ICO.ALTCOINOMY.COM

Altcoinomy ICO

Yellow paper

Hard Asset Revolving Initial Coin Offerings

OLIVIER NATHAN COHEN
NOÉ CURTZ

MARCH 2018

Abstract

In this yellow paper, we aim to design an organizational framework, backed by distributed ledger technologies, in order to set up a new model for the securitization of non-conventional investments such as the components of the Knight Frank Luxury Investment Index (KFLII)[1]. Initially, the objective is twofold: (1) first to use cryptographic methods for the notarization of the custody of hard assets on a public blockchain, and (2) second, to use cryptocurrencies in a manner to enable effective price discovery of such exotic or non-fungible hard assets. We believe that this framework will help in providing transparency and liquidity in markets traditionally plagued by layers of financial intermediaries as well as low levels of granularity.

The end goal of this project is to leverage the maturing blockchain ecosystem in order to accomplish what the blockchain technology was originally intended to create: the possibility of allowing anyone to transact and exchange value without any financial intermediation. However, unlike bitcoin which is backed only by trust in the network, fed by deflationary dynamics and valued against fiat in relation to the growth of its worldwide adoption rate, our currencies will be backed by real, hard assets. **Owning the token will be tantamount to owning the hard asset itself.** Co-ownership of these hard assets will be proved cryptographically: the investor will own the private key, thus co-owning the assets. The investor will be able to exchange co-ownership right peer-to-peer through the Ethereum protocol. The tangible assets will be managed by a not-for-profit foundation and held in custody in Swiss Freeports[2].

With this perspective in mind, we will:

1. Explain the necessity of a centralized approach in regards to the custody of hard assets as well as for the notarization of the proof of custody.

2. Explain the necessity of a decentralized approach in regards to the storage of the proof of custody (IPFS) as well as for the maintenance of a public ledger of cryptographically secured property rights (ERC20 tokens) which can be used by their holders as tradable IOUs.

3. Expose the underlying smart contract that will allow the entity to dynamically and continuously adjust the asset-backed monetary supply within an inflationary-neutral economic model – a process we will refer to as a "revolving ICO".

[1] The Knight Frank's Luxury Investment Index (KFLII) tracks the performance of a theoretical basket of nine selected collectible asset classes - such as art, classic cars and wine - using existing third-party indices. Each asset class is weighted to reflect its relative importance and value within the basket.

[2] The Geneva Freeport is 85% owned by the State of Geneva

In simpler words, we will explain in detail how we intend to tokenize tangible assets, and allow anyone to cryptographically prove transparent, undisputable, fractional ownership of an original Picasso painting, a Ferrari 250 GTO, or a collection of cases of Romanée-Conti, while relying on market efficiency for pricing such possessions.

Meet the new tokens :

WINE (fine wines)
GEM (high-end gemstones)
CAR (luxury and vintage cars)
WATCH (collectible watches)
ART (modern and contemporary masterpieces)
STRADIVARIUS (prestigious musical instruments)

Table of Contents

I. Introduction and problematics

Over the last decade, digital ledger technologies (D.L.T.) have gained undeniable credibility to serve as a universal support for the emergence of a new decentralized monetary system.

Bitcoin was the first fully autonomous protocol to utilize distributed consensus technology to create an efficient peer-to-peer, cryptographically secure, global payment network away from the traditional banking system. Bitcoin *de facto* removed the need for a middle man to act as a trustworthy, confidential fiduciary.

Beyond the utilitarian value of empowering decentralized financial transactions for their users, a few projects later came to life to enhance the capabilities of the blockchain ecosystem. Amongst them Bitshares, designed as a platform to decentralize the shareholding of digital assets and entities.

Furthermore, with the advent of the Ethereum blockchain and its related Virtual Machine, the possibility to execute the terms of a contract through a computerized transaction protocol was established. Laying the terms and triggers of a contract through a self-operating computer program offers the advantage of expecting a non-ambiguous and replicable outcome, freed from plural or legal interpretations. As smart contracts run on the blockchain, they run exactly as programmed without any possibility of censorship, downtime, fraud or third-party interference. Therefore, they can tremendously facilitate the exchange of money, content, property, shares, or anything of value.

In the same way the Internet has helped harness the combined power of all humanity to coordinate the discovery and aggregation of knowledge in real-time, for the first time in mankind's history, the allocation of resources can be transferred effectively toward their most productive and valuable use. Just like the Internet has freed *Information*, digital ledger technologies could theoretically set *Property* or *Ownership* free.

Interestingly, the adoption of Ethereum as a platform happened precisely because it facilitated the organization of crowdfunding through Initial Coin Offerings (ICO) rather than as a result of corporations or individuals actually drafting smart contracts between themselves to accommodate the conduct of business in the real world. In the same way bitcoin was originally designed as a payment system but was led astray and denatured into a speculative investment, Ethereum was originally designed as a decentralized contract platform for the corporate world but only gained mainstream adoption, through ICOs, because it revolutionized the transfer of property.

As of today, one can consider Bitcoin – read transfer of value – the killer app of blockchain technology and ICOs – read transfer of ownership – the killer app of smart contracts.

Throughout this yellow paper, we will try to push further the amazing potential that digital ledger technologies provide in order to facilitate the exchange of property between individuals and corporations. Surprisingly, this use case has been largely disregarded throughout the flurry of fintech ICOs since 2017, but might actually be DLTs' natural fit, if done right, and especially when applied to tangible, hard assets.

II. Necessary centralization ? The good, the bad, the ugly... The mandatory

"The objective of Satoshi Nakamoto and the early Bitcoin developers was to create a decentralized payment system that is both self-sufficient and self-contained. Perhaps naively, they thought it was possible to create a new technological infrastructure that would be able to govern itself – through its own protocols and rules – and that would not require any third-party intervention in order to sustain itself. And yet, in spite of the mathematical elegance of the overall system, once introduced in a particular socio-economic context, technological systems often evolve in unforeseen ways and may fall prey to unexpected power relations."

Primavera De Filippi

When drawing parallels between the traditional economy, and the new digital monetary system, points of centralization can already be brought to light across the economic spectrum: convergence of mining operations, concentration of trading volumes, geographic clustering of nodes, accumulation of crypto ownership, crystallization of governance around undemocratic structures, elitist congregation of development efforts... you name it; strong tendencies to centralization have repeated consistently all along the young history of most blockchain projects. Hubs have emerged, whether they relate to the centralization of operations, the hoarding of assets, or the concentration of decision powers.

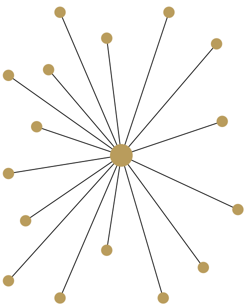
Even though DLTs were arguably designed to operate as distributed systems, they quickly morphed into decentralized systems instead. It is of the utmost importance here to try to understand if this process was due to exogenous or endogenous factors.

The question is actually twofold:
Have the projects derailed from their original libertarian vision due to inherent flaws in the way they were designed? Or, even more subversively, we could ask ourselves whether blockchain technologies are not actually more efficient as a decentralized system when articulated around strong hubs.

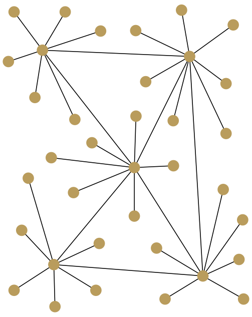
We will try to show that, especially when it comes to oraclizing or notarizing, centralization is a necessary condition for the system to operate efficiently and truly fulfill its disruptive potential. Refusing to accept this process may be what has been holding back smart contract technologies in the first place.

IIa. Endogenous factors to centralization – preferential attachment

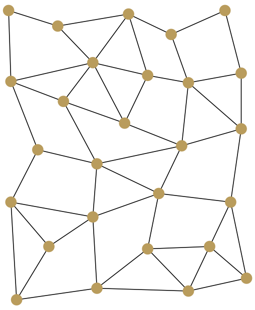
Consider the following infamous diagrams:



Centralized network



Decentralized network



Distributed network

There are indicators that the Bitcoin system is a "small world" network (as described by Watts and Strogatz (1998)) and converges to a scale-free network over time. The uprising of hubs in scale-free networks is inevitable and follows a well-documented power-law distribution. New nodes have a tendency to link to a node with a higher degree and not to a random node. This process is called preferential attachment.[3]

In simple words, following a rich-gets-richer process, big nodes tend to accumulate more links, and get bigger. This idea was introduced by Vilfredo Pareto[4] and it explained why a small percentage of the population earns most of the money.

Inherently, blockchain projects could not really be distributed if they are indeed scale-free networks. Let's study the dynamics at work here.

Currently, all blockchain consensus protocols have a challenging limitation : every fully participating node in the network must process every transaction and maintains a copy of the entire state, in the name of decentralization.

This process has been brilliantly explained by blockchain Engineer Preethi Kasireddy :

> *"While a decentralization consensus mechanism offers some critical benefits, such as fault tolerance, a strong guarantee of security, political neutrality, and authenticity, it comes at the cost of scalability. The number of transactions the blockchain can process can never exceed that of a single node that is participating in the network. In fact, the blockchain actually gets weaker as more nodes are added to its network because of the inter-node latency that logarithmically increases with every additional node."*
>
> **Preethi Kasireddy**

As a result, all public blockchain consensus protocols that operate in such a decentralized manner make the tradeoff between low transaction throughput and a high degree of centralization. In other words, as the size of the blockchain grows, the requirements for storage, bandwidth, and computing power required by fully participating in the network increases. At some point, it becomes unwieldy enough that it's only feasible for a few nodes to process a block–leading to the process of centralization.

[3] URL: https://en.wikipedia.org/wiki/Preferential_attachment

[4] URL: https://en.wikipedia.org/wiki/Vilfredo_Pareto

Many solutions to scaling have been considered by various projects, whether on-chain or off-chain scaling:

SegWit or lightening network for Bitcoin, increase of the block size for Bitcoin cash (which may arguably end up as an even more centralized network in the long run), off-chain scaling for Ardor, sharding for Ethereum, Plasma blockchain for project such as OmiseGo, modification of the distributed consensus mechanism on Maisafe.

There is little doubt that these efforts will yield impressive results medium term and will contribute to tackling the endogenous factors to centralization of digital ledger technologies. It might take time though, as development is operated in a trustless environment. Development and upgrades to the network shall not depend at any time on the intentions of any particular party, which could be arbitrarily malicious; carelessness could prove to be fatal to any project and ruin months of efforts.

IIb. Exogenous factors to centralization – capitalism and deflation

> *“It’s kind of funny because there’s such an obsession with creating a decentralized system. But, if you use a market-based mechanism to govern that system, obviously it’s going to centralize itself, you know? So, what’s the point? Why are you building a decentralized system in the first place?”*
>
> **Primavera De Filippi**

– MINING

Proof of Work incentive mechanism was designed in such a way that the network tends to amalgamate and assemble its participants. This inherent flaw is not simply associated with the technical scalability limitations mentioned earlier and listed as an endogenous factor. Centralization is also created by blockchain economics and markets rationalization.

Over time, any traditional blockchain-based network gets ruled by an increasingly oligopolistic market structure: as the mining difficulty grows, the associated block rewards decrease, settling the whole network economics into a highly deflationary, self-feeding spiral. Since the computational resources engaged by its participants to secure the network are increasing exponentially, hashing power gets concentrated within a few mining pools to increase the likelihood of sharing a block reward. Self-interests align in favor of their pool. Participants who would have originally distrusted each other now share the same economic interest, and unite to collectively control a larger share of the network hashing power - thereby making it more vulnerable to a 51% attack in the name of market efficiency.

Capitalism and elemental market forces have always proved more powerful than the original libertarian ideal. Despite a mathematically elegant design that does manage to bring together self-interested actors in the beginning, proof of work does not distribute incentive and consensus in a fair way in the long run. The distribution actually follows unregulated market laws, economic Darwinism in its ugliest form and ends up in a cartelization of the networks' resources.

To put it bluntly, miners, unlike nodes, are in it for the money, not for the ideology. How could it be otherwise since mining begets investments (hardware) and spawn bills (electricity) as the network grows?

- HOARDING

Further, as resources get scarcer and rewards are concentrated in the hands of early adopters, the possibility for new entrants to shake the existing dynamics at play gets considerably limited as time goes by. Within a deflationary economy, as the concentration of circulated money is greater than the expansion of the total monetary supply, the incentive to hoard grows stronger than the one to spend.

Since the crypto commodity is algorithmically bound to become scarce as the mining difficulty increases in time, adopters are likely to show a tendency to hoard, thus leading to spikes in prices as the supply gets even scarcer, bringing an even greater desire to accumulate from investors, speculators, or users.

Compared to the traditional economy, the wealth distribution pyramid in crypto currency is much more steep. A study of the block explorer and the bitcoin rich list, shows that over 95% of all bitcoins in circulation are owned by about 4% of the market. In fact, 1% of the addresses control half the entire market. According to a study[5] at block height 510160, about 0.00052% of bitcoin addresses own around 19.2% of all BTC.

[5] URL: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

Balance	Addresses	**%Addresses** (Total)	Coins	**%Coins** (Total)
0 - 0.001	13379144	**53.93%** (100%)	2,249 BTC	**0.01%** (100%)
0.001 - 0.01	5026854	**20.26%** (46.07%)	21,153 BTC	**0.13%** (99.99%)
0.01 - 0.1	4011996	**16.17%** (25.8%)	128,972 BTC	**0.77%** (99.86%)
0.1 - 1	1694421	**6.83%** (9.63%)	542,566 BTC	**3.23%** (99.09%)
1 - 10	545855	**2.2%** (2.8%)	1,444,050 BTC	**8.6%** (95.86%)
10 - 100	131730	**0.53%** (0.6%)	4,359,970 BTC	**25.95%** (87.27%)
100 - 1,000	15747	**0.06%** (0.07%)	3,728,212 BTC	**22.19%** (61.32%)
1K - 10K	1530	**0.01%** (0.01%)	3,351,588 BTC	**19.95%** (39.12%)
10K - 100K	109	**0%** (0%)	2,900,076 BTC	**17.26%** (19.18%)
100K - 1M	2	**0%** (0%)	321,428 BTC	**1.91%** (1.91%)

Bitcoin wealth distribution

In this context, the proposal by projects such as Ethereum to solve the scaling issue by migrating from proof of work to proof of stake could add unfairness to inequality and from an economic perspective discriminate further the late adopters. Arguably, it could crystalize the current situation that was inherited from endogenous technical flaws and heightened by exogenous market dynamics, eventually giving legitimacy to a sustainable but unfair economic status quo in the name of pseudo distributed security. In this model, the crypto rich then become a crypto caste.

As Kostakis & Bauwens summarized so clearly in their 2014 paper:

“Even a decentralized technology specifically designed to promote disintermediation and financial disruption can be unable to protect itself from the inherent tendencies of modern capitalist society to concentrate wealth and centralize power into the hands of a few.”

IIc. Necessary factors of centralization: trust, reputation and governance

It takes time to build trust. Trust accrues with time. Strong trust grows trust stronger just as the rich gets richer.

As explained succinctly above in sections a) and b), the current state of digital ledger technologies is not as decentralized as originally planned, whether for technical or economic reasons. With this perspective, it would be hypocritical for the crypto enthusiast to consistently vow for decentralization when in fact, blockchains have become all the more centralized as they turned more mainstream.

Our point here is to state that centralization could actually be an asset for the development of DLTs and not a hindrance. Especially on the service side of blockchains, where trust matters the most, central entities could be necessary for an efficient execution and smooth enforcement of smart contracts, adding a layer of reputation. We will study two use cases where centralization is an edge and not a drawback:

- ORACLIZING

The controversial role of oracles on the Ethereum protocol has been a major hurdle for a broader adoption as it reintroduces the need for a certifying third party to act as a trustworthy provider of reliable sources of information. In the absence of Artificial Intelligence which could help through neutral intermediation, smart contracts have not found their market yet (aside ICOs).

Since Blockchains cannot access data outside their network, they need trusted data feed – provided by third-party service, to trigger programmatically predefined algorithms and unlock the value held in the contract when certain pre-defined conditions are met. Besides, since oracles are not part of the blockchain consensus mechanism, the challenge here is not just to feed the smart contract with data in a secure confidential way, but also authenticate the data itself. As the execution of smart contracts is irreversible, the quality of data and the reputation of the oracle is of utter importance.

Take an example whereby the value held in a contract is conditional to a certain price of the EUR/USD cross. Even if you managed to populate the smart contract memory with Bloomberg data ticks through a secure dedicated channel, could you trust Bloomberg 100% with the live quality of its EUR/USD data feed?

The example above shows how dangerous it could be to rely on a third-party within the irrevocable world of blockchain and smart contracts, no matter how reputable your data provider is. Finding a consensus on different data-sources is a better way to go and provides extra reliability while still somehow using "centralized" data. Using an oracle network consensus instead of a single oracle reduces censorship, downtime, fraud and is less prone to error risk. However, it is cumbersome to implement, cannot be scaled and ultimately gives no guarantee of flawless data quality. A project like Gnosis, where the oracle function is centralized, strives to strike a balance between reputation and pseudo-anonymity but has not proved itself yet.

In this context, one can wonder whether a faultless, undisputable enforcement of smart contract execution could only be triggered by a state entity. What if it was in the interest of the decentralized network to give arbitrary oraclising power to a regulated institution, a notary or a magistrate with a view to protecting the involved parties and provide the highest guarantee of unbiased intermediation? Would it not be a paradox that as decentralized the blockchain can be, it may need a centralized entity or a trusted referee to trigger a smart contract? DLTs do work in a trustless environment, but it remains to be seen whether the same applies for smart contracts. Decentralization is what allows blockchains to substitute an army of computers for an army of accountants, investigators, and lawyers. However, a notary might still be needed in the context of smart contracts data validation.

- GOVERNANCE

"It is a tragedy indeed that new generations, taking office, attribute failures in governance to insufficient power, and seek more of it."

Mike Pence

Undoubtedly, there is a conflict between the libertarian vision of crypto projects and its governance structure which remains in most cases essentially despotic. The need for a leader with a vision has generally led adopters to place their trust in a widely undemocratic technocracy.

In a very centralized way, power is held by a circle of experts whose incontrovertible and unchallenged legitimacy is based on open source development and elitist co-optation. This process has been further strengthened by the fact that development is either extremely innovative and technically challenging, or impacts a large live network which could have serious consequences if poorly executed.

After all, co-optation was the method chosen by Satoshi himself, when he decided to move "to other things" in 2011, and delegated his control over the source code repository of the Bitcoin client to Gavin Andresen. Gavin replicated this method when he formed the *core developers* congregation by discretionarily electing Van der Laan, Maxwell, Garzik and Wuille. Ironically, three years into its birth, Bitcoin was already represented by a centralized profit driven organization.

With all due respect, Ethereum's founder Vitalik Buterin embodies even better the cult of personality crypto adopters typically bestow on star developers, as well as the limited accountability they request from them. Looking back at the DAO attack, which siphoned away almost 5% of the Ethereum in existence at that time, no blame can be given to the Ethereum protocol itself. However, the foundation and its politically-driven decision to hard fork will forever remain controversial. The reason why the blockchain was made immutable in the first place was to design a system resilient against human whims and corruption :

"code is law".

The vitriolic attack against Ethereum, on the Ethereum classic website frontpage is a state of the art critique of the centralized governance of most crypto projects :

"There are many problems that fester due to centralization and opaqueness ; corruption, unaccountability, nepotism, inefficiency and stagnation. Ultimately, centralization leads to fragility ; only decentralized systems can stand the test of time.

These problems can be only solved by adhering to governance systems that do not rely on a central point of failure. Just like distributed networks and the consensus protocol itself, we believe that only truly decentralized projects can survive in the long run.

Ethereum Classic manifests these values by relinquishing control by a formalized central foundation. The only hierarchy is that of transparent meritocracy and mutual reputation. No backroom deals or behind-closed-doors unilateral decision making ; just free and open discourse."

Ideology aside, the hard fork was considered the right move by most investors and the gap in valuation between ETC and ETH today reflects this reality, in favor of ETH. When one considers what it takes to reconcile the dream of a community to build an efficient decentralized system with the requirements of rigorous development, the centralization of decision power is sometimes a necessity.

IId. Conclusion : the necessity to centralize and regulate the oracle function

Historically, the evolution of crypto projects has shown a tendency to centralization :

- This process was driven by endogenous forces and inherent flaws in the retribution design of the proof of work algorithm protocol, independently of its technical soundness.
- This process was also driven by exogenous market forces and human nature which shows an unquenchable appetite to speculate, accumulate and hoard.
- Eventually this centralization process was unintentionally encouraged by the community itself and its developers, in the name of efficiency, reputation and best governance.

In light of the above, given the lack of internal arbitration mechanisms or external surveillance to preserve legitimate market dynamics, no crypto currency has ever managed to achieve a proper level of consumer protection and financial stability. Prices have therefore proved very volatile and equilibrium of forces at play were always temporary.

As smart contracts get deployed over public blockchains, a new layer of risk is added to the system. New powers are given to new actors ; Today oracles are granted the prerogatives of notaries in the digital world of DLTs.

When it comes to the validation of data within smart contracts, two approaches shall prevail:

- Oracles could to be subject to a decentralized reputation system where accurate reporting is incentivized in a trustless environment. (cf Augur's new whitepaper from February 2018[6])
- Oracles could be supervised by sanctioning bodies or regulators, but it requires:
    - trust in the sanctioning bodies
    - faultless notarization procedures.

Even though it is possible to decentralize the oracle function of a smart contract, and to handover the reporting and validation of data trustlessly on the basis of economically incentivizing the oracles for accurate reporting, a few problems remain:

1. If the incentive to be honest is small, or the data validation is considered as an administration task, the reliability of the reporter can be questioned in a system which does not use a centralized regulated oracle.
2. A continuous reputation attack leading to dispute forks is still theoretically possible in a decentralized system like Augur.

Even though centralization is not given much love in the blockchain universe, we have made a point in this chapter that it might actually sometimes be necessary and efficient. It is particularly true for the oraclizing and notarizing functions of a smart contract.

Similarly, the custody of assets needs centralization and regulation for maximum trust. It is simply impossible to decentralize the custody of hard assets in the real world. Hard assets are not digital money. They have to be stored securely. They are sometimes voluminous and need to be insured. A network of pawn shops for instance could serve as the backbone of a decentralized network of hard asset custodians, the same way regional banks have been custodying gold at the beginning of the last century before the Federal Reserve decided to take care of its custody at a national scale[7]. Let's consider a network of pawnbrokers: broadly decentralizing the safeguard of assets only diversifies the risk of the owner, but it does not protect against the potential corruption of any single malicious actor in the network.

[6] URL: https://www.augur.net/whitepaper.pdf

[7] The New Case For Gold by James Rickards

When hard assets are not granular or fungible, the problem becomes even more difficult to solve, because the assets cannot be fractioned, and the value/volume ratio increases, making the diversification into multiple custodians an even more strenuous effort.

The solution here is to recentralize the functions that need trust, so that blockchains as an environment of distributed trustless consensus gets more efficient.

The same way it seems wise and obvious to seek a state-own entity for the custody of hard assets, it might be worth considering handing over the oraclizing function in the Ethereum protocol to supervised financial intermediaries.

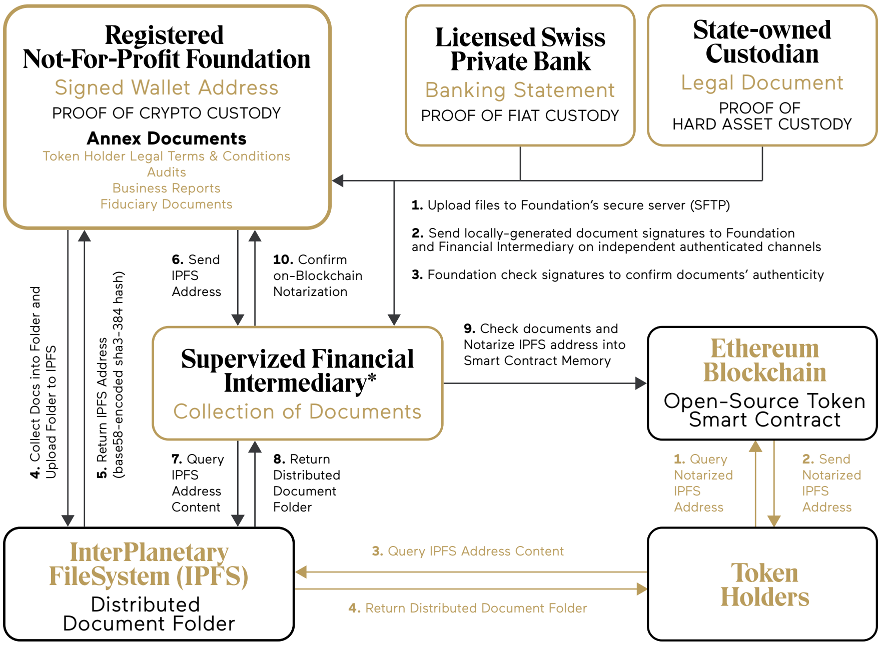
III. Necessary decentralisation. IPFS and asset-backed token economics

"Opportunity makes the thief [...] Power corrupts. Absolute power corrupts absolutely."

Lord Acton

IIIa. Description of the solution to tokenize and notarize tangible assets

Below is a flow chart reflecting how the process of a hard asset ICO should work, in regards to notarization and protection of the owner:


Registered Not-For-Profit Foundation
Signed Wallet Address
PROOF OF CRYPTO CUSTODY
Annex Documents
Token Holder Legal Terms & Conditions
Audits
Business Reports
Fiduciary Documents
Licensed Swiss Private Bank
Banking Statement
PROOF OF FIAT CUSTODY
State-owned Custodian
Legal Document
PROOF OF HARD ASSET CUSTODY
1. Upload files to Foundation's secure server (SFTP)
2. Send locally-generated document signatures to Foundation and Financial Intermediary on independent authenticated channels
3. Foundation check signatures to confirm documents' authenticity
4. Collect Docs into Folder and Upload Folder to IPFS
5. Return IPFS Address (base58-encoded sha3-384 hash)
6. Send IPFS Address
10. Confirm on-Blockchain Notarization
Supervized Financial Intermediary*
Collection of Documents
9. Check documents and Notarize IPFS address into Smart Contract Memory
Ethereum Blockchain
Open-Source Token Smart Contract
7. Query IPFS Address Content
8. Return Distributed Document Folder
1. Query Notarized IPFS Address
2. Send Notarized IPFS Address
InterPlanetary FileSystem (IPFS)
Distributed Document Folder
3. Query IPFS Address Content
4. Return Distributed Document Folder
Token Holders

Crypto/Fiat/Hard Asset **Notarization** and **Public Verification** Protocol

* The Financial Intermediary shall be supervised by a Self-Regulatory Organization.

As an example, the funds raised through the ICO will be employed to assemble a prestigious collection of tangible assets. At any moment in time, depending on the cycle of investment, the funds (i.e. the assets co-owned by the token holders) might be in the form of either cryptocurrency (ETH – by the time it takes to acquire the Collection, the funds will be kept in ETH), FIAT (CHF – during a very limited amount of time before acquiring a particular asset, the ETH will be converted in FIAT) or hard assets (wine, gems, cars… following the acquisition). In this context, the tokens holders shall have at any time a clear view of their assets. In this respect, the "proof of balance" related to each category of assets shall be available at any time for the token holders. The following set-up is for a Swiss-based ICO :

- A Not-For-Profit Foundation is in charge of managing the hard-asset collection on behalf of the co-owners of the assets ("Token Holders"). The foundation is contractually granted the discretionary mandate to :
    - Acquire the collection of tangible assets at the most competitive prices and through the toughest selectivity standards.
    - Sell the acquired assets to generate a profit and reinvest such profits in hard assets.
    - Promote the collection in the best interest of the community of owners.
    - Ensure fair treatment of each token holder with respect to the community as a whole.
    - Dispose of the funds whether crypto, fiat or tangible assets to fulfil the mission exposed above. This includes paying the collection managers, advisors, auditors and insurances with a goal to achieve self-sustainability on the long run.
    - Upload publicly (IPFS) all documents in relation to the collection with a view to providing full transparency around the funds (crypto, fiat, hard-assets) at all time.

- A Licensed Swiss Private Bank issues the banking statement related to any balance in cash being held in custody on behalf of token holders. Such a balance shall be kept very shortly to avoid being qualified as a "deposit under Swiss law". Any change in the cash balance of the token holders shall be publicly disclosed.

- Swiss Freeports act as the custodian of the hard assets. The Freeports issues a statement of custody and an extensive list of all the assets it safeguards.
- A financial intermediary affiliated to a Self-Regulatory Organization under Swiss law is in charge of pinning the IPFS folder to maintain persistency of the node and notarize the hash of IPFS folder address in the smart contract memory.

As explained in chapter 1, **centralizing the functions** of (i) custody and (ii) notarization is a necessary weakness in the context of hard-asset tokenization process. However, these functions are here split across four different supervised entities. The constant aim of this set up is to divide and arrange the several offices in such a manner as that each may be a check and balance on the other.

Further, the **decentralized functions** of the set up will now be detailed in the remainder of chapter 2.

They consist of (iii) using distributed technologies to maintain the persistency and public availability of the documents related to the collection as well as (iv) maintaining a public ledger of cryptographically secured property rights (ERC20 tokens) which can be used by their holders as tradable IOUs.

IIIb. The choice of IPFS as a storage layer over the insertion of data directly in the blockchain

> *"Blockchains are an extremely robust way of maintaining an immutable record of transactions; this is beyond dispute. At the same time, though, they make for lousy databases, only suitable for storing very small files and with read/write performance that is glacially slow. This means that only pointers to data, rather than the data itself, can realistically be stored in a blockchain.*
>
> *Blockchains are terrible as a mass storage container, so data still needs to be stored somewhere else, and that somewhere else still needs to be secured and persistent."*
>
> **David Irvine**

The objective of the foundation is to publicly display the various proofs of custody in a persistent, transparent, accessible and cost efficient way.

Since the appearance of Bitcoin, there have been many attempts to develop methods allowing anyone to leverage the immutability of the blockchain technology for purposes other than the transfer of currency.

The bitcoin protocol itself provides an opcode called OP_RETURN that lets the participants of the network to embed arbitrary data into the transactions they broadcast to the Bitcoin blockchain.

Originally OP_RETURN is a script opcode used to mark a transaction output as invalid. Since any outputs with OP_RETURN are provably unspendable, OP_RETURN outputs can be used to burn bitcoins. Using this loophole with a view to inserting data into the bitcoin blockchain has been controversial in the Bitcoin community. Many believe that Bitcoin was intended to provide a record for financial transactions, not a record for arbitrary data, especially so as the demand for external, massively-replicated data store is essentially infinite. Using the blockchain to store data was therefore officially judged irresponsible by bitcoin core developers. On the 19th of March 2014 they came out publicly about it[8] in Bitcoin Core release 0.9.0 :

> *“On OP_RETURN : There was been some confusion and misunderstanding in the community, regarding the OP_RETURN feature in 0.9 and data in the blockchain. This change is not an endorsement of storing data in the blockchain. The OP_RETURN change creates a provably-prunable output, to avoid data storage schemes – some of which were already deployed – that were storing arbitrary data such as images as forever-unspendable TX outputs, bloating bitcoin’s UTXO database.* ***Storing arbitrary data in the blockchain is still a bad idea ; it is less costly and far more efficient to store non-currency data elsewhere.”***

The first blockchain notary service to use this loophole was developed by Manuel Araoz and Esteban Ordano as an open source pro-

[8] URL: https://bitcoin.org/en/release/v0.9.0#opreturn-and-data-in-the-block-chain

ject and launched in 2013. They developed the concept of “Proof of Existence”.

The service allowed to store a timestamped cryptographic digest of a file in the blockchain, to let users prove they were in possession of the data without disclosing the data itself. The service is based on a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, that is, a function which is infeasible to invert.

Bruce Schneier has called one-way hash functions «the workhorses of modern cryptography». To put it in simpler words, the hash is a cryptographic fingerprint that is unique to a document, and that document only. The tiniest single change to the document changes the hash completely.

The proof of existence protocol imagined by Araoz and Ordano let anyone confirm the document’s existence at the timestamped time by :

- Calculating the document’s SHA256 digest
- Finding a transaction in the bitcoin blockchain containing an OP_RETURN output with the document’s hash prepended by the service’s marker bytes (which are 0x444f4350524f4f46 or ‘DOCPROOF’ in ascii.)

If the block time minus the block time variation is at most the time the document is claimed to have existed, the claim is valid.

The system is ingenious but unfortunately it does not let anyone access the data itself in a transparent and open way. Only someone already in possession of the data can check its authenticity and original timestamp. Other services like Stampery or Tierion have been making use of the Bitcoin blockchain to timestamp and verify data but, so far, the proof of existence has focused on ways to prove the ownership of a document without disclosing it to the world.

The problem is, the not-for-profit foundation does want to disclose legal documents publicly, to let token holders access the full details of the collection.

A beginning of a solution to this problem could be found in the Stampery whitepaper[9] , in the way of Merkle trees :

[9] URL: https://s3.amazonaws.com/stampery-cdn/docs/Stampery-BTA-v6-whitepaper.pdf

> *"Many single hashes corresponding to different pieces of data or files can be compiled into a single hash by building a binary tree in which every leaf node is populated with each of the hashes while every non-leaf node is populated with the hash of the merger of its child nodes. This type of tree is commonly known as Merkle tree. The tip node in the tree—the hash resulting from aggregation of all the hashes in the leafs—is called Merkle root or simply root. By aggregating multiple hashes into a Merkle tree and then publishing only the root, it is possible to anchor large volumes of data in a blockchain with a single transaction, which dramatically reduces costs and avoids the aforementioned bottlenecks."*

However, storing a large amount of data in the blockchain is still prohibitively expensive.

As the bitcoin value has moved to the upside, broadcasting a transaction containing a single OP_RETURN with a certain guarantee that it will be written into the next block and confirmed nearly immediately has increased accordingly. Bulk timestamping of hundreds or thousands of files and anchoring their hashes in the blockchain renders the OP_RETURN method unsuitable in terms of cost.

In a slightly different way, including data in a transaction on the Ethereum protocol works by sending a message call which allows the user to interact with other accounts or smart contracts without having to create their own contract. As anyone can guess, a message call costs gas, but the cost does not just depend on how big the data is but also how complex it is.

A fascinating medium post by Jamila Omaar (Forever Isn't Free: The Cost of Storage on a Blockchain Database)[10] compares the cost of storing 1GB of data on several public blockchain:

- Bitcoin: As of July 2017 the median Bitcoin transaction fee was about $1.82 1GB would need 12,500,000 OP_RETURN messages so would cost approximately $22,766,250.

[10] URL: https://medium.com/ipdb-blog/forever-isnt-free-the-cost-of-storage-on-a-blockchain-database-59003f63e01

- Ethereum: The cost to store data on Ethereum works out to approximately 17,500 ETH/GB, or around $4,672,500 at the same date.

The emergence of crypto projects like Factom or NEM (New Economic Movement) and its apostille system has brought new solutions to the notarization issue, but these projects have failed so far to gain momentum or mainstream adoption within the crypto community.

Besides, the creation of the Ethereum Virtual Machine (EVM) has provided another solution to notarization. Since the EVM is turing-complete, it offers a more expressive and complete language for scripting, and allows to insert data directly at a smart contract level.

EVM can indeed encode any computation that can be conceivably carried out, including infinite loops.

The owner of a smart contract can notarize documents by inserting hashes recursively and directly into the memory of the smart contract.

Further, as Solidity supports maps, bulk inserting of hashes is actually more cost efficient than a message call, but still too expensive for the mass storage of data, and especially cumbersome for the storage of documents specifically.

Not a good solution for our not-for-profit foundation.

In 2014, Juan Benet designed **the InterPlanetary File System (IPFS)**[11]. He took the Bitcoin blockchain protocol and network infrastructure as a model to offer a new decentralized persistent storage solution.

Like Bitcoin, IPFS has no single point of failure, and nodes do not need to trust each other (except for every node they are connected to).

At its core, IPFS is a versioned file system that can store files, manage them, tracks versions over time and remove duplicates. IPFS also accounts for how those files move across the network so with this perspective it can be considered a distributed file system, often compared to a single bittorrent swarm exchanging git objects. Being able to ask to be connected to whoever is closest that can provide a particular file is a much more resilient and useful

[11] URL: https://ipfs.io/

way to propagate content on the network than HTTP, and also provides higher-throughput.

Content flows naturally from computer to computer, peer-to-peer, as efficiently and robustly as possible, without depending on centralized services. Besides the possibility to identify content and fetch it is integrated natively, and the removal of duplicated content improves the security and resilience of the network dramatically, saving bandwidth and preventing DDoS attacks.

Any file on the network is hashed cryptographically, so instead of referring to the objects itself, IPFS refers to everything by the hash of the file. The content determines the address. Object are not referred to by their location but instead by their unique cryptographic representation, preventing other files to be represented as the same address.

The totality of IPFS objects forms a cryptographically authenticated data structure known as a Merkle directed acyclic graph (DAG) as explained in Benet's whitepaper.

An interesting point here is the distinction between storing data on the blockchain and storing hashes of data on the blockchain[12]. On the Ethereum platform you pay a rather large fee for storing data in the associated state database, in order to minimize bloat of the state database ("blockchain bloat"). Thus it's a common design pattern for larger pieces of data to store not the data itself but an IPFS hash of the data in the state database.

If the blockchain with its associated state database is already represented in IPFS then the distinction between storing a hash on the blockchain and storing the data on the blockchain becomes somewhat blurred, since everything is stored in IPFS anyway, and the hash of the block only needs the hash of the state database. In this case if someone has stored an IPFS link in the blockchain we can seamlessly follow this link to access the data as if the data was stored in the blockchain itself.

IPFS and the Blockchain are a perfect match. The Foundation can address large amounts of data with IPFS, and place the immutable, permanent IPFS links into a blockchain transaction. This will help timestamping and securing the content, without having to put the data on the chain itself. Such an approach has been adopted by Digix to proof-of-asset gold[13].

[12] URL: https://medium.com/@ConsenSys/an-introduction-to-ipfs-9bba4860abd0

[13] URL: https://digix.global/

If the collection of non-fungible assets is listed extensively and transparently in an IPFS folder whose hash is freely available for consultancy and inserted in the smart contract, we can expect the token to price the collection efficiently and dynamically.

IIIc. Tokens economics of a revolving ICO

Benefiting from the Ethereum blockchain capabilities, tokens allow to endow the (co-)ownership of a hard asset (or hard asset collection) with the following features:

- granularity
- fungibility
- liquidity
- ease of exchange
- storing safety
- provability of ownership

The above features are common to most tokens running on the Ethereum blockchain.

However, a feature that has never been explored before is the possibility to use the token as a valuation instrument for non-fungible assets. Projects like Bilur[14] or Digix have already envisioned the possibility to tokenize a fungible commodity, whether oil or gold. However, no project before has addressed tokenization of non-fungible assets. The reasons may have to do with the difficulty to find a sound custodian, as well as the expertise required to source and assemble the collection at a decent price given the liquidity constraints behind non-fungible assets. As detailed within their respective whitepaper, token projects such as WINE, GEM, CAR have already put together a team of worldwide renowned experts in their field to establish a plan for sourcing and managing the collection, thereby tackling the last challenge on the way to tokenize prestigious tangible assets listed in the Knight Frank Luxury Investment Index.

If the assets of the collection are extensively and transparently exposed on the blockchain through our notarization process, then the token's market capitalization is supposed to match the nominal value of the collection accurately, based on market efficiency dynamics[15]. In the case of non-fungible assets like fine arts, high-end gemstone, collectible cars, precious wines, we could argue

[14] URL: https://www.bilurmarket.com/home

[15] Market efficiency refers to the degree to which stock prices and other securities prices reflect all available, relevant information.
URL: https://www.investopedia.com/terms/m/marketefficiency.asp

that the token monetary supply priced at the token market rate is not a just a mirror of the nominal liquidation value of the collection; it represents the most accurate value of the collection at any time. **The token price gives a value to the collection, and not the other way around.** This is a major difference with traditional hedge funds of hard assets which generally rely of centralized entities like auction houses to sporadically determine the NAV price. The same way a company share's price ultimately determines its total capitalization, decentralized ownership through distributed ledger technologies allow for distributed consensus on asset price, not just on ownership.

Since the tokens are granular, fungible, liquid and easy to exchange, a real price discovery mechanism will dynamically permit a frictionless valuation of the collection. No central entity will arbitrarily decide on an estimated price for the collection. Only buyers and sellers showing their interest OTC or through the order book of a listed exchange will continuously express their estimation of the collection price. Arbitrageurs will ensure that the collection is accurately valued, by taking priced-in discounts or premium opportunities to their advantage and reducing any misprice according to their own valuation of the intrinsic value of the collection. The token becomes an instrument which inherently bears value. Besides, the token cannot be considered a derivative as its monetary supply always corresponds to the assets in custody and no further monetary printing is undertaken without a 1-to-1 hard-asset backing.

In this context, a token holder liquidating his co-ownership of the collection does not precipitate the liquidation of an equivalent nominal value of the collection, since the ownership is just transferred to another token holder, at a discount price if necessary. A token holder willing to exit his position and transfer his ownership in a hurry will only harm himself as he will have to temporarily weigh on the bid price to find enough buyers willing to enter at a preferential price. The implicit market value of the collection might go down for a short period of time. Meanwhile, the liquidation value of the collection will stay unscathed, which should encourage arbitrageurs to quickly step in, realigning the token price on par with the underlying value.

In this model, there is no liquidation of ownership, only transfer of ownership ; no redemption of tokens, only exchange of token. Liquidation at an individual level will not trigger liquidation at collective level since the not-for-profit foundation is self-sustained and acts on behalf of the community of co-owners, with a view to preserving their best interests.

Unlike traditional hard-asset hedge funds, the foundation does not offer a possibility to redeem the ownership in fiat. Indeed, the token can be freely exchanged against other cryptocurrencies and eventually against fiat, so the liquidity of the Property right (token) is fully decoupled from liquidity around the underlying assets constituting this Property (the collection). It is the sole responsibility of token holders to exchange their token in fiat to crypto exchange should they want to redeem their ownership. This might prove easier to them than within the current hedge fund model as they will not depend on a centralized entity to provide them with liquidity, and they can exchange peer-to-peer on the blockchain, without financial intermediation. Liquidity is added to the market through high granularity (divisibility to the 18th decimal), decentralization at a global scale and ease of exchange as the potential number of market participants should be substantially higher than what we see today in markets for illiquid assets.

This set up will help address the recurring problem of funds struggling to find sufficient cash to meet withdrawals, in case of a market downturn[16].

If the collection is strategically built to scrupulously represent its asset class in all its diversity, then the token price may *de facto* becomes the benchmark price of the asset class itself, as non-fungible assets are securitized into fungible tokens.

Asset tokens are an excellent use case for blockchain technology but are generally not as popular among investors because the value of the tokens does usually not exceed the value of the asset and thus have less upside potential than other types of tokens.

However, given the lack of transparent stable coins in the crypto market at the time of this writing, and the scarce alternative for crypto investors to find reasonable store of value and hedge against volatility, the tokenization of prestigious non-fungible hard asset could be perceived as a real progress.

Further, reducing the friction to trade could also attract to the blockchain investors who were only versed in the asset class itself so far. More market participants means more volume, smaller spreads, and less price impact. As explained by Stephen McKeon[17], liquidity is not binary, it is a continuum. Illiquid does not necessarily mean “unable to trade,” it means “costly to trade.” If trading a hard asset is more expensive in physical form than in token form, “traditional assets will tokenize because they will lose the liquidity premium if they don’t.”

[16] URL: https://www.ft.com/content/0117463e-ceab-11e2-ae25-00144feab7de
Regulator suspends redemptions from Nobles Crus wine fund.

[17] URL: https://hackernoon.com/traditional-asset-tokenization-b8a59585a7e0

The objective of our HARICOs is to remain inflation-neutral and increase the monetary supply on a revolving basis as tangible assets are added in custody following a no-leverage no-dilution economic model. The system would work in a very similar pattern to Tether[18], a cryptocurrency pegged to the US dollar, although it would provide complete transparency to the token holders as per what they actually own.

In this context, a WINE, GEM or CAR token are units of value as much as they represent a proof of digital ownership. They carry their value for their entire lifetime, the same as a dollar or a poker chip. The main difference is that they cannot be deemed obsolete as a result of the decision of a central entity (eg : a central bank changing paynotes or a casino closing its doors), since they exist on a substrate that ensures their security and validity ; they run on a decentralized network.

Besides, they are more advanced from a technological standpoint than colored coins (eg Omni protocol). The smart contract ensures that each token corresponds to the thing it represents and keep track of which tokens are in circulation. The not-for-profit foundation is legally and contractually bound to mint only insofar as corresponding assets are custodied at a separate state-own entity. No kingly right is granted to the foundation as regards to the control of the tokens on the secondary market. Upon minting, tokens are free for exchange and their value is tied to the liquidation value of the collection thanks to market efficiency provided at a smart contract level.

Given that the demand for hard assets is virtually unlimited, our hard-asset ICOs will virtually provide an unlimited supply of tokens as long as the monetary supply corresponds at any point in time to hard assets added to the custody. Therefore, the stability of our token will not depend on the economic health of a specific country ; its stability will be dynamically assessed in relation to the steadiness of the corresponding hard assets value relatively to the purchasing power of the token holder within its currency zone.

With this perspective, our asset-backed tokens may be coined as the firsts in a series of "international stablecoins" and may one day be a bridge to future government-issued cryptocurrencies. Instead of paying in EUR, USD or JPY, one can imagine paying in WINE, CAR, GEM or ART unit of value during a travel abroad, while preserving their purchasing power and protecting themselves against the typical crypto or forex volatility. The hard-asset IOU shall then become

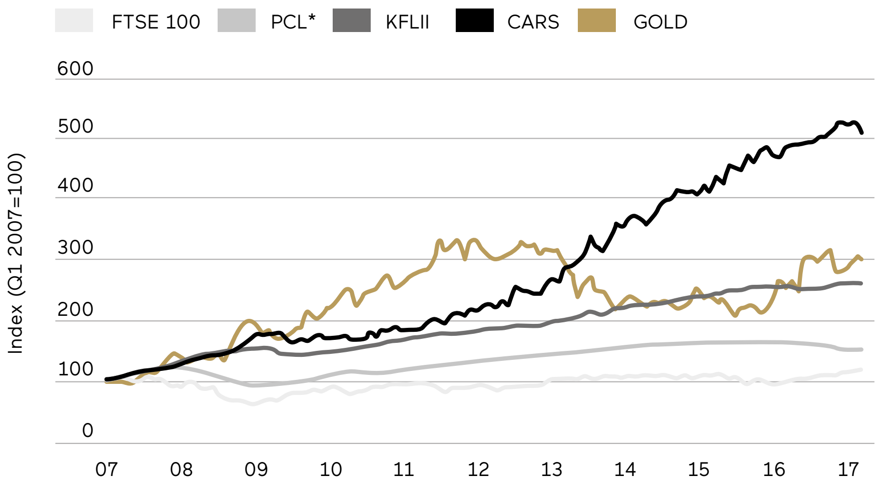
[18] URL: https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf

an actual currency – tradable, fungible and disintermediated - despite representing the ownership over unique, non-liquid items.

The HARICO economics turns out to be all the more interesting as these prestigious hard assets are deflationary by nature and tend to increase in value against fiat over time, as the next figure shows. Our tokens could therefore be classified as a moderately deflationary currency in value terms, inflationary in supply terms.

It shall be noted than in the current low rate environment, the initial quotation of the token might show a premium compared to the underlying assets during a sustained period of time, as market participant could have an interest to invest early to capture future returns. They would typically try to calculate the expected returns based on a guestimate rate of return in the hard asset and the risk free rate, essentially taking into consideration that the token pays no dividend as the foundation will reinvest the profits with a view to expanding the collection without inflating the token supply.

KFLII performance versus other asset classes (to Q1 2017)



Fractionalizing ownership of prestigious luxury asset should not neutralize their scarcity appeal. Additional round of money printing – revolving ICOs – will be conducted on a one-to-one reserve ratio between the issued currency token and its associated physical asset value added to the custody at the time of the mintage. The not-for-profit foundation will not just maintain price parity between tokens in circulation and the underlying hard assets held in custody, it will account for the accrued increase in value of assets held in custody so far. After the initial offering, tokens shall be issued a drop at a time, as demand for the assets to the foundation triggers the need and the means to acquire more assets.

* Knight Frank Prime Central London Residential Index. **Source:** Knight Frank Research

After the initial subscription period, when the collection has been acquired, other rounds of coin offering can be envisioned. In the long run, the foundation's wallet could be kept alive and open to sustain revolving coin offerings, should Swiss regulators approve of this innovative operational set up. In this context, AML will be conducted by the a regulated financial intermediary on a continuous basis. A small fee might be granted to the intermediary for supervising this task, as well as to the not-for-profit foundation for maintaining its operations, pay for auditors and employees as explained in the respective WINE, GEM and CAR whitepapers.

Lastly, the stable nature of our HARICOs is not only relevant from a fiat perspective but also crypto-wise. As explained by Pablo Eder[19]:

"The most exciting use of a stable token is to act as a reserve currency in case something drastic happens in a cryptocurrency ecosystem that requires a relatively non-volatile token. For example, if one were to implement a loan in a smart contract in Ethereum, one could technically insure this loan with a stable token. The mechanism of insurance is as follows: if the loaner does not repay in time, the interest can still be calculated based off of a relatively stable store of value. This allows us to use the decentralized nature of Ethereum to automate transactions instead of it going through a bank while still maintaining the ability to insure such a loan."

Cryptocurrency might become more widespread as a mean to transact peer-to-peer when the possibility to efficiently store value in this market can eventually be considered, without suffering the traditional volatility associated with crypto investing.

The emergence of stablecoin and tokenization of assets has only just begun.

"What makes tokens unique is their ability to trade cheaply and securely on the blockchain, without an intermediary or escrow service. This is the fundamental difference that will not just

[19] URL: https://www.linkedin.com/pulse/crash-course-stable-tokens-pablo-eder/

enable a niche of blockchain-based tokens but will replace most of our existing digital tokens with blockchain-based versions that are more secure and more efficient. You can call them tokens today, but in a few years we'll just call them dollars, tickets, reservations, stock shares, loans, physical asset. In twenty years, almost all of the physical or digital tokens we have now may simply exist on a shared ledger with far fewer intermediaries than we have today.[...]

Tokens that represent ownership of unique items are going to change their markets. Everything from land to art to jewelry to homes to cars, boats, and even memberships will become tradable tokens, leading to massive disintermediation, far more liquidity, and entirely new systems for managing these assets. Fractionalizing ownership of unique things will create new financial instruments, derivatives, and other products."

David Siegel

IV. The smart contract

Within the exposed perspective to securitize non-conventional assets, our framework enables virtualizing a hard asset collection into tokenized shares governed by both a central authority and a public smart contract on the decentralized Ethereum blockchain.

The role of the central authority is twofold:

- synchronize the token supply with the co-owners' monetary investments by minting or burning tokens in order to fulfill the revolving nature of the HARICO
- notarize all the real-world documents certifying the collection value by securely updating their cryptographic signature into the Ethereum distributed ledger

In this section, more targeted to developers and code-friendly readers, we present some technical features of our smart contract. At the time of writing this yellow paper, the language used is solidity version 0.4.19.

IVa. EIP 20 compatibility

The virtual assets underlying the hard asset collection are tokens on the Ethereum blockchain[20]. They are compatible with the ERC-20 standard[21] to ease integration with exchange platforms and other contracts. In particular the following variables and functions are implemented:

```
uint256 public totalSupply;

mapping (address => uint256) public balanceOf;

mapping (address => mapping (address => uint256))
public allowance;

function transfer(address _to, uint256 _value) public;

function transferFrom(address _from, address _to,
uint256 _value)
public returns (bool success);

function approve(address _spender, uint256 _value)
public returns (bool success);

function approveAndCall(address _spender,
uint256 _value, bytes _extraData) public returns
(bool success);
```

As one can infer, a token holder can transfer tokens to an arbitrary Ethereum address by calling the transfer function of the contract and signing the transaction with the corresponding private key. It is also possible to send to an address an authorization to later withdraw tokens by combining the approve and transferFrom functions.

Nevertheless ERC-20 token standard suffers a number of issues, including the potential to get tokens irreversibly locked inside a contract. Therefore improvements are being proposed by the community, such as EIP 223[22] or EIP 777[23]. It is not impossible that future HARICO smart contracts rely on a future ERC-777 standard.

[20] URL: https://www.ethereum.org/token

[21] URL: https://theethereum.wiki/w/index.php/ERC20_Token_Standard

IVb. Control of the market token supply

The digital central authority within our framework is the contract owner, which is initially the contract creator (the address which has signed the transaction deploying the smart contract on the Ethereum network). The contract features modifiers whitelisting exclusively authorized addresses to perform certain functions. This is the case for the mint and burn functions to create or destroy new tokens, which are in the like of :

```
/**
  * @notice Create `_value` tokens and send it to `_target`
  * @param _target Address to receive the tokens
  * @param _value the amount of tokens it will receive
  */
    function mint(address _target, uint256 _value)
    onlyGovernor public returns (bool success) {
        balanceOf[_target] = add(balanceOf[_target], _value);
        totalSupply = add(totalSupply, _value);
        Transfer(0, _target, _value);
        Mint(this, _target, _value);
        return true;
  }

/**
  * @notice Destroys `_value` tokens from sender's account
  * @param _value the amount of tokens to burn
  */
    function burn(uint256 _value) onlyGovernor public
    returns (bool success) {
        require(balanceOf[msg.sender] >= _value);
        balanceOf[msg.sender] = sub(balanceOf[msg.sender],
        _value);
        totalSupply = sub(totalSupply, _value);
        Transfer(msg.sender, 0, _value);
        Burn(msg.sender, _value);
        return true;
  }
```

Only the accredited *governor* address can successfully call those functions. It can be seen that the burn function doesn't allow a token holder to directly destroy his own token (although nothing would prevent him to send tokens to a burn address; however, in the latter case the totalSupply variable remains unaffected). Note

[22] URL: https://github.com/ethereum/EIPs/issues/223

[23] URL: https://github.com/ethereum/EIPs/issues/777

that according to the legal rules underlying the HARICO mechanism, the burn function is never used in practice, except if the Foundation responsible for the hard assets has to be dissolved, and the collection liquidated. In this scenario, the collection should be put to auction, and the proceeds of the sale converted back to Ethereum. Ethereum will be then sent to token holders, proportionally to their stake upon reception of their token by the foundation. Token will be burnt by the foundation and the foundation will be disbarred.

IVc. Notarization functionalities

As announced previously, a user with special credentials, the contract notary, has–exclusively–the capability to oraclize into the smart contract memory the IPFS hash pointing to the relevant address on the IPFS network.

```
string public notarizedIpfsHash = ‘’;

// notarization: write input hash into smart contract
   memory (transactional function)
   function writeNotarizedIpfsHash (string _hash)
   public onlyNotary returns (bool) {
        notarizedIpfsHash=_hash;
        Notarize(_hash);
        return true;
    }

// notarization: read smart contract memory
    (constant function)
    function readNotarizedIpfsHash() public constant returns
    (string) {
        return notarizedIpfsHash;
    }

// notarization: check input hash against smart contract
   memory (constant function)
   function checkNotarizedIpfsHash(string _hash)
   public constant returns (bool) {
        return cmpStrings(_hash, notarizedIpfsHash);
    }
```

The token holder is able to read to notarized address directly from the blockchain by calling the readNotarizedIpfsHash function or to check it against their own hash with the checkNotarizedIpfsHash method.

IVd. Transparency and Security

The contracts feature three types of accredited callers.

- The governor is the only user able to mint and burn token.
- The notary is the only user able to notarize the asset IPFS address.
- The owner is the only user able to initialize and update the accredited addresses.

Some safety measures have been taken regarding the execution of mathematical operations on the EVM. A SafeMath contract (inspired by both OpenZeppelin SafeMath library[24] and Dappsys DSMath contract[25]) ensures in particular that uint256 calculations overflowing the data type trigger a throw, as overflows can result in unpleasant consequences[26].

The full version of our smart contract will be audited by a dedicated external team before deployment, in particular the security risks will be assessed. The conclusions of the audit will be made public information.

The smart contract will be completely open source. Everyone will be able to compile it on their own and check the resulting byte code against the blockchain to ensure that the code announced is indeed the code executed.

As encoded in the smart contract in an immutable way, the tokens are exposed completely transparently on the ledger. Every minting or burning process is logged to blockchain clients. Every token transfer is logged to blockchain clients. As a consequence, all the balances of all the accounts detaining tokens can be publicly known, as well as the total supply on the market.

All in all, the panoptical nature of the framework ensures the token holders of the faithful knowledge of both the token distribution and the hard asset collection value at all times.

[24] URL: https://openzeppelin.org/api/docs/math_SafeMath.html

[25] URL: https://dapp.tools/dappsys/ds-math.html

[26] URL: https://en.bitcoin.it/wiki/Value_overflow_incident

V. The Conclusion

To summarize this yellow paper, the Hard-Asset Revolving ICO (HARICO) framework aims to achieve several entangled purposes.

Tokenization technology enables on-blockchain securitization of prestigious hard assets and grants distributed ownership to asset token holders. Not only it significantly lowers the barriers to enter exclusive hard-asset markets, it also triggers the technical possibility to trade fractions of non-fungible assets in a disintermediated and frictionless way.

The public nature of the blockchain allows token holders to access all the notarized documents certifying the content of the hard-asset collection as well as the token supply by querying the immutable token smart contract. This unambiguous design sets an unprecedented transparency standard and ensures fair and symmetric information to everyone in the perspective of a market-efficient pricing of the token. This openness is reinforced by the legal ICO framework set up by the Swiss regulatory body as it addresses the issue of legal accountability.

Finally, in these uncertain times it is worthwhile noticing that HARICOs might layout foundations to a manifold of asset-backed tokens which may be used as hedges against inflation, deflation, devaluation, and volatility, as they would be much less exposed to short and long-term market fluctuations than currencies and most of current financial instruments. The case for a stable coin mechanism is probably not the last exciting potentiality deriving from the upcoming real-life implementation of HARICOs.

“We believe that the most beautiful things in this world should belong to everyone and not just a few beautiful rich people”.

The ICO team at Altcoinomy.com

VI. Legal notice

INVESTING IN CRYPTOCURRENCIES AND OR TOKENS INVOLVES SIGNIFICANT RISK OF LOSS AND MAY NOT BE SUITABLE FOR ALL INVESTORS. INVESTORS COULD SUSTAIN A LOSS OF SOME OR ALL OF THE INITIAL INVESTMENT. INVESTORS SHOULD BE AWARE OF ALL THE RISKS ASSOCIATED WITH CRYPTO INVESTING AND THE BLOCKCHAIN TECHNOLOGY (INCLUDING AMONG OTHERS LEGAL AND REGULATORY RISKS, TECHNOLOGY RISKS, CYBERSECURITY RISKS AND OPERATIONAL RISKS) AND SEEK ADVICE FROM AN INDEPENDENT FINANCIAL ADVISOR.

This document is not oriented for and shall not be distributed to persons belonging to jurisdictions in which – due to the nationality of the person, their residence or other reasons – access to this document, consultation or availability are restricted or prohibited. Moreover, the token sale is strictly limited to people who are not citizens or residents of countries where such sale is forbidden. In this context, the following countries - and any jurisdiction into which such sale or distribution is unlawful - are excluded from the token sale: The United States (including its territories and dependencies, any state of the United States and the District of Columbia), Afghanistan, Angola, Aruba, Australia, Bangladesh, Belarus, Benin, Bhutan, Bolivia, Botswana, Brunei Darussalam, British Indian Ocean Territory, Burundi, Burkina Faso, Bosnia, Burundi, Cambodia, Cameroon, Canada, Cape Verde, Central Africa republic, Chad, Comorros, Congo, Congo Democratic republic, Cuba, Cote d'Ivoire, Djibouti, Dominica, Ecuador, El Salvador, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Guatemala, Guyana, Guinea, Guinea Bissau, Haiti, Honduras, Iran, Iraq, Ivory Coast, Japan, Jordan, Kenya, Kyrgyz Republic, Laos People's Republic, Lebanon, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Micronesia, Moldova, Mongolia, Mozambique, Myanmar, Nauru, Nepal, New Caledonia, Nicaragua, Niger, Nigeria, Niue, North Korea, Oman, Pakistan, Palestinian Areas, Papua New Guinea, People's Republic of China, Reunion, Rwanda, Samoa, Sao Tome and Principe, Senegal, Sierra Leone, Somalia, South Georgia, South Korea, Serbia, Sudan, Sri Lanka, Suriname, Syria, Swaziland, Tajikistan, Tanzania, Timor, Togo, Tonga, Trinidad and Tobago, Tunisia, Turkmenistan, Uganda, Ukraine, Uzbekistan, Vanuatu, Venezuela, Western Sahara, Yemen, Zambia, Zimbabwe.

This document is provided for information purposes only. It is not binding and is of descriptive nature only. It does not purport to be exhaustive and may be modified from time to time without prior notice. Any scenario analysis is based upon assumptions and do not constitute any representation or warranty. No information, opinions or other matter contained in this document shall be interpreted as investment, legal or tax advice. The content, information and materials contained in this document is provided « as is » and « as available », without any representations or warranties of any kind. This document is not a prospectus within the meaning of articles 1156 and 652a of the Swiss Code of Obligations or a prospectus under any other applicable laws. The information contained in this document shall not constitute an offer to sell or the solicitation of an offer to buy, in any jurisdiction in which such offer or solicitation would be unlawful prior to registration, exemption from registration or qualification under the securities laws of any jurisdiction.

TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT, SHALL ALTCOINOMY SA OR ANY OF ITS DIRECTORS, EMPLOYEES, CONTRACTORS, SERVICE PROVIDERS OR AGENTS HAVE ANY LIABILITY WHATSOEVER TO ANY PERSON FOR ANY DIRECT OR INDIRECT LOSS, LIABILITY, COST, CLAIM EXPENSE OR DAMAGE OF ANY KIND, WHETHER IN CONTRACT OR IN TORT, INCLUDING NEGLIGENCE, RELATED TO THE USE OF THIS DOCUMENT.

Altcoinomy SA retains all right, title and interest (including copyrights, trademarks, patents, as well as any other intellectual property or other right) in all information and content (including all text, data, graphics and logos) on this document and on any single section, part or page comprised in this document. The content of this document is to be considered as one and must be read in full and no section or page may be separated or read or considered separately. The full content is indivisible, especially the legal notice which is an integral part of this document.