed August 17, 2018)
48. Wood, G.: Ethereum: A Secure Decrentralized Generalised Transaction Ledger. URL: http://gavwood.com/paper.pdf (2014), (Accessed August 01, 2018)
49. Zimmerman, P.: PGP 2.X Manual. URL: https://web.pa.msu.edu/reference/pgpdoc1.html (1994), (Accessed August 30, 2018)

Disclaimer

It is forecasted that it will take over 10 years to exhaust the reserves within the DigitalBits Algorithmic Pool and Charity Pool. However, this is subject to several factors, including demand and the algorithms that will be integrated into the DigitalBits Algorithmic Pool. Therefore, this timeline cannot be guaranteed and forecasts may fluctuate from time to time.

This whitepaper is for information purposes only. DigitalBits Foundation does not guarantee the accuracy of or the conclusions reached in this whitepaper, and this whitepaper is provided as is. DigitalBits Foundation does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including, but not limited to: (i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or non-infringement; (ii) that the contents of this whitepaper are free from error; and (iii) that such contents will not infringe third-party rights. DigitalBits Foundation and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this whitepaper or any of the content contained herein, even if advised of the possibility of such damages. In no event will DigitalBits Foundation or its affiliates be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference to, or reliance on this whitepaper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses.