UDC: A Digital Currency for Unifying Global Commerce

Rafael Afonso Rodrigues

rafaelafonsorodrigues@gmail.com

Abstract. The proposal of a new mainstream digital currency oriented for local and global commerce called Unified Digital Currency ("UDC") is presented. UDC is a decentralized and distributed cryptocurrency without pre-minted monetary base, oversighted by a central bank ("WorldBank") and pegged to the most prominent fiat currencies. The digital currency is governed by accounts, cryptographically protected, and transactions executed between them, organized by a chain of Ledgers designed for reviewing the state of the currency and safeguarding all past information associated. Transactions can range from simple transfers to complex events defined by third-party Decentralized Autonomous Organizations ("DAO") and Distributed Automatic Services ("DAS"). In turn, UDC operates in a multi-level network composed by a multitude of participants with different roles and functions, each owned by independent third-parties that ensure a diversified decentralization, all of which follow the common protocols and consensus built upon existing cryptographic methods proven secure. A separate blockchain, Network Management Blockchain, is introduced to deal with the organization of the network, the currency and create initial trust. Based on what is proposed, emerges the foundations for a new digital financial ecosystem, more easily accessible by the world's internet users.

Keywords: UDC · cryptocurrency · Ledgers · smart contracts · DAO · Distributed Automatic Services · central bank · Network Management Blockchain

1 Introduction

In the wake of the modern digital currencies, popularly called cryptocurrencies, led by Bitcoin, created in 2008, and its numerous copies, "altcoins", arose the need for one

Paper version 1.0
October 2016, Belgium

that is not only more trustable and monetarily stable, but also faster and less computationally hungry. Allowing for concrete and useful applications, both locally and globally, and truly replace conventional forms of currency.

1.1 Existing Issues

The most common problems that emerge from those cryptocurrencies are their complexity from the perspective of an average person, from the incomprehensible addresses to the acquisition of currency, sometimes regarded as an obscure process or even borderline legal. The lack of a diverse ecosystem with applications and services of high quality, which is often both cause and effect of the limitations observed of a currency's use, where its sole employments are either value speculation, gambling or black market activities. Granted, the judgement bearing this problem, questions only the lack of diversity and not its content, which are beyond scope and should be is irrelevant to a truly open currency. Even more when its network is only there to validate transaction and incompetent to analyze the nature of those transactions, leaving it to each's own discretion.

Other problems exist within the currencies themselves. Be it the pre-minted monetary base, indiscriminately owned by their founders or some few lucky investors, who them cash in on pre-sales or early buy-outs; the mining rewards and transaction fees, which are rapidly hoarded by whomever comes first and has the most computational power. Of course, those incentives help grow the currencies and their networks, however they are still unfair advantages and dominance given to a small group, who will generate wealth only because of the arrival of newcomers. Coupled with this, power shifts or desires to control a currency by an organization emerges, a recent example was seen with Bitcoin during the conflict between the Bitcoin Core developers and the Bitcoin Classic group, which was backed by important miners. The conflict arose mid-2016 when deciding which route to follow for the currency's future and from it appeared the possibility of the currency being forked into two new currencies. It does show the risk of having small groups each with opposed views, interests and ideas, with sizeable amounts influence and control over a currency nearing $10B of market capitalization. How can a participant, regardless of its stake in the currency, have faith and trust over its long-term existence and value in those conditions? Even aside the risk of having a select few capable of altering the software used to run the currency's network, there's still the theoretical risk of some agglomerate owning the majority of the network or computational power and taking over the whole currency. And then, there's also the possibility of having forks of the blockchain governing a currency, where portions of the network create and follow different blocks, those problems are eventually detected and corrected but only after a couple of blocks. Even worse is the ulterior rollback and alteration of a blockchain, called hard fork, defeating the purpose of using such mechanism and destroying the credibility and trust put onto such cryptocurrency. An event that happened recently with a then promising cryptocurrency, Ethereum, which executed a hard fork in July 2016, in order to revert the execution of a smart contract and thus alter the balance of an address without using the private key supposedly protecting such address. Although it happened due to a flaw on The DAO smart contract, with

some researchers even warning about eventual risks before its launch, it was still the execution of the smart contract, whose code was publicly available before-hand, that allowed it and not some malicious attack or breach of the currency or network themselves. Furthermore, it invalidates the existential principle of immutability required by any trusted cryptocurrency.

Another point is the limitation of what a transaction can be, normally being only a monetary transfer from an address to one or more different addresses. Although, there are some exceptions, the most prominent being Ethereum, which allowed to appearance of more advanced transactions, dubbed smart contracts. It is, in my regard, an essential topic, as it allows for a versatile currency, where applications can be built on top of it and thus, lead to a faster growth and adoption of its ecosystem.

Finally, from a practical point-of-view, we have uncertainty and volatility of a currency's value; long confirmation times, relative to equivalent payment systems of fiat currencies, often with the necessity of waiting for additional blocks; and, difficulty of currency exchange. Notwithstanding the challenges inherent to using cryptocurrencies for the average person, these are all recurrent complications that should be addressed when designing a digital currency intended for worldwide adoption.

1.2 Proposal

Based upon those issues, the idea for a new digital currency that could resolve them, at least partially, and in a way capable of democratizing its use by anyone was formed. The conceived currency is translated into a solution which differs on a couple of key points with respect to existing proposals and exhibits some innovative features:

- It incorporates a central bank capable of issuing new currency or removing what it owns from circulation, guarantees currency exchanges, and who provides the groundworks for all initial operations and local partnerships.
- It is pegged to the ten most traded and important worldwide currencies, giving it an extrinsic value with low volatility, maintained by the central bank through the safekeeping of equivalent fiat reserves, instead of artificially through controlled sales and purchases at fixed prices.
- There is no pre-minted amount of currency nor limits, since it depends exclusively on the reserves infused into it, thus removing the unfairness towards newcomers.
- Short intelligible alphanumeric accounts, each permanently linked to a unique ECDSA[1] key pair, replace the lengthy hexadecimal addresses.
- Ranges of accounts can be independently managed, leased and reserved by third-parties either for internal or commercial activities.
- Chained Ledgers, which provide a complete overview of the state of the currency and keep track of all transactions processed during its span, replace the traditional blockchain.

[1] Elliptic Curve Digital Signature Algorithm

- Proof-of-Stake and Proof-of-Work methods are replaced by qualified majority consensus with auto-correcting mechanisms, which impede chain forks and reduce the ever-increasing computational requirements and energetic waste of the network.
- Validation protocols designed to reduce the processing of transactions to mere seconds, without requiring waiting for the Ledger they belong into to be closed nor awaiting multiple confirmations ahead when published.
- Decentralized and distributed multi-level network with ensured diversity through the attribution of network IDs associated with ECDSA key pairs enabling the authentication of all peers.
- Mining fees and block rewards are replaced with transaction, service and network fees, fairly and procedurally redistributed among the peers sustaining the network.
- Supports multiple types of transactions and additional third-party commercial services, based on event-oriented transactions and vetted by the community, can be offered by the network through protocol and software updates.
- Decentralized Autonomous Organizations ("DAO") provided by independent third-parties can be incorporated into the network and operate in concurrence to other existing services.
- A separate dedicated blockchain is established to manage the network itself, all of its components and participants, which also provides a base of trust necessary to operate a secure currency and independent network.

By having faster validation cycles, guaranteed currency trades and lower value variance; by being more user-friendly and capable of supporting smart contracts; It can rapidly expand its digital ecosystem by penetrating local commerce through facilitated integration and near real-time processing, and also supporting more complex and modern applications built on top of it. With the expectation of all of the above combined lead to an accelerated proliferation and adoption to eventually being able to reach ubiquity as a global exchange medium.

2 The Currency

2.1 Unified Digital Currency

Unified Digital Currency, referred to as UDC from here onwards, is the proposed currency. Its name originates from the aspiration to replace and consolidate the market share of the cryptocurrencies that came after Bitcoin.

Its main monetary unit is designated *Uni*, derived from the "Unified" part of UDC while also coinciding with the word universal, which represents one of its goals. As with most currencies, its monetary unit composed of a subunit, called *unicent*, in the ratio below:

$$1\ Uni = 100\ unicents \tag{1}$$

Its symbol, necessary for mainstream visual recognition, is a capital letter U, with a double strikethrough of its left half as depicted here through Figure 1.

Fig. 1. UDC monetary symbol

As stated before, UDC is pegged to a basket of 10 fiat currencies, all chosen for their international and economic importance. Using a simple formula, applied to all existing fiat currencies, the 10 currencies with the highest importance factor (I_{FAC}) were selected.

$$I_{FAC} = FOREX\ Share * (1 + Trade_W) \tag{2}$$

$$Trade_W = \frac{\sum(Exportations + Importations)}{\sum GDP}\ (in\ \$USD) \tag{3}$$

Where the FOREX Share is the currency's share in either buy-side or sell-side of the worldwide foreign currency exchanges, also referred to as its turnover. The currency's importance factor is then obtained by increasing this share by its trade weight ($Trade_w$). The trade weight is computed by calculating the total trade, exportations with importations, in percentage of the GDP, of all the countries officially covered by its central bank; where each national value is converted into United States Dollars of the same year as the data. Thus only the importance factor of the Euro is calculated using data from multiple countries, 19 currently.

The part of each fiat currency in UDC is then retrieved by calculating the proportion of their respective importance factor.

$$Porportion = \frac{I_{FAC}}{\sum I_{FAC}} \tag{4}$$

Based on the latest official data available, (2) was applied to all possible currencies. From there, the top 10 currencies, I_{FAC}-wise, were ten extracted and their respective proportions computed using (4). The results are shown in Table 1 and a visual representation of their distribution is provide in Figure 2. Together, those 10 currencies account for more than 90% of the global foreign exchange turnover, while their economies aggregate over 70% of the world's GDP and are responsible for almost 70% of the global trade of goods and services. They are therefore representative enough of the global commerce and thus an appropriate basket for a digital currency wanting to unify them.

Appendix A depicts the datasets, with their sources, used to reach these results, although limited solely to the selected currencies, enough to corroborate the proportions obtained. The data being freely and publicly available, the results are easily verifiable by anyone wishing to confirm them. Specifically, for the national economic indicators, GDP, total exportations and total importations, the data was obtained from The World Bank Group, for the latest concluded year, 2015. With relation to the foreign exchanges data, it was retrieved from the latest Triennial Central Bank Survey regarding foreign exchange turnover in April 2016, published by the Bank for International Settlements.

Having chosen the pegged currencies and computed their proportions, only their relation with UDC remains to be defined. Setting the exchange rate w.r.t the basket is an important point, since the concerned local economies are somewhat different, trying to reach for parity with an expensive currency can make UDC's value drift towards the living costs of the related region while seeming more disparate compared with the remaining ones. On the other end, a disproportionate rate will surely give the impression of it being a "cheap" currency, without any connection with the local realities and distant from what most people are used to, complicating the assimilation of its value with the habitual prices of goods and services applied.

Therefore, a tradeoff has to be made in order to reach a good rate. Which is why, after some deliberation and analysis, the rate presented in (5) was adopted.

Table 1. UDC pegged currencies (source: refer to Appendix A)

Currency Denomination	Currency Code	Proportion
United States Dollar	USD	41,44%
Euro	EUR	21,66%
Japanese Yen	JPY	10,91%
Pound Sterling	GBP	7,42%
Swiss Franc	CHF	3,81%
Australian Dollar	AUD	3,59%
Hong Kong Dollar	HKD	3,14%
Canadian Dollar	CAD	3,12%
Singapore Dollar	SGD	2,83%
Chinese Yuan Renminbi	CNY	2,09%

$$3\,Uni = \sum Proportion \tag{5}$$

$$\begin{aligned} 3\,Uni = {} & 0.4144USD + 0.2166EUR + 0.1091JPY + 0.0742GPB \\ & + 0.0381CHF + 0.0359AUD + 0.0314HKD \\ & + 0.0312CAD + 0.0283SGD + 0.0209CNY \end{aligned} \tag{6}$$

With (6), it is now possible to calculate the indirect exchange rate of UDC with each of the pegged currencies. Table 2 exemplifies such rates, extrapolated by using the fiat currencies' exchanges rates for the 1st October 2016, whose full data in depicted in Appendix B.

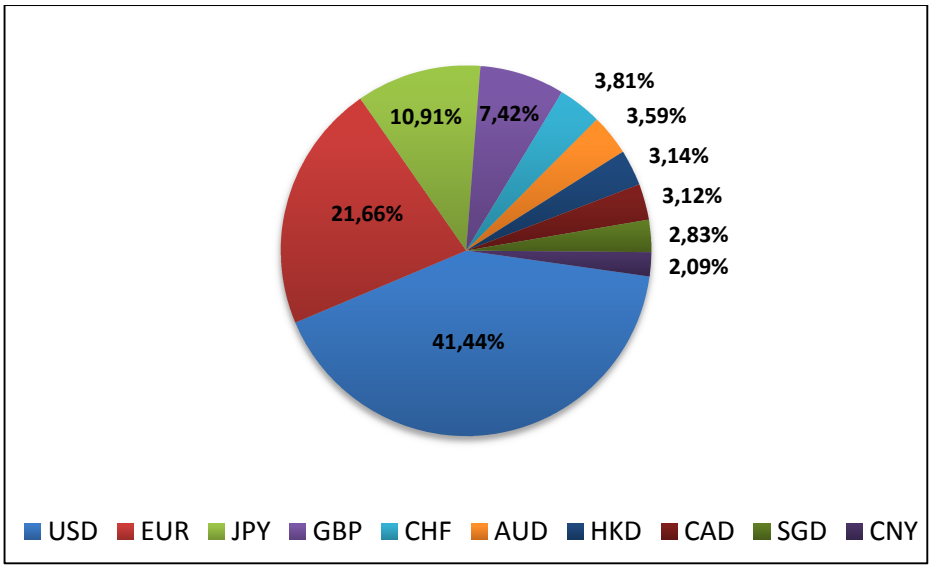

Fig. 2. UDC currencies distribution (data from Table 1)

Table 2. UDC exchange rates as of 1st October 2016 (source: refer to Appendix B)

Currency Denomination	Per 1 UDC	1 Per UDC
United States Dollar	1 Uni = 0,2912 USD	1 USD = 3,4345 Uni
Euro	1 Uni = 0,259 EUR	1 EUR = 3,8606 Uni
Japanese Yen	1 Uni = 29,5054 JPY	1 JPY = 0,0339 Uni
Pound Sterling	1 Uni = 0,2245 GBP	1 GBP = 4,4552 Uni
Swiss Franc	1 Uni = 0,2828 CHF	1 CHF = 3,5360 Uni
Australian Dollar	1 Uni = 0,3802 AUD	1 AUD = 2,6301 Uni
Hong Kong Dollar	1 Uni = 2,2584 HKD	1 HKD = 0,4428 Uni
Canadian Dollar	1 Uni = 0,3823 CAD	1 CAD = 2,6156 Uni
Singapore Dollar	1 Uni = 0,3969 SGD	1 SGD = 2,5194 Uni
Chinese Yuan Renminbi	1 Uni = 1,9426 CNY	1 CNY = 0,5148 Uni

2.2 Accounts

In UDC, the addresses, representing the ECDSA public keys, traditionally used in cryptocurrencies are replaced with account numbers resembling more what is usually used with the banking system.

Each account is a 10-character long easily identifiable alphanumeric key, composed of 3 uppercase letters, A to Z, and 7 digits, 0 to 9. With this format, there are 176,760,000,000 unique accounts, able to be used in UDC. An example of an account is portrayed in Figure 3.

Since their access and utilization has to be secure, each account is uniquely linked to an unchangeable ECDSA cryptographic public key, to be set when activated.

In order to provide sufficient level of protection, such key pair has to respect the network's cryptographic guidelines. For accounts, this means the ECDSA key pairs can only implement elliptic curves based on prime numbers and with key sizes of at least 256bits, guaranteeing cryptographic security on a medium to long term scale, at least until quantum computing becomes widespread and threatening enough, though by then, the network's security would already have evolved. Virtually all cryptocurrencies use a key size of 256bits, although even the most popular, Bitcoin, has only used less than 300 million unique addresses[2]. With multiple being mapped to the same ECDSA private key, which means that even accounting for the remaining cryptocurrencies, it is probable that not even 2^{30} (~1 billion) out of the possible 2^{256} have been used for those purposes. Therefore, the risk of collision, even excluding the larger key sizes, is insignificant.

Slots. In UDC, accounts are virtually regrouped into sequential ranges called Slots. Where each Slot is a 4-character long prefix of an account, representing all letters and the first digit, as exemplified in Figure 3. Slots are used to facilitate the activation of new accounts, and their allocation, management or reservation by third-party organizations, effectively dividing them into virtual zones within the currency's network. In total, there are 176.676 unique Slots, each containing 1 million account numbers.

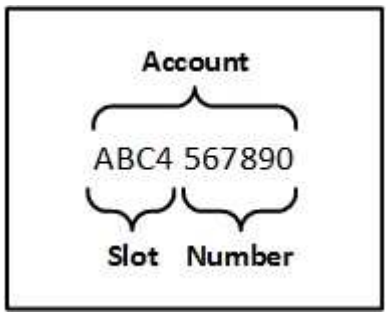

Fig. 3. Example of an account and its breakdown

2.3 WorldBank

Central Bank Role. WorldBank is the organization that will act as the foundation and the central bank of UDC, although with certain limitations. Its functions as the central bank are comprised of:

- Printing currency whenever a purchase of UDC with fiat currencies is made.
- Removing currency, owned or sent to it, from circulation whenever UDC is bought back using its fiat reserves.

[2] 293,459,622 unique addresses as of 5th October 2016, source: `https://blockchain.info/charts/n-unique-addresses`

- Safekeeping the monetary reserves of the pegged currencies and ensuring that they remain equivalent, at all times, to the total amount in circulation of UDC.
- Guaranteeing exchanges between UDC and any of the pegged currencies at the fixed exchange rate characterized in (6).

Hence, with the assertion of the value of UDC being always backed by equivalent reserves, it cannot employ interest-rates policies or any other procedure leading to the unwarranted issuance of new currency. As to ensure the, vital, trust and responsibility put on the WorldBank, creating or destroying currency is a complete transparent process, since it is accomplished through normal transactions, processed, validated, published and registered into Ledgers like any other transaction. However, they involve UDC's base account, "UDC0000000", controlled by the WorldBank, which is used exclusively for those two kinds of operations. When printing currency, the WorldBank emits a transaction stating this account as the sender. While destroying currency is simply a matter of submitting a transaction posing the base account as the receiver.

In order for the WorldBank to succeed in its exchanges guarantee, it will have the charge of seeking local partnerships and develop affiliations with banks or major financial services providers, as to provide a large range of trading options, with the objective of maximize the accessibility and convenience for the average user of UDC. First prioritizing all countries officially associated with the pegged currencies, and then, ultimately, all remaining countries.

Finally, besides having exclusive rights for the control of the monetary base, it also holds all privileges over any other digital or physical representation of UDC, thus being the only restriction put on third-parties involved with the currency.

Slots Role. The WorldBank cannot, and should not, control the activation of all accounts by itself. So, in order to accelerate the growth of the currency, yield its independence and decentralize the management part of the network, unallocated Slots can be attributed to independent organizations requesting them. These organizations can then fully manage the Slots, independently and as they see fit, offer services and build applications on top of the currency and reap benefits including transactions fees over accounts related to those Slots. In turn, they must follow certain essential guidelines, destined to protect the users, and have the obligation of providing nodes to help sustain and diversify the network. The WorldBank will also function as a litigation center to resolve disputes over Slots allocations and unethical or illegal managing practices, such as, but not limited to, lies, misrepresentation or disinformation about transactions fees.

The WorldBank also manages the official Slots, and has to comply with the same rules and obligations just like any other organization. The official Slots and their descriptions are represented in Table 3. Furthermore, some Slots are initially in a reserved state, it includes all those corresponding to the 3-letter country codes, as specified in ISO 3166-1 alpha-3, and those with the initials "GOV", GOV0 to GOV9. The reason is to allow an examination period to further study their usefulness and potential, and in determining the possibility of institutional uses by national governments or ad-

ministrations after the currency's launch. All the remaining ones are available for assignment, depending on the spread of the request, its targeted application and dedicated investment.

Table 3. UDC's official Slots

Slots	Description
UDC0 to UDC9	Used by the WorldBank for its internal and official operations, employees and direct clients
DAO0 to DAO9	Reserved for Decentralized Autonomous Organizations
DAS0 to DAS9	Reserved for Distributed Automatic Services

Community Role. For any digital currency to become mainstream and succeed, it requires a strong community, able to develop and propose new applications or features. One of the WorldBank's tasks will be to help initiate and oversee, if necessary, such community, creating a varied cooperation of developers, users and commercial partners. Together with this community, the WorldBank will be able to implement new functionalities, keep updated the currency and network protocols, vet third-party services, smart contracts and Decentralized Autonomous Organizations to be incorporated into and provide through the currency's network.

Network Role. One of the primary tasks of the WorldBank will be to set up, and maintain, a public key infrastructure (PKI) with a new self-signed root digital certificate. This PKI will allow to create a starting point for the security and integrity of the network and currency, without exposing it to risks of external pressures or malicious attacks perpetrated through weak or complicit Certificate Authorities (CAs). The WorldBank will use it to certify and authenticate internal operations, but also, provide certification services to any users, organizations, companies or services associated with UDC or its network. For this reason, intermediate CAs are to be created, each dealing with a limited subset of activities, with the intent of providing a structured and transparent system. Initially, 4 intermediate CAs will be made available:

- UDC WorldBank Intermediate CA - Internal: for WorldBank's internal operations;
- UDC WorldBank Intermediate CA - Commercial: for WorldBank's commercial activities and its clients;
- UDC WorldBank Intermediate CA - Network: for UDC network participants;
- UDC WorldBank Intermediate CA - Third-Party: for third-party applications and other non-UDC related certifications;

As stated before, to operate within the network, the WorldBank has also to provide computational resources in the form of nodes. However, unlike most existing cryptocurrencies where users can be part of the network by running a local node through their wallet program or any other multitude of heterogenic dedicated software, with UDC, the network operations are not intended to be supported by basic users. Although it removes the burden from those wishing only to use its monetary services, it is due in

fact with the level of quality of service required and ambitioned for the network. In pursuance of this necessity and in accordance with the network's architecture envisioned for the currency, two types of active nodes, with clearly defined function, exist. The first type is to be operated, and each node built individually by, the organizations managing the Slots, while the second is open to any third-party wanting to contribute or apart of the network. The latter type however, which is responsible for the core operations involving the processing, validation and publishing of transactions, will be a homogeneous node, whose software is to be provided and maintained the WorldBank, wishfully in cooperation with the community. Additionally, since all details are publicly accessible, a layer of security and authentication is required, in consequence all nodes will acquire specific networks IDs destined to cryptographically protect them and set up an identification medium.

Finally, the WorldBank will also put forward basic services for its direct clients, through its official website[3] or its API, however in a limited capacity as to pose no risks of competition, since it is not its intended function; offer all possible documentation about the currency and, most importantly, provide a fully-fledged public data tracker displaying the latest and all past data related to UDC and its network, although other trackers are more than welcome, and actually recommended, to usher in as to increasingly separate the network from the WorldBank.

Long-Term Funding. The independence of the WorldBank, in its capacities as a central bank, from any external organization is primordial for the sustainability and credibility of UDC. Which is why it needs a, constant and regular, stream of revenue to fund its elementary activities. Such revenue is envisioned to be acquired primarily through leasing and renewal fees from the Slots' allocation, and complemented by the transaction and network fees, and other network services, such as the certifications.

2.4 Transactions

Transactions govern the currency as they let users perform, cryptographically authenticated monetary operations across the network, from simple transfers between two accounts to third-party payments authorizations or even complex smart contracts designed by third-parties. Specifically, they are pieces of data in compact JSON, each uniquely identified by a 40-Bytes long hexadecimal representation of the hash of its contents, computed using the RIPEMD-160 algorithm[4]; and contains an indication of its transaction type and a timestamp to give it a temporal context. Timestamps are values representing the Unix Epoch time in nanoseconds, this precision allows identifying incomplete transactions within the network, even during periods of elevated transaction throughput. Since UDC contains a decimal monetary subunit, all monetary amounts of UDC are expressed directly in unicents, enabling the more simplistic use of integers. Furthermore, to provide web compatibility, signatures are always encoded in Base64.

---

[3] UDC's official website: `https://www.udc.world/`

[4] RACE Integrity Primitives Evaluation Message Digest cryptographic hash function with a digest size of 160 bits.

So far, 5 transaction types have been defined, as presented in Table 4, although within the same transaction type, with the exception of the Basic type, multiple events can exist, leading to the execution or request of different actions. The first 3 are generic types with final structures already set, while the DAO and DAS ones vary accordingly to their sub-type, indicating which Decentralized Autonomous Organization or Distributed Automatic Service they correspond to, and which are defined by community-vetted third-parties. Additional types are being studied and will be incorporated if deemed useful.

Table 4. Types of supported transactions

Transaction Type	Code	Description
Basic	00	UDC's default transaction for direct monetary transfers between two accounts
Delayed	01	For Basic transactions with deferred execution times
Future	02	For pre-signed one-time transactions, of up to a pre-defined amount, executed by authorized third-parties
DAO	4F	For all smart contracts related with the Decentralized Autonomous Organizations
DAS	53	For all smart contracts related with the Distributed Automatic Services

Generic Transactions. Whenever currency is transferred across the network using a generic transaction, transaction fees might incur. In fact, when an account, the sender, submits such transaction, signed using its ECDSA private key associated with the account, the amount transferred departs through the Outbound Entity and arrives, through the Inbound Entity, into another account, the receiver, which can be part of the same or of a different Slot. A visual representation of this flow is presented with Figure 4. It is in those Entities, which are the organizations managing the related Slots, that the transaction fees are specified, though they can also be null in either or both sides. The information related to the fees is appended into the transaction by each side as a sub-object, named respectively "outbound" or "inbound", signed using their EDCSA private key. Table 5 contains the details of that additional information. The Entities' signatures differ from the signature made by the sender. The Sender signs the contents without fees, while the Outbound Entity, signs the sender's signature with his added information, and the Inbound Entity, signs the Outbound Entity's signature also with his added information. Thus, always ensuring the signatures refer only a specific transaction. An important point is the difference between the hash and signatures, the hashes use the complete JSON object while signatures use the concatenation of the values only.

Table 5. Transaction fees information

Field Name	Description
account	Account receiving the transaction fee
fee	Transaction fee in unicents
signature	Outbound/Inbound Entity's signature

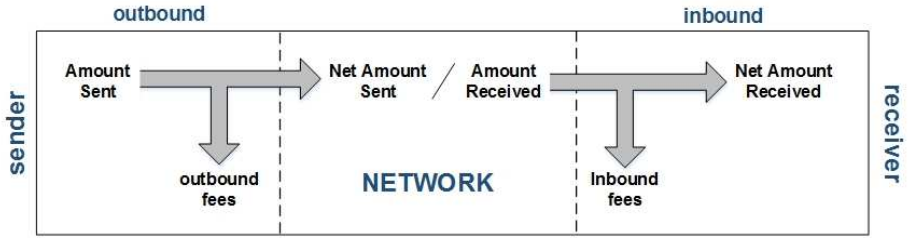

Fig. 4. Generic monetary transfer flow

Basic Transactions. Besides the mandatory type, timestamp, and signatures, these transactions only require two accounts, the sender and receiver, and the amount requested to be transmitted. A generic example is written below in non-compact JSON.

Delayed Transactions. Delayed transactions offer the same result as Basic ones, however they differ about when exactly the transfer of currency is executed. This postponed execution decomposes a single transaction into two events, Request and Release, for accountability reasons.

Request events are similar to Basic Transactions, except with the appropriate type and event. They also feature an execution timestamp, indicating when they want the transfer to be performed. A Request is created by the sender and upon its validation, only the transaction fees are debited from the account.

Release events are created directly by the network at the execution time and go through the same processing as any other transaction. Only after being validated, is the amount, already deducted of the fees, effectively transferred to the receiver. Although, if the sender has insufficient funds, the Release fails and the Request is ignored. Thus, the preemptive payment of the transaction fees serves as a penalty cost for improper requests, compensating the network for its work nonetheless, and also as a deterrent flooding attacks attempted on the network. The structure of Release events is somewhat different, rather than having a signature, they contain the hash of the Request event. Also, the timestamp, is the execution date, and the amount, the same being transferred to the receiver. Therefore, regardless of where and how the Release event is created, it will always generate the same transaction hash, since only one set of values is correct and corresponds to the related Request.

Generic transactions of both events are provided in Appendix B.

Future Transactions. Future transactions allow third-parties to execute a transaction at an ulterior date and for variable amounts, through pre-signed authorizations. It is also decomposed into 2 events, Authorize and Execute.

First, a sender issues an Authorize event, specifying a maximal allowed amount and setting its validity. The authorization can be unrestricted or restricted to either a single account or a Slot. After the Authorize has been accepted and published by the network, the sender has to sign the resulting transaction hash and transmit it confidentially to whomever it was destined to. Since the signed hash is the proof of authorization, anyone with having it can claim the available funds, therefore the sender should be wary of how and with whom he shares it.

The third-party simply has to submit an Execute event, pointing out which Authorize it concerns, specifying its transaction hash and the corresponding signature. An Execute event has the same structure as a Basic transaction, except containing the event attribute and another, designated "future", pertaining to the related authorization hash. All monetary transfers, including transaction fees, occur only with the Execute event and, similarly to a Release event of the Delayed type, they can fail if the sender has insufficient funds. Although, in this case, the Authorize event remains valid, unless its validity expires, and therefore multiple Execute events can be attempted until then. In Appendix B, examples of both events are displayed.

2.5 Decentralized Autonomous Organizations

Decentralized Autonomous Organizations (DAO) are on part based on the recent smart contracts experiment, The DAO, built on top the Ethereum cryptocurrency. Although, this experiment sadly failed due to security flaws unrelated to its actual vision, its creators ambitioned the creation of a decentralized investment firm, with dynamic investors and funds, where projects could be funded through internal voting mechanisms. Such autonomous companies with decentralized ownership, or lack thereof, have already been contemplated throughout previous years, however they are well in par with current trends. Since, with the recent, and projected, advances in machine learning and artificial intelligence, coupled with the democratization of technology-driven paradigm shifts, such as the "uberization of everything", it is in my opinion, that the next step to follow will be a massive increase of autonomy, automation and intelligence of those newly created services.

For this reason, the concept of a generic DAO was added to the currency. Third-party organizations or individuals can then create their own DAOs to offer or simply allow advanced interactions, processes and applications to exist through the network and accessed using complex smart contracts. The internal functions can be designed to support cognitive or reasoning capabilities, within a certain limit with relation to the computational resources required, and even be able to retrieve foreign data, through secure channels and always with the network's s impregnability in mind. All of which doesn't necessarily have to be made public or open access, nor constrained to commercial operations. Even their organizational structure may be freely defined, although each DAO will have a designated supervisor, at least for now. Since some human resource will most likely be required initially, as to define all the specifications and

provide documentation, albeit the goal should always remain to bring greater autonomy to the organization.

In UDC, all DAOs will have a unique ID and be integrated directly into the network's nodes, after a vetting process. These organizations will most likely generate revenue through their smart contracts, as such, each DAO is assigned an official account, from one of the reserved Slots, to where all service fees are automatically credited. Granted, since they are supported by the network, specifically by its nodes, it is only fair that a compensation and incentive is dispensed to the nodes in exchange for the computational resources and processing they require. Therefore, a global network fee rate for DAOs, (7), is levied from their share each time they generate revenue. This is accomplished through the appending a sub-object to all transactions with service fees.

$$Network\ Fee\ Rate_{DAO} = 10.00\% \tag{7}$$

The network share is each time credited into the DAO base account, "DAO0000000", to be then redistributed evenly between all nodes. Such division is done DAO-wise, the compensation funds pertaining to each one is divided equally among all nodes supporting it, while indivisible amounts, fractions of a unicent, are reported. Those surplus are bundled together and kept until the next redistribution, this time to be split indiscriminately between all existing nodes. The redistributions happen hourly, at HH:40:00Z, using a dedicated DAO transaction, containing the period it concerns and an overview of all shares and surplus, created by each node and duly processed. Appendix B illustrates both an example of a basic DAO transaction and a generic DAO transaction for fee redistribution purposes.

2.6 Distributed Automatic Services

Distributed Automatic Services (DAS) are simple services created by third-parties which become fully integrated by the nodes, through a network update, such as to automatically provide them within the network. Those services are vetted by the community beforehand and registered into the network's transaction protocols by the WorldBank, however they are overviewed by a manager, the company or individual that created the DAS, whom is responsible to define the service itself, the transaction events, logical processes and all necessary documentation. Unlike DAOs, these services are compelled to have a smaller extent, with limited events and targeted effects accomplished through less complex smart contracts, and obligatorily open to all. On the other hand, the generated revenues and related compensations, using (8), follow the same rules as with DAOs. Although, the redistributions happen hourly at HH:20:00Z instead. And the comparable DAS transactions are also provided in Appendix B.

$$Network\ Fee\ Rate_{DAS} = 15.00\% \tag{8}$$

2.7 Ledgers

In UDC, the currency is managed through a Ledger chain. However, the primary function of those Ledgers is being the monetary organizational medium, for long term safekeeping, facilitate synchronization and dissemination tool; rather than for confirming transactions. Each Ledger is a snapshot providing an overview of the current state of the network. Created hourly, they regroup all transactions published during that period, from HH:00:00Z to HH:59:59Z, and present all accounts, with a non-null balance at closing, paired with their funds, along with other related metrics.

Practically, Ledgers have their own file extension, ".ldgr", but still use a compact JSON representation for their contents. Each is identified by both a sequential numerical identifier, ID, and a hash[5] of its contents, effectively creating an unbreakable link with the Ledger chain. Its hash is computed from a combination of possessed variables, as illustrated in Figure 5, which unequivocally ensures its contents integrity and chains it with its predecessor. It includes the presence of the Ledger ID, which guarantees a different hash up to the proven collision resistance inherent to the RIPEMD-160 algorithm; the hash of the previous Ledger engraves the chain connection; a state hash, computed from the attribute listing all account-funds pairs; and the root of the Merkle tree[6] built from all of the transactions hashes. The remaining variables are left aside, since they implicitly stem from for already protected data and would be redundant. Although, the complete structure of a Ledger is exposed in Appendix C.

All Ledgers are created directly by each network node, but follow their own network protocols and validation mechanisms before being publicly disseminated, designed to self-correct and impede any deviation.

Genesis Ledger. The Ledger chain starts, commonly to other cryptocurrencies, with a special Ledger designated by Genesis Ledger which possesses the ID 0 (zero). Although it has the same structure, the corresponding values are all either empty, zeroes or null RIPEMD-160 hashes. With the notable exceptions of its closing timestamp, effectively signaling the actual beginning of the network's monetary operations of the first Ledger; and of its hash, which is computed with the same procedure, concatenating in this case the ID 0 and trice the RIPEMD-160 null hash[7].

---

[5] A 40-Bytes long hexadecimal representation of the RIPEMD-160 digest obtained from its contents.

[6] A Merkle tree is a binary tree where all non-leaf nodes contain the hash obtained from the concatenated values of their two child nodes and its leaf nodes contain the ordered hashes of the data items building the tree. UDC uses the RIPEMD-160 algorithm throughout the tree and in the event of an odd number of items, it appends the null RIPEMD-160 hash. In this case, the ordered transaction hashes are directly used as the values of the leaf nodes.

[7] Whose value is « 9C1185A5C5E9FC54612808977EE8F548B2258D31 ».

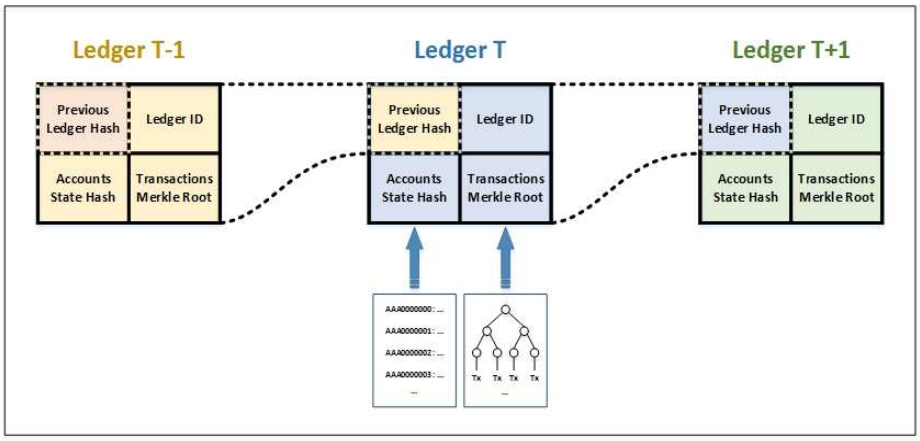

Fig. 5. Ledger chain

3 The Network

UDC is operated through a multi-layered network, that is both decentralized and distributed, constructed by a multitude of different actors running diverse network components interlinked to each other and with contrasting objectives, some to support the currency, perform its role within the network or even operate some external service. Most of the network's components have been addressed thus far, although others still remain to be formalized. Those with a direct influence and relevance to the network's own existence are the following:

- Managing Entities;
- Signing Nodes;
- Validating Nodes;
- Data Trackers.

Together, these components form the network's 3-layer architecture, illustrated in Figure 5 and detailed beneath.

- The outer layer is formed by the Signing Nodes, which are controlled by the Managing Entities. They are the connection medium between the network and the currency' users, allowing the submission of transactions onto the inner layer, and are responsible for management of accounts among other functions. Since each Managing Entity is affected only a small number of Slots, the layer becomes heterogeneously decentralized.
- The inner layer is composed solely by the Validating Nodes, the workers of the network, who form a homogeneous decentralized and distributed sub-network. All currency operations are performed in this layer, their function is to create, process, validate, publish any piece of information related to it and provide the available services or integrated ones originating from the DAOs or DASs.

- The external layer represents the Data Trackers and any other data subscribers of the Validating Nodes. Through them all information created and originated from network is disseminated to the public. Though initially this layer is most-likely centralized due to the few number of public Data Trackers, it will tend to decentralization as the network grows.

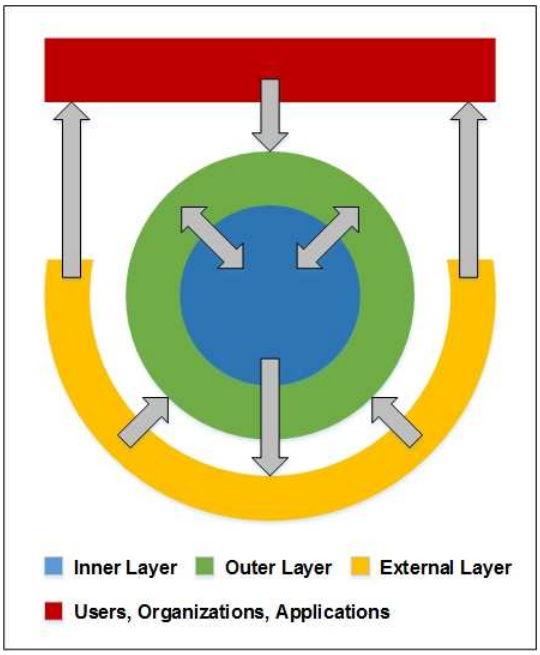

Fig. 6. Network 3-layer architecture diagram

3.1 Network IDs

All organizations, network components, DAOs, DASs and any other entity that participates, be it in a public or private capacity, in the UDC network is attributed, openly by the WorldBank, a unique network ID. The functions of those IDs are to identify any party engaged with the network and authenticate all actions performed by them, with the intention of protecting the currency and its network from external or malicious attacks. To this extent, each is associated with an ECDSA public key, corresponding to a key pair implementing a prime-based elliptic curve with a key size of at least 384bits. The paired public key can be changed anytime, simply by issuing a new one signed with the private key of the old one.

Network IDs are 8-characters long hexadecimal codes, where the first 2 characters form a prefix, which identifies the corresponding type, within UDC's network, of the associated entity. While the remaining 6 characters are used to differentiate between those of the same type, allowing for 16,777,216 unique codes of each type, more than enough

for the foreseen future. Table 6 offers an overview of the existing types and their use, all remaining prefixes are unallocated and have no use at the moment.

Table 6. Network IDs

Prefix	Example ID	Used for
45	45A1B2C3	Managing Entities
4E	4ED4E5F6	Validating Nodes
4F	4FA1B2C3	Decentralized Autonomous Organizations
50	50D4E5F6	Passports
53	53A1B2C3	Distributed Automatic Services

Passports. UDC Passports are the most elementary source of information available within the network, representing a basic form of identification and authentication of all of its participants, that is publicly and freely accessible. Each Passport can contain essential information such as general contact information, an individual's or a company's name, a website, an email or even a digital certificate, all of which cryptographically protected and modifiable using the associate key pair of their Passport ID. All other types of network IDs are directly linked to a Passport, enabling the same organization to operate multiple components, DAOs or DASs in a structured manner, while those connections being completely transparent to everyone else.

Passports, however, have nothing to do with accounts, their activation, the public keys linked to them or their owner's identity. All accounts are pseudonymous and the anonymity of the users is left at their discretion and at the discretion of the agreements they subscribed with the organizations managing the Slots.

3.2 Managing Entities

Any independent organization, who have been allocated at least a Slot, with the responsible managing it, is referred to as a Managing Entity of UDC. When leased a Slot by the WorldBank, it retains all possible rights over that Slot. Those include the possibility of sub-leasing the Slot to another Managing Entity in the conditions it chooses, control over the activation of any account contained by such Slot, therefore enabling the delivery of commercial services or an organization's internal management using bulk accounts; and, its topmost benefit, the selection of the outbound and inbound transaction fees. The specification of fees is however conditioned to an ethical rule, all fees must be explicitly conveyed to the sender beforehand, however the manner of communication is irrelevant, since they could be public, agreed through private bilateral accords or anywhere in between that expressively ensures their knowledge by the sender at all times. This beneficial privilege is giving with the objective of incentivize the support of the network and help its development, albeit upon its maturation and if in the interests of currency and users, such privilege could be extended to public Managing Entities, making the submission of transactions open to any of them.

Depending on the commercial services and other applications, a Managing Entity will most certainly have to develop web services, APIs or other networked infrastructure as to accomplish their role of bridging the users with the currency's network, since it is through them that the managed accounts can submit transactions. To this extent, each Managing Entity has to provide its Signing Node, built by it and implementing the UDC network protocols, and operate a Validating Node, running the official release and which is created in cooperation with the community and the WorldBank. It is through this node that they can be kept up to date with relation to all monetary operations and network changes in general.

Regarding the activation and cryptographic pairing mechanisms of accounts, they are unconstrained to any condition, albeit being encouraged to broadcast any new account. However, each is obligated to maintain a complete database of all activated accounts, paired with the respective ECDSA public key, and respond to any public key request emanating from a network peer.

Finally, there are no restrictions concerning the activities a Managing Entity is allowed to perform or which services they can create and provide to end users surrounding their allocated Slots. Neither with reference the levels of security or extra layers they wish to implement, although the overall computation time and throughput of the network, with relation to transactions, should be thought of when introducing additional redundant checks, since all transactions are always entirely verified regardless.

3.3 Signing Nodes

Signing Nodes are the entry point to the network for the Managing Entities, as they are connected directly to all other nodes. Albeit no, physical or virtual, separation from whatever else is offered by those Entities is required, therefore using the same computational resource, most likely a server, is acceptable. The main functions of a Signing Node are to sign and submit new transactions received from users or other nodes. It can insert the transaction fees information whenever appropriate and transmit either to an Inbound or Outbound Entity, through its Singing Node, or directly to a random Validating Node. It is also via this node that requests soliciting the public key of a managed account arrive from the network.

As stated previously, a Signing Node can also include an extra layer of security by certain verifications about the signatures, funds available and possible duplicates, made already at this network level. However, a tradeoff between having those redundancies, intended to reduce the number of to-be-rejected transactions being handled by the Validating Nodes, and the computational overcharge on itself, resulting from them, should be analyzed with respect to the overall resources the Managing Entity pretends to provide.

3.4 Validating Nodes

The currency's autonomous and independent workers are called Validating Nodes, with regards to their main role as components of the network. Unlike Signing Nodes, which

are exclusive to Managing Entities, Validating Nodes can be operated by any independent third-party, organization or individual, wanting to grow and support the network or with other interests. In exchange, an incentive, other than altruism and assuring true decentralization of this layer, is the redistribution of network fees originated by the third-party services supported by the node. This type of nodes is solely responsible for:

- Broadcasting new transactions, received from the Signing Nodes, to all other Validating Nodes;
- Accepting or rejecting transactions, through extensive processing and verification;
- Creating the resulting Ledgers;
- Providing access to the DASs;
- Supporting and operating the DAOs;
- Publishing all pieces of data validated and created, such as transactions and Ledgers.

The validation decisions are always reached through the currency's consensus mechanisms. Any deviation, be it from internal errors, attempts of tampering or malicious attacks, are detected by all and automatically corrected. Furthermore, each node individually creates and maintains a point-based reputation system, classifying all of his validating peers, used to detect and keep apart bad performing Validating Nodes, prioritizing the broadcast of new transactions randomly to the better performing ones. The reputation of each node starts at 0 and is affected depending on their correctness of validated transactions or created Ledgers. Each node's owner can, only, retrieve the reputations to monitor the others' efficiency. In a more mature network, an extension to this reputation system will be tested, including the integration of neural networks, as to analyze whether the network's performance can be optimized.

The publication of any transaction or Ledger, in order to publicly disseminate all information about the currency, is a function strictly reserved for these nodes. The actual moment of publishing each piece of data obligatorily happens after and only if the consensus reached validate by hash such piece. Afterwards the data is published to all of the Validating Node's subscribers. Those subscribers can be anyone authorized by the node's owners, and they are able to select the type of data wanted or, ultimately, unsubscribe.

Validating Node can also synchronize themselves, for example when they start up, resorting to his peers or, if necessary, trusted public Data Trackers, to retrieve and load all missing Ledgers.

3.5 Data Trackers

Data Trackers are unregulated third-parties without a network ID, which are subscribed to one or more Validating Nodes, and whose function is to provide access, publicly or privately, to all the information available about the currency, monetary activities and the network organization. They play an essential role in the dissemination of information towards all users and organizations involved with UDC. Which is why the WorldBank will operate separately a public Data Tracker to offer free and indiscriminate access by anyone. It will be hard coded into the Validating Nodes, as an additional

source of information when necessary, allowing for a quicker synchronization of the required data. But the objective is to, later on, add other reliable trackers into the source code, not only to render the network more independent, distancing itself from the WorldBank, but also to reduce additional strain put unto the Validating Nodes due to those synchronization exchanges.

3.6 Network Management Blockchain

UDC generates a myriad of diverse information dealing with its organization, which is bound to grow proportionally with the network itself and the use of the currency. The importance of this information is critical for allowing the external audit of any data generated by the network. Be it to review its validity, authenticity or integrity; guarantee the immutability of the chain and activated accounts; or even identify all peers. With the intent of ensuring complete transparency, long-term archival, further self-reliance and independence from the WorldBank, a secondary blockchain, called Network Management Blockchain, is used in UDC to regroup, disseminate and corroborate all necessary information that isn't monetary flows, already contained by the Ledgers.

The Network Management Blockchain is formed of Network Management Blocks (NMB), created every half-hour by both the Signing and Validating Nodes and utilize the dedicated file extension, ".nmb". Each NMB is composed of metadata, about its position in the blockchain and the period of time it pertains to; and a collection of Network Management Entries (NME), analogous to the Ledger's transactions, that are submitted by any network node. NMBs also uses compact JSON, continuing the web-friendly approach of the network, and their structure is specified in Appendix C.

Like Ledgers, each NMB is identified by a unique numerical identifier, ID, and a hash of its contents, linking it with the rest of the Network Management Blockchain, as pictured in Figure 7. Similarly, the hash is obtained from the ID, the hash of the previous block and the root of the Merkle tree created with the ordered entries hashes. While all NMBs are created by both types of nodes, their validation still follows the network's protocols and consensus mechanisms, and since that the broadcast of new NMEs can only be made through them, Managing Entities are required to support and integrate the Network Management Blockchain into their respective Signing Node.

Network Management Entries. While they can only be submitted into the network by one of its nodes, NMEs can be created by anyone that has a Network ID. All NMEs share the same generic structure, although, they are categorized by a resource type, which specify the kind of information being relayed and the structure of its data. These resources can have different levels of protection and authorizations, allowing for example that information about a Network ID can only be updated by itself. Currently 8 different resources exist and they can be observed in Table 7. Besides those attributes, each NME also contains metadata about itself, such as its creation timestamps; its version, proactively supporting future for network or Network Management Blockchain updates; and an entry type, to designate the effect being accomplished through it. Entry types are limited to a small set of actions, intended to either create, update, renew or cancel the related information. However, some types are not necessarily accepted by

all resources, the notable case being with the resource Account which is limited to creation NMEs. Appended to each NME is always indicated the identify of its issuer, referred to as the signer, and a signature of the hash of its contents[8]. A generic NME is provided in Appendix B.

Comparable to transactions, NMEs are uniquely identified it within the network through their hash. However, the contents used to compute the hash differ. Where, instead of using all of its attributes, only a sub-object containing the resource, data and meta attributes is hashed.

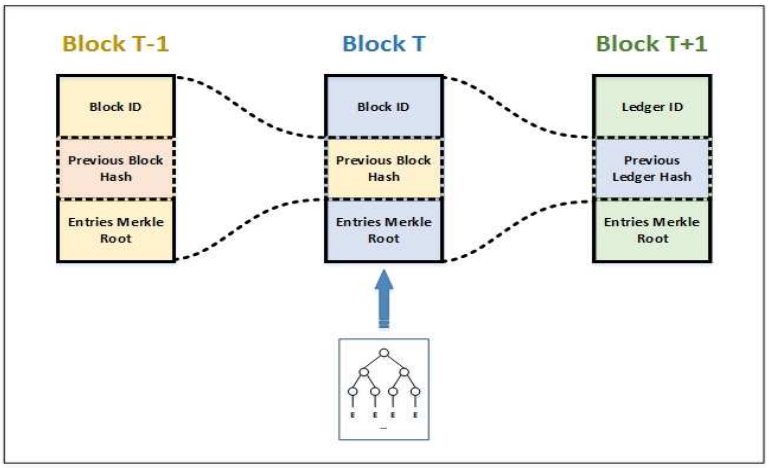

Fig. 7. Network Management Blockchain

Table 7. Network Management Entry resources

Resource Category	Description
Resource	Is used to manage and protect the resource types, containing general information about them and metadata.
Passport	Contains all basic identification and authentication data about any participant of the network.
Entity	Gathers all information about the Managing Entities and their Signing Nodes.
Node	Regroups all information about the Validating Nodes.
DAS	Contains information about the Distributed Automatic Services provided by the network.
DAO	Contains information about the Decentralized Autonomous Organizations that exist within the network.
Slot	Specifies the leasing and attribution of the Slots to Managing Entities.
Account	Maps accounts to their respective public keys.

[8] A 40-Bytes long hexadecimal representation of the resulting RIPEMD-160 digest.

Genesis Network Management Block. Unlike the Ledger Chain, this blockchain starts with an essential Genesis Network Management Block, which, besides signaling the start of the network operations, constructs the base upon which UDC and its network can operate in complete security and with trust. In total, it regroups 19 different NMEs, the minimal amount necessary to set up all the different topics and protect them beforehand. It includes building the PKI trust chain, defining the WorldBank and its nodes, creating the resources and activating the official account. A complete list is presented below, with the NMEs in sequential order:

- 1 Passport NME for the UDC root CA, self-signed;
- 4 Passport NMEs for the intermediate CAs;
- 1 Passport NME for UDC WorldBank, signed by the appropriate intermediate CA;
- 8 Resource NMEs for the activation and protection of all resources;
- 1 Entity NME for the Managing Entity of the WorldBank;
- 2 Node NMEs for both Validating Nodes of the WorldBank;
- 1 Slot NME for allocating the official Slot UDC0 to the WorldBank;
- 1 Account NME activating the UDC base account, UDC0000000.

After setting up the WorldBank's passport, all subsequent NMEs are signed by it directly.

4 Network Protocols

Having defined the structure and composition of UDC, only remains now the internal logic, shared by all participants, that controls how it operates.

4.1 Communications

UDC defines its own network communications protocols, specifying how the essential participants can interact with each other in a standardized, secure and rapid way, using TCP packets with mostly one-way transmissions, some exceptions include exchanges with Data Trackers. Specifically, these protocols provide all the messages between Signing Nodes, Validating Nodes, their subscribers, Data Trackers and the WorldBank, that are required for:

- Validating Nodes – synchronization and consensus of Ledgers and transactions, and broadcast of transactions;
- Signing Nodes – signing requests and transmissions of transactions;
- Signing Nodes and Validating Nodes – identification, connection management, submission of new transactions, public key requests, NMB consensus and synchronization, and broadcast of new NMEs.
- Signing Nodes and Validating Nodes with Data Trackers – synchronization of Ledgers and NMBs.

- Signing Nodes and Validating Nodes with the WorldBank – initial first-time registration if it wasn't done previously through a NME signed by the WorldBank when attributing its network ID.
- Validating Nodes and their subscribers – managing subscriptions and publishing the latest transactions, Ledgers and NMBs.

Each message, the TCP packet's payload, follows the common structure depicted in Figure 8, although, there are some exceptions such as keep alive or exit messages, which only contain the message code, transmission of Ledgers and NMBs, which use length fields of 4 Bytes, or even specific messages whose content does not require being signed. UDC's message codes are regrouped functionality-wise, with dedicated range of values and available exchanges, into multiple categories, presented in Appendix D. The content of a message can sometimes contain individual values of unknown size, although a fixed-size length field always precedes them, in which case, the signature is computed excluding those.

Field Size	2 Bytes	2 Bytes	1 Byte	[Signature Length] Bytes	[Total Length – 1 – Signature Length] Bytes
Field Name	**Code**	**Total Length**	**Signature Length**	**Signature of Contents**	**Contents**

Fig. 8. Network message format

4.2 Consensus

UDC's network consensus differ from common cryptocurrencies as it does not employ either Proof-of-Work or Proof-of-Stake methods. Rather, it implements qualified majority decision mechanisms which allows the network's nodes, to reach a common final result on all processed data and automatically correct themselves. Thus removing the risk of forks for either chain, while reducing the total workload for Validating Nodes, since not all of them will have to process every single transaction submitted to the network. Normally any decision based on a majority would lead to the same problems existing in Proof-of-Work blockchains, where an entity who has enough processing power, or in this case controls enough nodes, could take-over the currency. However, by virtue of the use of Network IDs and the network's goal of having a diversified decentralization, where any participant or even the WorldBank has control over only a limited number of components, it cannot happen with UDC. This fact is accentuated by how Managing Entities are structured, each has to operate a Validating Node but only oversees a small quantity of Slots, which is negligible compared to the total number of Slots and will therefore lead to the existence of many Managing Entities. Furthermore, unrelated organizations can also run a Validating Node, which coupled with the transparent identification of any participant dilutes any control possessed by a single group.

Any new transaction submitted by a Signing Node onto the network to a random Validating Node is then broadcasted to a certain percentage of its peers for processing, with that percentage defined by the Transaction Broadcast Ratio (TBR). Afterwards, each time a node asserts its validity, it broadcasts a vote to all other peers,

identifying it by its hash. If a transaction reaches the consensus, defined by the Transaction Confirmation Threshold (TCT), it becomes accepted by the network and can be published and registered into its Ledger, while the invalid transactions are routinely discarded. This method is able to reduce the resources used by the network for processing each transaction, through the avoidance of unnecessary repetition of work, and ensures that any transaction has already been agreed by the network as a whole by the time it is published by any Validating Node. The ratios to be used initially in UDC for transactions, are specified in (9) and (10).

$$TBR = 0.8 * Number\ of\ Validating\ Nodes \tag{9}$$

$$TCT = 0.6 * Number\ of\ Validating\ Nodes \tag{10}$$

For Ledgers and NMBs the process is somewhat different, upon their creation, each node broadcasts a vote for the hash they computed. However, since the network has obligatorily to arrive at an agreement about the next piece of the chain, unlike with individual transactions, if no hash reaches the required threshold, defined by the Ledger Confirmation Threshold (LCT) and Block Confirmation Threshold (BCT) respectively, a special resolution mechanism, called Collective Rebuilding, is activated. With Collective Rebuilding, each node broadcasts all hashes, of transactions or NMEs respectively, it validated, and then recreates the latest chain link[9], using only those that attained the same threshold. Afterwards a second vote is initiated, however this time, the ratio is disregarded and the highest voted chain link is imposed. The initial values to be applied are (11) and (12).

$$LCT = 0.7 * Number\ of\ Validating\ Nodes \tag{11}$$

$$BCT = 0.6 * Number\ of\ Signing\ and\ Validating\ Nodes \tag{12}$$

There is no consensus for NMEs, as they are not published on their own and because the execution of each should lead to the same results across the network, since they are broadcasted to all nodes.

All ratios are hard-written into the source code of the Validating Nodes and can be changed in the future by the WorldBank with the community and other involved parties, if after extensive study and analysis of the network's traffic and data obtained by the reputation systems it concluded that other values would optimize the network efficiency and performance.

4.3 Logical Flows

Transaction Life-Cycle. From conception to registration, a transaction has to go through an extensive number of steps, as it is possible to observe in Figure 9, which depicts the life-cycle of a valid new transaction.

[9] Represents either the latest closed Ledger or Network Management Block.

Transactions mostly emerge directly from an end-user, be it a person or an organization, although they can be conceived by a Managing Entity for internal operations or external payments for example. Although, all new transactions always end up at the Signing Node responsible for the related Slot. In this phase, the Inbound transaction fees are appended, if applicable to its type, and it is transmitted to the Outbound Entity if necessary. The transaction is either submitted directly, or indirectly by the Outbound Entity, to the network through a random Validating Node, ultimately balancing the workload instead of constantly overcharging the same node. This random node is then responsible for broadcasting the transaction for processing by its peers, according to the network's validation mechanisms. It also, upon ending the verification, returns a preliminary response to the Signing Node that communicated the transaction, indicating if it was validated or rejected, stating the error encountered, if so. Although it has no definitive implication, since it does not affect other nodes or their responses, and therefore, neither the transaction's consensus, it might serve as an expected result.

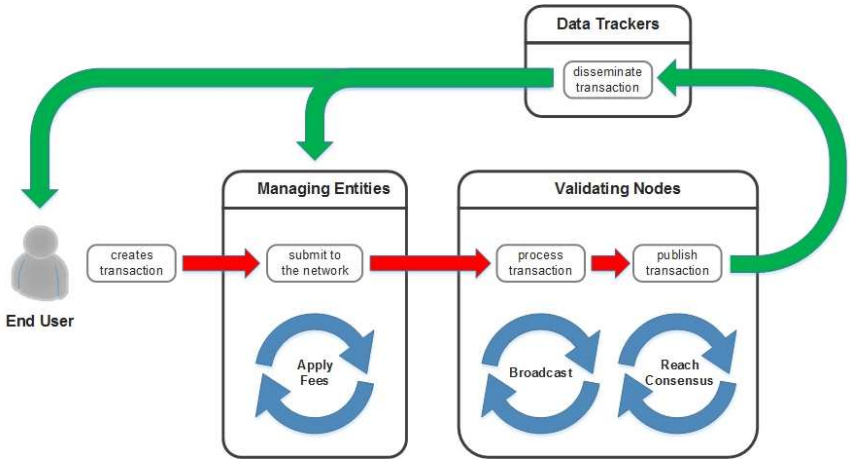

Fig. 9. Life-cycle of a valid transaction

After the transaction is processed, all Validating Nodes corroborating its veracity broadcast a vote in its favor, tagging it by its hash, forcefully starting the decision process. If the network reaches a consensus, the transaction can finally be executed, registered into its corresponding Ledger and published to all the node's subscribers that are subscribed to transactions, otherwise it is plainly discarded. Validating Nodes that didn't received initially the transaction or incorrectly processed it, can directly request one of those who did to rapidly execute, register and publish it.

Afterwards the transaction can finally be disseminated publicly and the end-user informed of its registration, either directly by its Managing Entity, who can be one of the subscribers or at least itself informed by one of them, or openly through a Data Tracker.

Network Management Entry Life-Cycle. Compared to transactions, NMEs have simpler validation processes. They can be created directly by a Signing or Validating Node, or externally, by anyone with a Network ID, who then has to submit it to the network through a Managing Entity. This node then broadcasts the NME to all his peers for processing. Each other node then verify it and respond indicating whether it was accepted or rejected, in which case they include an error code signaling the problems encountered. If the NME was validated, it is then executed by each node, if its contents were relevant for such node, and directly registered into the current NMB. Unlike transactions, NMEs are only published collectively through their NMB and not on their own, reducing the network resources required by the Validating Nodes for publishing data and without impacting overall propagation of data since NMBs have shorter duration.

Ledger and Network Management Block Life-Cycle.
Ledgers and NMBs both follow the same global control logic, although with NMBs, Signing Nodes, and not just the Validating Nodes, participate in the processes. The creation process begins at the closing time of the chain link, although, closing is not immediate to account for pending transactions or NMEs, whose timestamps fall within the encompassed period and lateness can be attributed to network delays. The moment this network grace period ends, the chain link is permanently closed and built locally by each node. The computed hash can then be broadcasted and signal the start of the consensus. The consensus ends if either a hash reaches the required majority or the time limit was attained. In the latter case, the Collective Rebuilding process is activated. Each node broadcasts all included hashes, of accepted transactions or NMEs respectively, and rebuilds the chain link with the ones agreed up until the allocated duration. This process then finishes with the selection of the most prominent hash, also ending the consensus. Validating Nodes can afterwards publish the correct new chain link to all of their subscribers.

All nodes who generated an incorrect chain link, can simply request the right one from the correct peers randomly, execute it internally while reversing the effects of incorrectly executed transactions or NMEs, and, eventually, publish it to its subscribers.

5 Envisioned Digital Ecosystem

For UDC to attain its very difficult and ambitious goal of unifying global commerce, it has to be useful and practical, otherwise it will not reach ubiquity and worldwide adoption. Therefore, it is imperative that an enormous digital ecosystem is created, ensuring that the services provided through UDC are numerous and diverse, and that it is accepted and recognized locally but also globally, encouraged by the reduction of currencies conversion fees in international trades, and thus attracting vendors and consumers, or more generally users and organizations.
Although UDC envisions much greater applications as a digital currency than being just used as medium for digital payments, solely penetrating the Payments Industry and rivalling any of the current major players will be a remarkable but decisive feat to be accomplished, preferably, in the medium-term. As it is possible to examine in Figure

10, the market size of digital payments is gigantic and bound to grow annually around 10%. Even limiting to the regions affected by the pegged currencies, it would correspond to a volume of more than 200 billion transactions annually, to either erode in UDC's favor or complement. With Table 8, we can observe however the disparity of the market's share between the world's leading players in debit and credit cards payments, online payments and cryptocurrency respectively. Interestingly, we can extrapolate a tendency of higher profitability[10] and monetary volume[11] per transaction for the smaller players. Bitcoin's growth, should also be taken into account, it is expected to reach 80 million transactions executed in 2016[12], an annual increase of almost 74%. While being negligible compared to the market size, reaching and surpassing it is of course an intermediate objective of UDC, although being able to cross the 1 billion mark will be a shocking milestone, especially if as the first digital currency to do so.

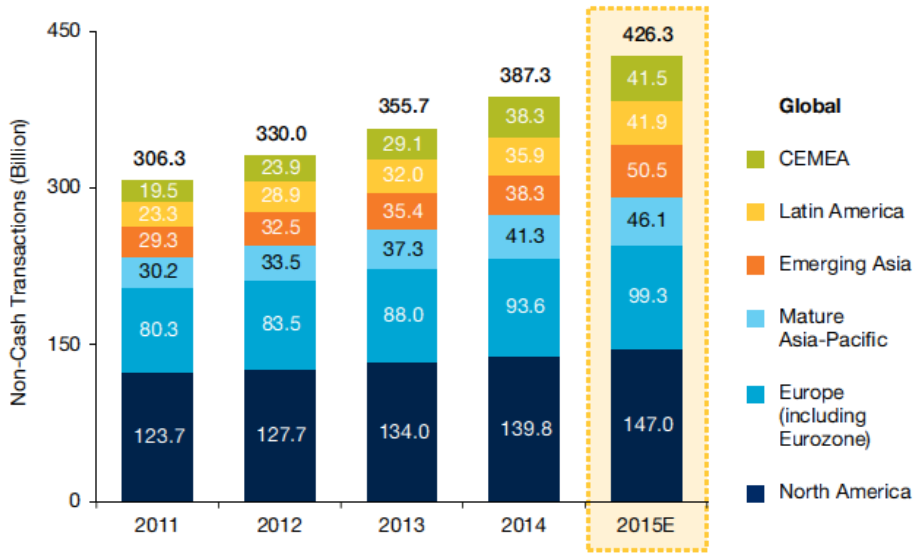

Fig. 10. Worldwide non-cash transactions (source: Capgemini, World Payments Report 2016)

[10] Visa Inc. has a revenue rate per transaction of ~0.15$US, against ~1.88$US for PayPal and ~8.26$US, although Bitcoin revenues are skewed due to the blocks mining rewards.

[11] Visa Inc. has an average amount transacted of ~55.30$US, against PayPal's ~57.55$US and Bitcoin's ~589.95$US. The considerable difference is due part to the transaction rates used by the source, which could be misrepresentative of the value of Bitcoin at the moment of each transaction, and the elevated speculation, commonplace in the cryptocurrencies environment.

[12] Around 60 million transactions have been executed as of 1st October 2016, making an average of 20 million per quarter. (source from note 15)

Table 8. Payments Industry, market share indicators for 2015, in millions

	Revenue ($US)	Payments Volume ($US)	Transactions
Visa Inc.[13]	13,880	4,931,000	89,160
PayPal[14]	9,240	282,000	4,900
Bitcoin[15]	380	27,000	46

5.1 Financial Services

Financial services are the backbone of any digital currency. Although the WorldBank will provide certain of such services, they will be limited by design and intended to not expand the already vast range of responsibilities it possesses.

The most basic ones encompass of course, the general purpose Payment Services Providers. Although, simple repetition without innovation or differentiation might not lead to the adoption ambitioned for UDC. From one side, services targeting users should be offered, easing the currency's use and abstracting the inner workings of the network, such as multi-platform desktop wallets, mobile wallet apps, with direct access to an account, and even web plugins, enabling the creation or signature of transactions in simple and fast manners. From the other side, we have the merchant services, which imperatively have to go hand in hand with the costumer side. These services have to surpass the usual merchant gateways and online shop payment integrations, to include POS[16] applications and interfaces, essential to branch the currency into local adoption, and innovative mechanisms to allow wireless and biometric-based payments.

Afterwards, comes the currencies and securities trading platforms, which go further than the limited deposits and withdrawals offered by the Providers. Albeit, its more judicious having the existing platforms integrate UDC, and thus directly connect it to the other cryptocurrencies and non-pegged fiat currencies, rather than recreate whole platforms who function the same exact way, except being centered around a different currency.

Such integration, this time with relation to already established Payment Services Providers, can indubitably happen for the basic services previously discussed. And an extension of this, is the acceptance of remittances and currency exchanges through local businesses, either nation-wide or globalized, which increases the overall utility an d adoption of UDC. On the same topic, the lack of offline monetary transfers is also a critique often attributed to digital currencies, partly by people seeking reassurances and

---

[13] Visa Inc., Press Release, 2015 Full-Year Earnings Report, `http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=2104992`

[14] PayPal, 2015 Results, `https://www.paypal.com/us/webapps-/mpp/about`

[15] Revenue from `https://blockchain,info/charts/miners-revenue`, Payments volume from `https://blockchain.info/charts/estimated-transaction-volume-usd`, total number of transactions from `https://blockchain.info/charts/n-transactions-total`

[16] Point-of-Sale

some form of control over their wealth. This issue is recurrent whenever a push for greater digitalization of fiat currencies or limitation of the maximum authorized amount for cash payments[17] is proposed. Although in those cases the fear is the growing power and control that is transferred from each individual to the banks in general, leaving their wealth without protection over the direct effects of interest-rate policies or service-wise problems, whose resolution can sometimes take longer than desired, depending on the bank's costumer service. All of which are not necessarily present in UDC, since regardless of the Slot or the current Managing Entity, the only thing controlling an account is solely the private key protecting it. Therefore, secure mechanisms and services enabling offline transactions should be proposed, and incentivized, due to their relative importance and positive impact on the more reticent public.

Peer-to-peer lending, a recent and growing financial concept emanating from the sharing economy construct; and project funding in general, either through venture capital (VC) funds or crowdfunding, which has gained huge traction and popularity these last couple of years, especially with the success of Kickstarter; have all great importance for the growth of a digital currency. Be it to stimulate and support the innovative projects brought on by the community's developers, or merely to offer investment capabilities in par other economies and in a more direct form for either side of the investments. Those types of services are essential and can very well be provided within UDC's ecosystem, either built on top of it, such as a company operating as a Managing Entity, or fully integrated, such as automatized services functioning with their own logical processes, or decentralized organizations conducted with variable levels of autonomy defined by vetting and decision mechanisms internally managed, as was, for example, ambitioned by Ethereum's The DAO project.

Lastly, UDC is also capable of providing its own, transparent and trustworthy, solution to the pervasive problems of scamming, fraud and theft, that have plagued digital trades and exchanges since their existence. Escrow services can be implemented to provide the crucial level of protection that is required and desired by all parties of any exchange, while relinquishing unpredictable[18] intermediaries, once again, either directly using DAOs or indirectly by a third-party. Such escrow practices can include automatized features like transfers triggered by appropriate events; support for payments originating from diverse providers and even in other currencies, verified through

---

[17] The limitation of cash payments regards mostly Europe, where the maximum authorized amounts can be as low as 1,000€ for purchases of goods and services, while it can increase up to 15,000€ in special conditions, like for real estate, non-residents or between private individuals. It includes so far 12 countries or the European Union, including Belgium, France, Italy and Spain; while 8 others have functional limits. (source: European Consumer Centre, `http://www.europe-consommateurs.eu/en/consumer-topics/financial-services/banking/means-of-payment/cash-payment-limitations/`)

[18] This unpredictability refers to the lack of absolute certitude that one or more of the parties involved can have on the intermediary, regardless of previous interactions or existing feedback and especially if it is an individual. Since collusion with another party, usurpation of identity or opportunistic behavior due to high enough benefits are no uncommon in online trades.

external legitimate sources; and creation of external payments submitted through approved affiliations.

5.2 Commercial Services

Commercial services provide a legitimate usage for UDC, and can occur in the form of peer-to-peer auction platforms or marketplaces, specialized or generalized, covering goods and services, freelancing or even crowdsourcing, which can become totally decentralized within the network. For example, peer-to-peer platforms could function as a DAO, whose transactions and events would manage the dynamics of such system, including the items, trades, users and payments, while third-party websites would simply have to deliver such information to the users.

Private shops can also be incorporated directly into the network or, including physical shops, integrate UDC in their infrastructure. The great benefit that emerges from how UDC and its network are structured is that individual companies, groups of companies, or companies providing services for constructing online shops can replace their financial intermediaries by becoming Managing Entities themselves and receive direct payments from customers, as they only have to redirect the transaction to the appropriate Entity; have complete control over their accounts, removing any risks of frozen assets or fraudulent chargebacks; and reduce fees, since they're the ones setting them.

With the current and next trends in mind, automatized commercial services can be implemented, encompassing automatic subscription systems or other more futuristic activities such as local transportation, including even autonomous taxis, or local deliveries, using for example autonomous drones. More common services, distributed through the network, can include secure email providers or encrypted content applications, because even though it would increase the volume of transactions flowing across the network, their validation overhead would be quite limited.

5.3 Entertainment Services

The entertainment services include the ubiquitous and profitable gambling industry. All forms of gambling, including lotteries, casino games, card games and other innovative gamified gambling, can without a doubt integrate UDC or be provided through it, either managed by third-parties or designed as decentralized peer-to-peer systems. On the spotlight within the gambling industry there is also the prolific betting sector. Services from traditional or personalized peer-to-peer bets to sports and, with ever-growing popularity, e-sports bets, with different levels of complexity, automatic payoffs and real-time verification from accredited sources, can be proposed. While at the same time being transparent and distributed, and reducing welching, insecurity or other risks often associated with them.

Related to e-sports and the expanding gamification comes the associated need of systems capable of supporting micropayments, especially for indie developers or individuals. Similar to the private shops question, such services can be assured without any intermediaries or at least in better conditions and more malleable. These types of

services can also extend, or be applicable, to events booking, which are currently provided through platforms that are recurrently deemed controversial and questionable by both sides, customers and performers. Such booking systems could easily be incorporated and automatized through UDC.

5.4 Miscellaneous Services

The range of usages that can be associated with UDC is of course very broad and encompasses a multitude of sectors, since, although, its goal is to unify global commerce, it should by no means limited to that scope. Although a few other categories or specific services can be highlighted. An example already addressed is that companies can become emancipated their financial intermediaries by managing their own Slots. As Managing Entities, they can therefore increase the control they have on their assets, reduce costs, perform internal operations such as payroll handling, and even external operations, including receiving payments from customers or paying suppliers directly. With the only counterpart of running and developing a Signing Node and operating a Validating Node. Besides this and more generally, any type of organization, privately owned or with dynamic ownership, its websites or could be created within UDC's network as DASs or DAOs.

Besides Data Trackers, more advanced data-oriented services can exist. They can focus on providing analytics or access to refined data and other types of knowledge, including distributed and decentralized information, such as an online identity system. Somewhat related, albeit divergent, are the masquerading, anonymizing or coin mixing services, whose intention is to provide a greater sense of privacy within a completely open currency. These services already exist within other cryptocurrencies and can be applied with ease to UDC as well. Notarial, authentication and other certification services integrated within blockchain systems have also been studied before. Such services can be used for applications ranging from transfers or proofs of ownership, of property and other goods, to certifications and third-party mediations of business or private contracts.

Finally, UDC can be used as a valuable medium for receiving and sending donations transparently, while, at the same time, remove the illegitimate control over the funds that is sometimes used to silence or pressure organizations. Even charities could integrate the currency or be established within it.

6 UDC Launch Outline

An overview of the plan for launching UDC and its network can be outlined as follows:

1. Announcement of the Unified Digital Currency through the publication of this proposal. Launch of the temporary official website, providing general information and a starting point for the community, and develop its social media presence.
2. Request for funding and search for investments or partnerships to develop the WorldBank's infrastructure and finish the first complete version of the Validating Node, whose core components are already built.

3. Publication of the detailed network communications protocol and the standards for the development of DAOs and DASs modules to be integrated into Validating Nodes, both of which are currently near completion.
4. Launch of the full official website and the WorldBank's API. Completion of its Signing Node and of the official Data Tracker.
5. Opening of the candidacies for the allocation of Slots and proposals for the creation of DAOs and DASs. Search for local and online currency exchange partners.
6. Completion of the Validating Node v1 Release Candidate 1, construction of the final Genesis Network Management Block and review of candidacies and other preparations for the currency's launch.
7. Launch of UDC and integration of approved Managing Entities, DAOs and DASs.

After its effective launch, the next goals for UDC are to consolidate the WorldBank's reserves and international financial partnerships; raise awareness of the general public and grow the community; and most importantly, help the expansion of the network by providing frameworks and greater support, with the optic of increasing the number of Managing Entities, existing companies integrating the currency and applications being built around it.

Appendix A

Table A1. Economic indicators for 2015, in millions of current US$

Country or Region	GDP	Exports of goods and services	Imports of goods and services
Australia	1,339,539	265,116	284,024
Canada	1,550,537	488,963	524,778
China	10,866,444	2,431,264	2,045,761
Hong Kong	309,929	623,451	616,126
Japan	4,123,258	738,085	778,281
Singapore	292,739	516,670	438,003
Switzerland	664,738	422,034	339,851
United Kingdom	2,848,755	781,530	837,558
United States	17,946,996	2,253,425	2,782,325
Euro area	11,539,744	5,289,875	4,784,164
World	73,433,644	21,274,331	20,652,682

(source: The World Bank Group, World Development Indicators of 2015, `https://databank.worldbank.org/data/reports.aspx?source=world-development-indicators`)

Table A2. Currency distribution of foreign exchange average daily turnover in April 2016

Currency Denomination	Share	Rank
United States Dollar	87.60%	1
Euro	31.30%	2
Japanese Yen	21.60%	3
Pound Sterling	12.80%	4
Australian Dollar	6,90%	5
Canadian Dollar	5.10%	6
Swiss Franc	4.80%	7
Chinese Yuan Renminbi	4.00%	8
Singapore Dollar	1.80%	12
Hong Kong Dollar	1.70%	13
Total	200.00%	---

(source: Bank for International Settlements, Triennial Central Bank Survey – Foreign exchange turnover in April 2016, `https://bis.org/publ/rpfx16fx.pdf`)

Table A3. UDC pegged currencies statistics

Currency Denomination	Trade Weight	Importance Factor	Proportion
United States Dollar	0.28059013	1.12179696	41.44%
Euro	0.87298641	0.58624475	21.66%
Japanese Yen	0.36775933	0.29543602	10.91%
Pound Sterling	0.56834939	0.20074872	7.42%
Swiss Franc	1.14614502	0.10301496	3.81%
Australian Dollar	0.40994738	0.09728637	3.59%
Hong Kong Dollar	3.99955546	0.08499244	3.14%
Canadian Dollar	0.65380015	0.08434381	3.12%
Singapore Dollar	3.26117061	0.07670107	2.83%
Chinese Yuan Renminbi	0.41200462	0.05648018	2.09%
Total	---	2,70704528	100.00%

(source: Tables A1 and A2)

Appendix B

This Appendix contains examples of different types of data used within the network, such as transactions and events, and Network Management Entries, all presented here in non-compact JSON for illustration purposes.

Code Block B1. Generic Basic transaction

```
"[Transaction hash]": {
    "type": "00",
    "timestamp": ##################,
    "sender": "XXX#######",
    "receiver": "XXX#######",
    "amount": [unicents],
    "signature": "[Base64 encoded signature]",
    "outbound": {
      "account": "XXX#######",
      "fee": [unicents],
      "signature": "[Base64 encoded signature]"
    },
    "inbound": {
      "account": "XXX#######",
      "fee": [unicents],
      "signature": "[Base64 encoded signature]"
    }
}
```

Code Block B2. Generic Delayed transaction for a Request event

```
"[Transaction hash]": {
    "type": "01",
    "event": "request",
    "timestamp": ##################,
    "execution": ##################,
    "sender": "XXX#######",
    "receiver": "XXX#######",
    "amount": [unicents],
    "signature": "[Base64 encoded signature]",
    "outbound": {
      "account": "XXX#######",
      "fee": [unicents],
      "signature": "[Base64 encoded signature]"
    },
    "inbound": {
      "account": "XXX#######",
      "fee": [unicents],
      "signature": "[Base64 encoded signature]"
    }
}
```

Code Block B3. Generic Delayed transaction for a Release event]

```
"[Transaction hash]": {
    "type": "01",
    "event": "release",
    "timestamp": ###################,
    "request": "[Request event's transaction hash]",
    "sender": "XXX#######",
    "receiver": "XXX#######",
    "amount": [unicents]
}
```

Code Block B4. Generic Future transaction for an Authorize event

```
"[Transaction hash]": {
    "type": "02",
    "event": "authorize",
    "timestamp": ###################,
    "validity": ###################,
    "sender": "XXX#######",
    "receiver": "XXX#######", /*optional*/
    "slot": "XXX#", /*optional*/
    "amount": [unicents],
    "signature": "[Base64 encoded signature]",
}
```

Code Block B5. Generic Future transaction for an Execute event

```
"[Transaction hash]": {
    "type": "02",
    "event": "execute",
    "timestamp": ###################,
    "sender": "XXX#######",
    "receiver": "XXX#######",
    "amount": [unicents],
    "future": "[Authorize event's transaction hash]",
    "signature": "[Base64 encoded signature]",
    "outbound": {
      "account": "XXX#######",
      "fee": [unicents],
      "signature": "[Base64 encoded signature]"
    },
    "inbound": {
      "account": "XXX#######",
      "fee": [unicents],
      "signature": "[Base64 encoded signature]"
```

```
    }
}
```

Code Block B6. Example of a DAO transaction

```
"[Transaction hash]": {
    "type": "4F",
    "DAO": "4FHHHHHH",

    /*Custom transaction Content*/
    …
    "timestamp": ###################,
    …

    /*Optional Fees Detail*/
    "serviceFees": {
      "account": "DAO#######",
      "fees": [unicents],
      "networkFee": [unicents]
    }
}
```

Code Block B7. Generic DAO transaction for fee redistribution

```
"[Transaction hash]": {
    "type": "4F",
    "DAO": "4FFFFFFF",
    "start": ###################,
    "end": ###################,
    "total": [unicents],
    "reported": [unicents],
    "shares": [
      /*Repeat for each Validating Node*/
      {
        "node": "4EHHHHHH",
        "account": "XXX#######",
        "share": [unicents]
      },
      …
    ]
}
```

Code Block B8. Example of a DAS transaction

```
"[Transaction hash]": {
    "type": "53",
```

```
    "DAS": "53HHHHHH",

    /*Custom transaction Content*/
    …
    "timestamp": ###################,
    …

    /*Optional Fees Detail*/
    "serviceFees": {
      "account": "DAS#######",
      "fees": [unicents],
      "networkFee": [unicents]
    }
}
```

Code Block B9. generic DAS transaction for fee redistribution

```
"[Transaction hash]": {
    "type": "53",
    "DAS": "53FFFFFF",
    "start": ###################,
    "end": ###################,
    "total": [unicents],
    "reported": [unicents],
    "shares": [
      /*Repeat for each Validating Node*/
      {
        "node": "4EHHHHHH",
        "account": "XXX#######",
        "share": [unicents]
      }
    ]
}
```

Code Block B10. Example of a resource-generic Network Management Entry

```
"[Network Management Entry hash]": {
    "resource": "[NME resource]",
    "data": {
        /*Custom resource data*/
    },
    "meta": {
        "type": "[NME type]",
        "date": ##########,
        "version": "...",
    },
```

```
    "signer": "[Network ID]",
    "signature": "[Base64 encoded signature]"
}
```

Appendix C

Table C1. JSON structure of a Ledger

Attribute Name	Data Type	Description
ledgerId	Integer	Ledger numerical identifier
ledgerHash	String	Current Ledger hash
previousLedgerHash	String	Previous Ledger hash
accountsHash	String	Hash of the accounts array
transactionsRoot	String	Root of the Merkle tree built with all transactions hashes
opening	Integer	Ledger's opening timestamp in seconds
closing	Integer	Ledger's closing timestamp in seconds
numberOfAccounts	Integer	Number of existing accounts with a non-null balance
numberOfTransactions	Integer	Number of transactions executed within this Ledger
amountInCirculation	Integer	Total amount of currency in circulation
amountTraded	Integer	Total amount traded during course of this Ledger
feesCollected	Integer	Total amount of fees collected during the course of this Ledger
accounts	Array	Alphabetical list of all account-funds pairs with a non-null balance
transactions	Array	Chronological list of all transactions executed during the course of this Ledger

Table C2. JSON structure of a Network Management Block

Attribute Name	Data Type	Description
blockId	Integer	Block numerical identifier
blockHash	String	Current Block hash
previousBlockHash	String	Previous block hash
date	Integer	Block's closing timestamp in seconds
entriesRoot	String	Root of the Merkle tree built with all Entries hashes
data	Object	Collection of all submitted entries

Appendix D

Table D1. Network message codes categories

Codes category	Code range (hex)	Uses
Management	0x0000 – 0x00FF	Connection management
Registration	0x0100 – 0x01FF	Registration requests and responses
Identification	0x0200 – 0x02FF	Identification requests and responses
Account	0x0300 – 0x03FF	Accounts' public key requests and responses
Transaction	0x0A00 – 0x0A1FF	Requests and responses for the submission of new transactions and their transmission, broadcast and consensus
Ledger	0x0A20 – 0x0A2FF	Consensus and transmission of Ledgers
NME	0x0A30 – 0x0A3FF	Requests and responses for the submission and retrieval of NMEs
NMB	0x0A40 – 0x0A4FF	Consensus and transmission of NMBs
Subscription	0xB000 – 0xB1FF	Publishing of new data and management of subscriptions
Tracker	0xB200 – 0xB2FF	Ledgers and NMBs requests and responses