Ascension Project

White Paper, v. 1.9.1
29th December 2017

Kevin Wilkerson
Sean Daley
Jim Davidson, editor

Abstract

The history of Bitcoin and blockchain technology is reviewed, keeping in mind the goal Satoshi identified at the outset: to create a private, censorship-resistant, non-state currency which can be utilized as the nucleus of a larger ecosystem. This paper identifies 15 significant issues impeding the realization of that goal. Several information theory and computer science rules and experiences are examined to discern necessary elements in a set of economic technologies that would meet that goal. Fundamental issues in scalability and decentralization are considered, with reference to current legacy systems.

We then examine Ascension, a set of technologies residing above the blockchain that have worked together since 2011, designed at the end of the digital gold era in 2008. These solutions provide full scalability; untraceability; transaction speeds in seconds; distributed functionality with controllable software updates; independent issuance of monetary instruments with independent monetary and reserve policies among private issuers; a lightweight client architecture; local-only private keys giving access to only that user's transactions; transaction records are only seen by sender and receiver, can be permanently deleted, and are stored in the user's wallet only at the option of the user; using XMPP provides innate encryption and inherent intra-community messaging; individually owned and operated exchanges and marketplace businesses foster decentralization as the ecosystem grows.

We then examine the Ascension blockchain layer, which is permissioned to reduce or eliminate dust spam DDoS, bogus spends, nearly-empty block mining, and other bad behaviours; employs decentralized contracted mining to provide censorship resistance and impose obligatory software updates; smart contracts are published only as approved by Ascension. In regard to the Ascension Foundation, we then consider monetary engineering policies to match real-time economic situations; various revenue sources including a coin sale; and an in-depth review of legal challenges and obstacles.

The development roadmap and model for use of funds are then discussed. Ascension has a highly experienced team with long track records in digital currencies, but not just in digital currencies alone. Our wallet design already supports multiple assets, already has an operational escrow-enabled exchange, and already has a functioning marketplace app. There is also a sandbox for testing with test currencies. Our goals have been to hide complexity from users; make wallets reasonably hack-proof;

minimize and compartmentalize the damage a hostile party can do even as an insider; make network eavesdropping very difficult and not rewarding; make wallets friendlier with human readable addresses, lost credential recovery features, and user control of transaction history; lighten the footprint of blockchain clients so that wallets can be accessed safely on any device (even devices not belonging to the wallet's owner); anticipate and circumvent potential protocol blocking and national firewalls during any future crackdown on cryptocurrencies. Plans for future clients and the API are also discussed.

Ascension is a next-generation cryptocurrency system aimed at expanding the crypto-economy of the future. Our mission statement is: “To promote the growth of robust, borderless, wealth generating, free market ecosystems.”

Table of Contents

I. Introduction

It has been just over nine years since the Bitcoin white paper *(1)* was published by Satoshi Nakamoto *(2)* in October 2008. This paper led to the debut of the Bitcoin network in January 2009. The growing success of Bitcoin has spawned a surrounding cryptocurrency industry of wallet providers, exchangers, mining consortiums, media outlets, promoters and consultants, and to date, more than 1300 "altcoins." *(3)* Many altcoins are independent blockchain currencies based loosely on Bitcoin, while some are smart contract *(4)* tokens deployed on another underlying blockchain platform, such as Ethereum. *(5)* A few cryptocurrencies (such as Ripple) *(6)* are built on their own distinct technology. Bitcoin itself retains nearly half (40.2% at this writing) of the $600+ billion aggregate market cap of all extant cryptocurrencies.

A. Learning From the Past

With this rich history to draw upon, it is now possible to identify and evaluate most of the design deficiencies of Bitcoin and other decentralized public blockchain networks, with an eye toward suitably addressing these problems in order to design a superior next generation of cryptocurrencies. The basic goal remains the same as in Satoshi's paper: to create a private, censorship-resistant, non-state currency which can be utilized as the nucleus of a larger ecosystem. However, in order to achieve this goal the following list of significant issues must be addressed:

1. **Lack of scalability**. Decentralized networks and blockchain databases are inherently slow and low-capacity, compared with existing centralized clearing and storage solutions.

2. **Lack of privacy**. Recording all transactions on a distributed public ledger is inherently anti-privacy. At least one third of all "anonymous" bitcoin addresses have been de-anonymized, and this is enough to permit highly effective tracing *(7)* of money flows through the network. *(8)*

3. **Lack of final decision-makers**. Because no one owns or controls Bitcoin, all proposals for meaningful changes to the protocol are potentially contentious, resulting in ongoing civil wars, consensus failures, and ultimately hard forks of the blockchain. These events generate confusion and retard progress.

4. **Unacceptably long settlement times**. Bitcoin transactions can take anywhere from a few minutes to many days to clear, depending on a variety of prevailing conditions, most of which cannot be controlled by the average user. In the 21st century, this is absurd.

5. **A requirement to run full nodes** in order to enjoy benefits fully. It is often argued that only users running "full nodes"*(9)* (i.e. nodes that download and verify the entire blockchain) can provide true decentralization and censorship-resistance to the network. Full nodes also allow users to generate and control their own private keys, and to specify transaction fees. Yet such

nodes have an enormous footprint, imposing non-trivial hardware and bandwidth requirements.

6. **The need to see all transactions**, not just one's own. Related to points #2 and #5, users who are not mining blocks should have no need to concern themselves with transactions belonging to other parties. (And for reasons of privacy, should not see others' transactions.)

7. **De facto centralization** of mining, development, and exchange functions (among others). As the network grows in value and participation, the result is that important aspects of the surrounding ecosystem become increasingly centralized into fewer hands.

8. **Inability to control access level** on a public blockchain. By definition, on a "public" blockchain anyone running the necessary software can read, write, or validate (mine blocks) on the network. The result of this has been ongoing problems with dust spammers (DDoS), bogus spends *(10)* submitted in order to push up transaction fees, mining nearly empty blocks *(11)*, and a number of other antisocial behaviors.

9. **Inherently deflationary currency**. Many would construe this as a virtue (especially speculators), but a currency with a permanently fixed supply favors creditors, just as an inherently inflationary fiat currency favors debtors. Neither is a good long term solution for economic growth and stability.

10. **Minting and transaction clearing functions are conflated**. In most blockchain systems, especially those like Bitcoin which are built around a Proof-of-Work (PoW) mining method, the party who mines a given block collects both the new coins in the block reward, and the transaction fees for all the transactions contained in the block. This is akin to letting a mint clear checks, or letting a payment processor like PayPal print physical cash currency. The mint and the clearinghouse are, or should be, two logically and legally distinct entities.

11. **Inability to push out server software updates**. Because nodes on a blockchain violate the logical separation between server and client side functions, every client is also potentially a server. This makes it extremely difficult to ensure that software updates are installed by all of the nodes functioning as servers in the network. Consequently servers running non-conforming stale revisions present an ongoing problem.

The following additional issues apply to cryptocurrencies such as Ethereum, Ethereum Classic *(12)*, EOS *(13)*, and EOS Gold *(14)*, which facilitate the deployment of "smart contracts" *(15)* (i.e. distributed software applications) onto a "Turing-complete" *(16)* network:

12. **Smart contracts cannot be very smart**. Due both to execution cost and the need for provable correctness before deployment, smart contract programs must necessarily be of limited scope and complexity. (A few hundred bytes is typical.) Execution cost (i.e. "gas") also creates a perverse disincentive against sanity-checking code.

13. **Turing completeness is neither necessary nor desirable**. The ability to run any arbitrary code on the blockchain is also a liability *(17)*, because it assumes distributed scalability, ignores problems with running untrusted code, and relies on installing complexity inside the network itself, where it does not belong. Blockchains with more limited scripting languages (such as Bitcoin) do not flout such basic laws of computer science. Providing a complete virtual machine is fraught with inherent dangers. *(18)*

14. **No vetting of smart contracts before publication**. In the context of a public blockchain, there is simply no way to vet, verify, or prevent code from being published and run on the network, whether it adds 2+2 or implements a whole new cryptocurrency via the ERC20 *(19)* protocol.

15. **Computing power on the network doesn't increase with more nodes**. No matter how many nodes are added to a Turing-complete network, it does not run any faster, because every node executes exactly the same software code when invoked. The overall effect is a globally distributed computer with the approximate processing capacity of a late 1990s cell phone. *(20)*

A few of these issues are comparatively minor, but most are quite serious, and some are potentially catastrophic. Nor are we alone in making these kinds of constructive critiques *(236)* of blockchain tech. From these observations we can draw a couple of general conclusions. First, it is effectively impossible that any existing cryptocurrency could ever replace most national fiat currencies, regardless of the tacit permission, or even active endorsement, of governments or central banks. This is not to say that various "GovCoins," such as the Russian CryptoRuble, will not attempt to do exactly this. They will doubtless learn the same hard lessons about latency, complexity, and scalability. (A good survey of development projects under way in support of Bitcoin scaling can be read here.) *(21)*

Second, it is now obvious that even a scalable cryptocurrency does not constitute an entire ecosystem by itself. Blockchain is a shiny new tool in the toolbox for building a better, more equitable economic structure for the future. But it is not, by itself, the entire system architecture, nor is it the solution to every extant problem in software or economics. Blockchain cryptocurrency needs to be utilized in an appropriate manner, to achieve appropriate objectives, as part of a larger crypto-economic ecosystem design.

B. Designing for the Future

In the balance of this paper, we will discuss many of the problems enumerated above in some detail, and show how the Ascension Project will solve them by using a mixture of blockchain technology, a suite of existing transaction clearing and wallet client technology running above the blockchain, APIs for asset exchange and marketplace distributed applications, sound monetary policies based on price feedback mechanisms, and several tried-and-true business organization strategies. In particular we will demonstrate that:

- Our wallet and payment clearing network, which is built using Voucher-Safe *(22)* technology,

sits on top of the Ascension blockchain (also other blockchains), and provides transaction settlement that is fully scalable (solving issue #1 above), equally untraceable as physical cash (issue #2), and practically instantaneous (issue #4). Note that this technology already exists (beta deployment occurred in 2011), and accomplishes essentially everything that is hoped for from Lightning networks *(23)*, or Lumino *(24)*, and more. While functionality is distributed between servers with distinct functions, software updates are always controllable (issue #11).

- This higher level wallet payment network is "money agnostic," meaning that it allows any kind of currency or asset to circulate invisibly in the form of digital cash, such as cryptocurrencies, precious metals, even stored fiat currencies. Each digital voucher currency is emitted by an independent Issuer, which is free to follow its own individual reserve and monetary policy (issue #9), and is entirely separate from the payment clearing engine (issue #10).

- Our user client architecture is lightweight (addressing issue #5), provides access to private keys only on the user's own device, and can access only the wallet's own transactions (issue #6). Transaction receipts are seen only by payer and payee, and can be permanently deleted. Because the protocol tunnels over XMPP, it provides innate connection encryption and a superior resistance to protocol-based detection and interdiction, along with end-to-end encryption and easy access to intra-community messaging (since wallet clients are also chat clients).

- Our SilentVault Exchange (SVX) and SilentVault Marketplace (SVM) architectures and APIs (built using SilentVault *(25)* technology) provide p2p asset exchange with escrow (in the future possibly including atomic swaps between blockchains), and independent Marketplace applications accessible from right inside the wallet. These Exchanges and Marketplaces are meant to be individually owned and operated, much like franchises or stores in an electronic mall, leading to a robust economic ecosystem, decentralized by means of its business model. In this way as the total ecosystem grows, it becomes more decentralized rather than less (issue #7).

- Our Ascension blockchain will be permissioned, thus solving issue #8. Validators (miners) will be franchised out to multiple parties under contract in various parts of the world, thus providing adequate censorship-resistance under a PoW system, plus eliminating all possibility of the dreaded "51% attack." Validators will also be connected together across a special-purpose VPN for improved security. Timely installation of software updates by validators will be made a contractual requirement (issue #11). User blockchain clients will be limited to client-only functions: reading blocks or submitting coin transactions for validation. However our expectation is that most wallet transactions will continue to take place at the voucher level, even after the Ascension blockchain launches. The voucher level is completely permission-less. Publication of smart contracts (assuming these are supported) will require validator-level permissions, with pre-approval by Ascension. This single proviso neatly addresses issues 12-15, as well as providing a revenue source for Ascension.

- The Ascension Foundation will be able to administer monetary engineering for its own blockchain, and thus also for all of its special-purpose sub-currencies backed by its Lyra blockchain coins. The existing OTO ("overcome the odds") voucher cryptocurrency, introduced in late 2016, is 100% backed by Lyra coins, and will remain exchangeable at 1:1 with those coins even after the genesis block is initialized. Other currencies used in our Marketplace DApps (such as InsurBucks, SportsBucks, TradeBucks, or Quantz) may have a fractional backing versus Lyra. Additional Lyra on the blockchain can be minted in any given block. The Foundation can also repurchase Lyra coins and transfer them to a sequestered address block it controls, where surplus Lyra can be held. (Note however that on a blockchain, coins never go out of circulation once minted.) This will allow the Foundation to adjust available monetary supply as required to avoid any inherent inflationary or deflationary bias (issue #9). The idea is to balance supply and demand for the currency, as indicated by long-term coin price trends versus a basket of external assets. It should be noted that currency growth occurring in our DApps is conducted in a manner intended to squeeze out risk from betting and trading applications. By building out both the ecosystem demand for coins and the coin supply at the same time, the goal is to create a stable, private money that allows growth with low volatility – something the world has not seen since the years of the classical gold standard prior to WWI. *(26)*

- The governing board of the Ascension Foundation will also act as a steering committee to make decisions on direction and vision as the system grows, thus insuring that issue #3 does not arise. It should be noted that our charter members have been involved in the alternative payments industry since the days of digital gold currencies, a decade or more before Bitcoin was proposed.

- To provide funds for future development, and the implementation of its monetary engineering goals, the Ascension Foundation will raise money principally in two ways: 1) Through the sale of its existing OTO voucher currency (representing claims upon an equal number of future blockchain Lyra coins), during a presale, followed by a series of rounds offering progressively more coins at progressively smaller advance discounts. This sale will be uncapped and is thus not truly an ICO, but is rather a release of coins to be circulated in the ecosystem being developed. OTO will not be marketed to the public directly, but only by means of referred introductions through an affiliate marketing program (not multilevel). 2) By charging fees for licenses and franchises to independent businesses. This includes selling rights to operate DApps inside the in-wallet Marketplace (or on the blockchain itself), SVX franchises, rights to operate independent voucher currency Issuers, voucher network gateway servers, and possibly even licensing of the complete server and/or blockchain software itself. These application and licensing fees will be payable only in OTO (or equivalent Lyra coins) . The Foundation will also offer consulting and software development services to its business partners, likewise payable in OTO/Lyra.

- By design, OTO presale vouchers are a privately issued virtual currency and not a commodity

or security. We will delve into this in detail below, but for now observe that there is no investment in a common enterprise. While speculative profit is certainly possible, earnings of commissions by sales affiliates are naturally proportional to their own efforts; while future profits of independent businesses who join the ecosystem (e.g. to operate Marketplace stores) are necessarily dependent upon their own custom software development, successful marketing, and profitable execution on their own individual business plans. Token sales do serve the purpose of recruiting a base of customers holding the currency, representing a pool of potential future demand. (This same phenomenon has been observed with Ethereum vis-a-vis ICOs.) However the future value of our coins will depend as much upon the success of individual competing businesses serving that pool of demand, as it does upon the efforts of the Ascension Foundation itself. It should also be noted that other cryptocurrencies besides our own (e.g. bitcoin, litecoin) are already circulated within our wallet system, and that our "secondary market" to date is entirely internal.

- Our architecture confines government monitoring, regulation, and licensing narrowly to the level of the currency Issuers and separate wholesale fiat exchangers, which is where it belongs. Each Issuer will comply with the applicable rules for virtual currencies in the jurisdiction where it is established. This protects the ecosystem at its interfaces with the legacy banking system.

The Ascension Foundation's mission statement is: "**To promote the growth of robust, borderless, wealth-generating, free market ecosystems**." In the sections below we will expand upon the various points mentioned above, at a much greater level of detail.

II. Blockchain Challenges: achieving scalability, speed, and privacy, while maintaining censorship resistance

Most of the controversy in the Bitcoin arena to date can be traced directly to varying visions for achieving the scalability necessary for a cryptocurrency to play a role as a significant global currency, and not merely as a party favor for giddy speculators. Because this is such an important issue in the marketplace, and because our solution approach is quite different, we will delve into this matter at some length. We shall begin with a more general discussion on the role of centralization in clearing mechanisms, while keeping in mind our desired separation of the minting and clearinghouse functions.

Blockchains famously represent a decentralized architecture for clearing payment transactions. This is because transactions broadcast to the network are collected and "mined" into blocks, theoretically by any full node that first solves the block. However in general there exists an inverse relationship between the number of eligible settlement nodes and the clearing efficiency and capacity of the network. In this section we will examine some of the tradeoffs associated with greater or lesser degrees of centralization.

Consider the diagram in Illustration 1 below. This diagram reflects the possible degrees of

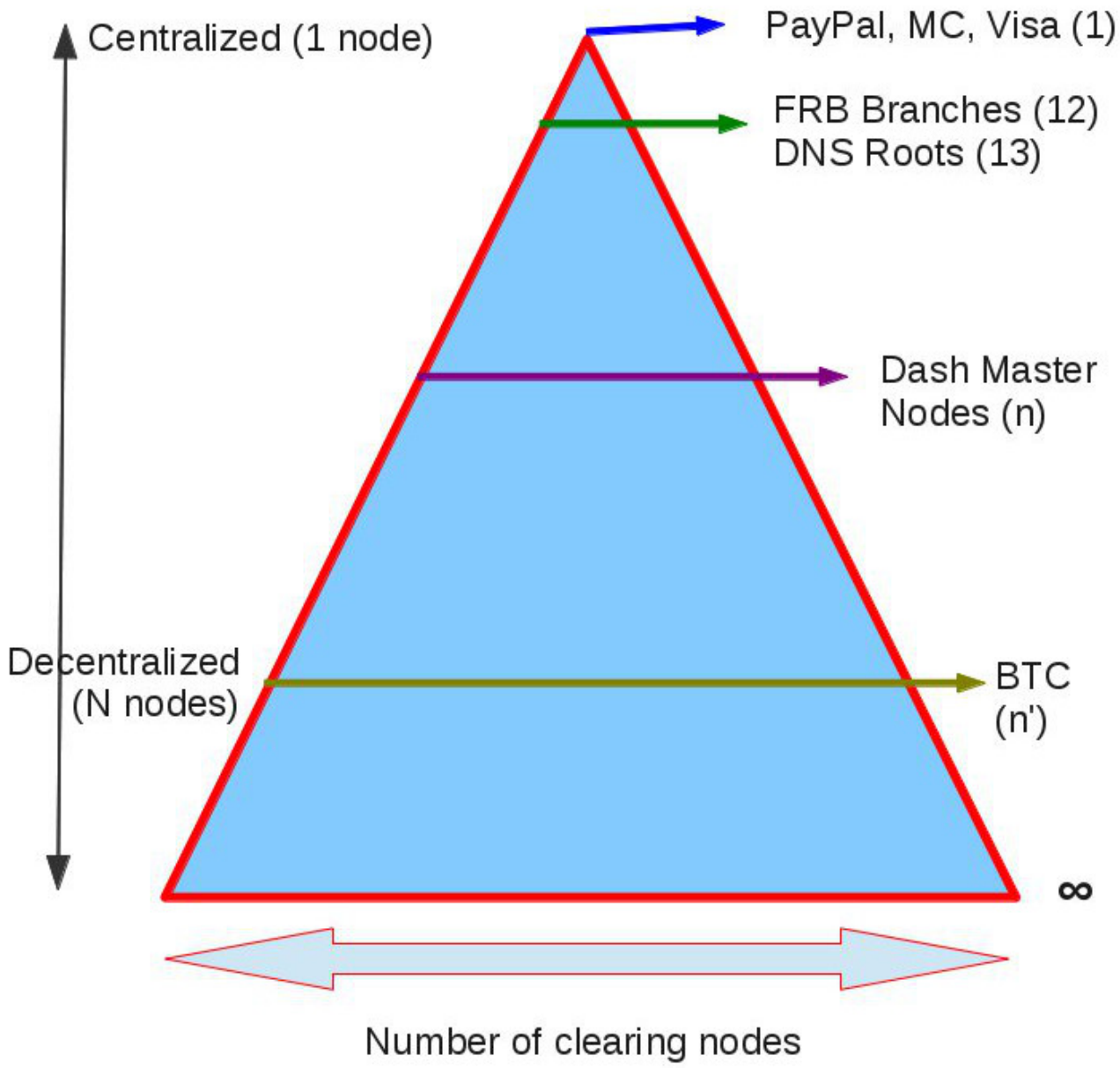


Illustration 1: Clearing Centralization

centralization in a settlement architecture, from total centralization around a single node, to an arbitrarily large number of clearing nodes. While there are of course no actual architectures at the extreme of an infinite number of nodes, there do exist actual examples of total centralization around a single node. PayPal *(27)*, MasterCard, Visa and other credit card networks, money transmitters such as Western Union and MoneyGram, ACH-based *(28)* networks like clearXchange (aka Zelle) *(29)*, and inter-bank settlement systems such as CHIPS *(30)*, SWIFT *(31)* and FedWire *(32)*, all serve as large scale examples of centralized settlement. Naturally a single clearing node does not imply a single computer; but since a CPU and database cluster controlled by one company is involved, it can fairly be considered as a single logical node. These types of systems are not “p2p” (direct person-to-person) because they always clear and record on the books of a third party, with which both of the parties to the transaction typically have accounts.

The example of clearing checks, ACH payments, and other transfers between USA bank accounts presents a variable degree of centralization. If both the sending and receiving account are held in the same bank, this is a degenerate case in which a matching debit and credit to the two accounts on the bank's ledger suffices to settle the payment. If however the two accounts are in different banks, then the transaction requires a clearinghouse *(33)* to settle between the respective banks. About $1.2 trillion per day of this activity is handled through the CHIPS system. CHIPS was organized in 1970 by eight New York banks who were members of the Federal Reserve System. CHIPS is thus both a competitor and a customer of the Federal Reserve. The clearing function is ultimately handled by the regional Fed banks (of which there are twelve). Clearinghouses like CHIPS and SWIFT act to "net out" *(230)* a large portion of the transactions for speed, so that the Fed banks only see the net flows between member banks. So-called "international" wire transactions also involve the correspondent accounts of the foreign banks at banks in the USA. (Technically all US dollar-denominated retail accounts anywhere in the world are in actual fact held at one of 13 US domestic commercial banks. Thus there is really no such thing as a "foreign" bank account denominated in US dollars; an inconvenient fact that cryptocurrency exchanges have recently learned to their cost.) *(34)* Ironically, all of this legacy system architecture is not dissimilar to the current design for Lightning Networks!

An important observation is that the number of processors required to settle a US dollar bank-to-bank payment varies, depending upon the *geographical* locations of the parties to the transaction. Also, due to their being rooted in an accounting system called double-entry bookkeeping (used widely by banks since the end of the 15th century) *(35)*, banks historically settled transactions on the basis of a "business day." This may be visualized as analogous to a "block" (in the blockchain sense) spanning at least 24 hours (longer where weekends or holidays are involved), in which the final balances of each account after all of the transactions have been settled represent the set of unspent transaction outputs (UXTOs) for the next block. Prior to January 2001, CHIPS settled at the end of the day, but now provides intraday payment finality through a real-time system.

While it isn't related to payments, the internet's DNS (domain name service) lookup mechanism is also semi-centralized, much like the 12 regional FRBs. There are 13 root servers (A – M), any one of which can be contacted to initiate a domain-IP lookup. Changes to the database have to propagate before the result will become consistent across all 13 root servers, a process which can require several hours. This serves as an example of just enough decentralization to provide robust parallelism, without introducing excessive synchronization overhead. While it's not perfect, the mechanism suffices because most domains don't change their IP address blocks very often (and for those that do there's dynamic DNS).

The clearing mechanism used by the cryptocurrencies DASH *(36)* and PIVX *(37)* presents an interesting middle case. Payments are submitted by ordinary client nodes, but aggregated and settled by "master nodes," which are high-volume clients accorded special privileges. Although the motivation for this aggregation is privacy, via the obfuscation of individual transactions by mixing them with unrelated ones (using an algorithm known as "CoinJoin") *(38)*, the effect is to create a clearing layer *(229)* where the number of nodes involved with transaction settlement (~4600 for Dash) is much less than the total number of nodes in the system. The distributed ledger system Ripple

similarly operates with a significant but fixed number of transaction validators. *(39)*

Bitcoin itself, along with most altcoins, employs a highly decentralized clearing architecture where the number of settlement nodes is bounded only by the number of "full nodes" (with mining activated) that are participating in the network. However due to such nodes banding together into mining pools, which can sometimes be viewed a single logical node controlled by only one operator, the degree of decentralization is actually much less than it appears. Most bitcoin users and merchants do not operate their own full nodes, and instead rely on wallets hosted by third parties. This results in further operational centralization. As a practical matter, exchanges on which bitcoin can be bought and sold for national fiat currencies are typically very centralized, and many of these operations often hold large proportions of their clients' coins in trust at addresses controlled by themselves. If the exchange is honest, this isn't inherently bad (give or take hacking risks); *(40)* but it definitely isn't congruent with the popular vision of users personally controlling their own coins.

Efficiency and Throughput

In general there exists a positive correlation between the centralization of a settlement architecture and both its efficiency and its throughput. PayPal is reputed to be able to process on the order of 400 transactions per second (tx/s), while major credit card networks can process on the order of 50K tx/s or more. *(41)* These networks typically process transactions in seconds, certainly in no longer than a minute. Moreover whenever greater capacity is required, additional computing resources should suffice to provide the expansion (although not necessarily in a linear fashion). By contrast Bitcoin, the most popular cryptocurrency, requires anywhere up to 10 minutes or more to record a transaction, or up to an hour if 6 confirmations are wanted. By design, a single Bitcoin block can only hold enough transactions to support around 3.5 tx/s. Bitcoin's own popularity is thus limiting its potential market penetration, through unacceptably slow clearing, grossly inadequate throughput, gradually increasing fees, and poor reliability (especially when low fees and smaller transactions are attempted). Faster clearance requires higher fees *(42)*, since price is a rationing device for scarce block space. Inadequate fees lead to a large backlog of unconfirmed transactions. *(43)*

While the gospel of cryptocurrency avers that decentralization is always good and centralization is always bad, we should duly note that decentralized cryptocurrencies currently handle only a miniscule portion of global payment transactions, both from the perspective of aggregate value and also by transaction count. This is actually not surprising given the inherent correlation between increasing decentralization and increasing synchronization overhead. In a fully centralized system there is one node, and it is fully trusted. In a decentralized architecture there are many nodes, and for safety's sake they must all be assumed to be bad actors, since an internet connection is the only requirement for entry into the network. (Being able to deal with this assumption about hostile actors is known as Byzantine fault tolerance *(44)*, which is a common characteristic of blockchain systems.)

If we let N be the number of clearing nodes, then we can broadly (and simplistically) define network clearing efficiency E thus:

$$E = 1 / N$$

This implies that efficiency is maximized with 1 clearing node, and approaches zero as N approaches infinity.

Similarly, we can define the effort (overhead) required for network synchronization S as:

$$S = N * (N – 1) / 2$$

Actually this is a worst case, since the network can relay blocks *(45)*, making it unnecessary *(46)* for a node which clears a transaction (i.e., mines a block) to inform directly every other peer besides itself. The important inference is that this effort increases as a function of the number of peer nodes in the network, as well as with the volume of transactions. This factor generates an inherent and unavoidable tension in blockchain systems between decentralization and efficiency. Even blockchain systems developed after Bitcoin have a maximum "speed limit" which is far below that of centralized clearing mechanisms: Hyperledger Fabric can do about 400 tx/s *(47)*, while Ethereum can do up to 10 tx/s. *(48)* (Which may prove insufficient to keep up with the crypto kitties.) *(49)* By contrast the logging system Apache Kafka *(50)* (which only needs to be crash fault tolerant) can do millions of tx/s.

The point is that there is always a maximum speed for any distributed system, inherent in the fact that it's distributed, which will *always* be lower than in a centralized system. In a distributed system, every new user/node has to track state for every other user/node at a rate that is not sustainable. This is a known problem of long-standing in computer science. *(51)* Simply put, you cannot publish ever increasing quantities of data onto the network, and simultaneously reduce (or even maintain) the time interval it takes for the data to become globally consistent. This isn't just "a hard problem," it's actually a logical fallacy. It ceases to be a fallacy only if one can assume the existence of both infinitely fast nodes and infinitely low (i.e. zero) latency across the network, neither of which can actually exist. We sincerely wish the brilliant Mr. Buterin good luck solving this conundrum with sharding. *(52)*

Why then is decentralization inherently "good" while centralization is *ipso facto* "bad"? This dictum is plainly not related to concerns about efficiency or throughput (which concerns by themselves would lead one toward the opposite conclusion), but is derived instead from exogenous non-technical aspects related to ownership, control, censorship resistance, economic theory, and even political ideology. For example, centrally regulated banks in the nation of Cyprus at one point told their depositors that they could not access their own money; and similar scenarios may yet unfold in other nations as well.

Ownership and Control

Diversity of ownership and control for settlement mechanisms generally parallels the degree of decentralization. A single clearing cluster is typically owned by one corporate operator, such as PayPal. A multiplicity of clearing nodes typically has many individual operators. Therefore a decentralized system requires the consensus of the network; whereas in a centralized clearing system

the issue of achieving consensus is moot. This follows logically because "consensus" is really a mechanism for resolving blockchain forks (i.e. figuring out which is really the longest chain), and in a single-node clearing system, no forks will ever occur.

We should note that in the case of PoW blockchains, the formation of mining pools effectively generates more relative centralization than the raw number of client nodes suggests. Although it has never occurred so far with Bitcoin, it is possible that a mining cartel could be formed which could exert effective central control over a public blockchain, even a very large one, by controlling 51% of the hashing power on the network for a sustained period.

In a Proof-of-Stake (PoS) blockchain, it is frequently the case that a small number of owners (founders, developers, early adopters) control a majority of the coins in the system, and consequently have the ability to control consensus; and thus dictate what happens – or doesn't happen – on "their" blockchain. Ethereum's Vitalik Buterin called pure PoS systems "permanent nobilities where the members of the genesis block allocation always have the ultimate say." *(53)* In such a system, ownership and control are potentially quite centralized, despite being implemented as a "decentralized" public blockchain.

The ability of a development team to control updates to client code can also create a quantity of effective centralization. For example there have been a number of updates to Bitcoin Core (such as the introduction of SegWit) *(54)* that have not been unanimously agreed upon. But this form of control was never more clearly demonstrated than by the hard fork of Ethereum (ETH) that spawned Ethereum Classic *(55)* (ETC). A project which was a major early adopter of Ethereum's smart contracts technology, called the DAO, failed catastrophically *(56)*, and the Ethereum Foundation elected to roll it all back in order to restore the investors' losses. This was done despite strong warnings *(57)* that such intervention effectively nullified the concept that "the code is the law," potentially opening up a Pandora's box of additional cases in which a similar decision could be taken by those in effective control of the technology. "Ethereum Classic" or ETC represents the continuation of the original ETH blockchain, in which the DAO episode was not rolled back, for philosophical reasons.

What we see illustrated here is that a consensus failure (that is, a failure to achieve consensus, rather than a consensus that a failure has occurred!), leads to a hard fork in the blockchain. A consensus failure could arise as the result of a code change (as occurred with BCH and will occur again if B2X is ever launched), due to a data change (such as the DAO rollback), or from a 51% hashing attack. The latter cause has shown itself to be an unlikely possibility on a widely used blockchain, but the others have actually precipitated forks.

Having many communal owners or stakeholders in a network is seen as democratizing, and therefore as a social good. Given the extraordinary abuses seen with national fiat currencies, and the central banks that issue and operate those currencies, this is quite understandable. There is definitely something to be said for a network that is naturally resistant to dictatorial control. Unfortunately the flip side of this characteristic is the impossibility of final decision-making, precisely because there exists no ultimately responsible party. Bitcoin is presently in the midst of a full-blown civil war about scalability solutions, which is becoming increasingly bitter, acrimonious *(58)*, and indeed childish, while usability is

plummeting and innovation is stalling out – or more accurately, moving into other technologies such as Ethereum, Hyperledger *(59)*, and private permissioned blockchains. *(60)*

Many decentralized owners is also seen as fostering censorship resistance, because it becomes much harder to shut down widely scattered nodes, and because no one party can be served with subpoenas, cease-and-desist orders, or the like. However this supposition may be naive. In fact since Bitcoin (and practically every altcoin) utilizes a distinct protocol for all network communications, it wouldn't be particularly difficult to program intelligent edge routers (say, at a national border) to drop all packets conforming to that protocol, by means of what is known as "deep packet inspection." It should also be noted that the censorship resistance derived from having no single point for legal process can also be achieved by means of software design, coupled with sufficient jurisdictional arbitrage embedded within the operational business model. (More on this topic later.)

The Bitcoin Block Size Debate

Which brings us to the ongoing civil war in Bitcoin about scalability. The basic problem is that Bitcoin has become too popular for its own good. There are too many transactions being posted in competition for limited space in blocks. The space is limited because of the fact that blocks are currently capped at one megabyte (1 MB) in size. The block size is a parametric value established in the source code (known as a "hard coded" value). The negative result of the competition for scarce block space is twofold: 1) transaction fees have climbed sharply as price gets used as a rationing device; 2) wait times for block confirmations have also increased, to the point where it isn't unusual for a posted transaction (particularly a small one) to require several *days* before it gets mined into a block. The result is that Bitcoin becomes ever more expensive *(61)* and/or ever more inconvenient to use. It is of course possible to "cut in line" by bribing miners with higher than average fees. But as a general rule of business, declining service coupled with rising price is not a recipe for increasing market share. Growth tends not to be a problem for the private sector, but is frequently an onerous burden for the public sector; and Bitcoin's communitarian nature bestows upon it a number of public sector characteristics.

There are two main factions or camps *(62)* within the Bitcoin community on the subject of whether or not the block size should be increased. The first is the "NO2X" faction, indicating opposition to doubling the present blocksize to 2MB. This group, including most of the current and former principal development team (known as the "Core devs"), wants to keep the block size unchanged. Instead, they promoted the adoption of SegWit *(63)* (Segregated Witness), and the future use of Lightning hubs to move retail transactions off chain. The pro-blocksize increase faction is lately associated with the "B2X" version of Bitcoin, based on the "2X" part of the SegWit2X plan adopted in the New York Agreement. In the past this faction was also associated with the alternative client Bitcoin Unlimited, as well as with advocacy for the Bitcoin Classic and Bitcoin-XT clients. It is also involved with promoting Bitcoin Cash, which forked off of Bitcoin earlier in the year and implemented 8MB blocks without SegWit.

It should be understood that in order to effectuate a change to the underlying protocol, nodes

representing a majority of the hashing power on the network must “signal” that they wish to adopt the proposed change. (For a general discussion on Bitcoin “governance,” see this.) *(64)* For example, SegWit was adopted on the Litecoin altcoin network when a majority of blocks (51+ out of the last 100) were mined by nodes signaling for SegWit. This has now also occurred on the Bitcoin network, after 80% of hashing power signaled support for it.

The “too long; didn't read” (TL;DR) explanation of SegWit is that it modifies the protocol to shift some of the transaction detail data (mainly signatures) now stored in the blocks themselves into an adjunct data appendix (called an “extension block”), which is incorporated by reference inside the block transaction. The net result is about a 60% increase in the number of transactions which can fit inside a single block. Thus SegWit is about using space more efficiently, rather than increasing the amount of raw space.

SegWit is at best a stopgap which will buy only a limited amount of headroom for the Bitcoin blockchain -- at the cost of increasing the complexity of the protocol going forward. However since its adoption, only a low double-digit percentage *(65)* of bitcoin transactions have availed themselves of the new SegWit functionality. (But it's early yet.)

Lightning networks *(66)*, previously known as “side chains,” are a mechanism for moving a block of bitcoins into a special reserve, or anchor address (typically one having multi-signature controls). The coins are then cloned onto an entirely separate blockchain, where they can circulate freely (potentially according to entirely different rules) without needing to post any additional data onto the origin blockchain. Each Lightning network effectively represents an independent local centralization, or at least a concentration, of settlement nodes. The Lightning networks taken as a group act to fragment the Bitcoin blockchain. (Indeed the same concept in Ethereum parlance is referred to as “sharding.”) While this idea could potentially buy Bitcoin considerably more headroom than SegWit, even this concept doesn't achieve arbitrary transaction throughput. *(67)* (See also this *(68)*, and this *(234)*). One good reason is that there will always be synchronization overhead associated with moving coins in or out of Lightning networks, or from one Lightning network to another. At some point, such necessary synchronization of coins would itself potentially eat up100% of the base Bitcoin network's capacity.

An analogy can be drawn with the NUMA *(69)* (non-uniform memory access) computers popularized in the 2000s. At some point, adding more CPUs to a NUMA computer ceases to increase the total capacity, because the synchronization of inputs and outputs between each CPU's individual memory cache saturates the main data bus, all by itself. How many Lightning networks could operate without similarly saturating the underlying Bitcoin blockchain with their synchronization traffic? This would depend upon the degree of economic independence between the user and business communities being served by each Lightning network. It can safely be concluded however that the answer, as with NUMA CPUs, is finite and probably not all that large.

The NO2X faction tends to view the “pain points” of long delays and high transaction fees as useful and necessary in order to impel the industry to adopt technologies like SegWit and Lightning. This amounts to believing that Bitcoin is not in fact a retail payment network, and should not be used as one.

In this view, inevitable user dissatisfaction is a spur to innovation, which will take place mainly "off chain." Thus the NO2X camp is remarkably insouciant about the growing pains of Bitcoin. NO2X adherents also tend to be "Bitcoin maximalists," meaning that they see value in altcoins only insofar as they enable Bitcoin to improve, viewing them as an exegesis on the principal Bitcoin technology.

The Bitcoin 2X (B2X) faction, championed by Roger Ver and others, is in contrast much more alarmed by the growing unusability of Bitcoin for retail customers. While the Core devs tend to see Bitcoin users as nodes in a software system, B2X adherents view them as retail customers in the business sense – customers who are not at all well served *(70)* by the status quo. A summary of arguments for Bitcoin Unlimited, along with some remarkably blasé quotes from the Core dev team, can be found here in this slideshow *(71)* prepared by Roger Ver. In particular, the graphs showing the growth of altcoin market cap at the same time that Bitcoin's user performance falls, are noteworthy. Certainly from a business perspective, as opposed to a software perspective, leaving the block size at 1MB is a non-starter, bordering on insane. Of course it can also be argued *(72)* that using Bitcoin as a network platform for retail consumer payments is a fundamental mistake to begin with.

There are however consequences to raising the block size. The amount of memory required to verify 1MB Bitcoin blocks (never mind mining them) is already substantial. Devices with only a few gigabytes of RAM available perform block verification multiple times slower than devices with significantly more RAM. If the block size increased substantially (note the Bitcoin Unlimited plan called for gradual steps up to as high as 8GB!), it would very quickly require hardware well beyond the reach of casual retail users and small businesses. The result would of course be further centralization, not only of the mining function, but also of the verification of the blockchain by non-miners maintaining full nodes. This would have the eventual effect of centralizing all blockchain activity around a small number of participants that owned enormous computing resources. Ordinary users would be relegated to operating web-based clients hosted at those major vendors, probably no longer in sole control of their own private keys. Thus the B2X vision ultimately entails sacrificing the distributed, democratized, decentralized nature of Bitcoin on the altar of good customer service. To refer back to our pyramid diagram, B2X would shift Bitcoin from near the bottom of the pyramid upward to near the top, gaining efficiency while losing decentralization.

If Bitcoin were a business operated by a single company, very likely the B2X option would already have been embraced. However as matters stand this is not the case, and since so many oppose deviating from the original vision of a decentralized community-based currency issued by no one, even all the money which is getting left on the table by Bitcoin's inability to expand, and all the R&D budgets now pouring into alternative technologies, hasn't been enough to rudder the ship onto a different course. What we see here is literally a case where arguably needful business development is being restrained by ideology. But this is hardly unprecedented, after all: didn't the Soviet Bloc and Maoist China constitute exactly such an example on a massive scale for most of the 20th century?

The Bitcoin community is stuck behind the reality that not to decide is in itself a decision, and this does not appear likely to change anytime soon. Because SegWit2X requires agreement by a majority of hashing power (BIP 9 activation), which appears most unlikely to occur, yet another hard fork of

Bitcoin seemed inevitable, until the B2X side "blinked" and elected to save face by postponing the activation. *(73)* This B2X fork would have occurred in mid November, and follows closely on the heels of the Bitcoin Cash *(74)* (BCH) fork *(75)*, and the recent (friendlier) Bitcoin Gold *(76)* (BTG) fork *(77)* on 25th October. (Bgold is aimed at creating an ASIC-resistant Bitcoin.) So understandably some of the community felt that Bitcoin had just dodged a bullet. *(78)* But the irony is that even if they were all adopted on the main chain, ultimately such reforms are merely a stop-gap that would only kick the can down the road.

Which would have been the rosy scenario. The actual result is multiple permanent hard forks into (so far) four coins: original BTC, BCH, BTG, and BCD (Bitcoin Diamond *(79)*, a version based on PoS mining), and now a fifth in B2X *(80)*, not to mention various copycats. *(81)* Without bidirectional replay protection, it's also possible that one of two chains could subsequently replace its rival even after hundreds of blocks have elapsed (an event known as a "wipeout," which is every bit as bad as it sounds). Miners may opportunistically flip-flop back and forth from mining on one chain to mining on another, depending upon prevailing conditions. *(82)* Mining pools may allow their members to pick which chain should be mined. Some may make a "none of the above" choice by opting to mine Bitcoin Cash, which already increased the block size to 8MB, or 4x bigger than SegWit2X's 2MB. It's interesting that BCH's price nearly doubled immediately after B2X was suspended, especially given that some had argued that B2X was essentially mooted by BCH. It should be noted that we have the ability to bring any worthy Bitcoin forks into our ecosystem.

At this point the civil war is all about bitcoin businesses picking sides *(83)*, and even deciding which coin *(84)* will be designated as "the true bitcoin." Clearly the lack of a "decider" has multiplied risks, increased uncertainty, and generated much confusion. As a result, practical survival guides like this one *(85)* have begun to appear in the community. While this state of affairs should be enough to stand anyone's hair on end, the anticipation of "fork dividends" (derived from receiving equal coins on the other fork as a windfall) has only driven the price of bitcoin higher. *(86)* (However, this fork dividend concept may yet prove to be a faulty expectation.) *(87)*

The remarkable fact though is that neither NO2X's vision nor 2X's vision is workable for Bitcoin in the long term. The NO2X path will lead to an oligarchy of Lightning hub operators, which will still have limits to scaling. *(88)* The 2X path will lead to an oligarchy of miners who clear all the transactions, plus an oligarchy of web wallet providers, and likely still won't solve all the problems with latency. There simply isn't a path forward which will allow Bitcoin to become the global cryptocurrency to obsolete other cryptocurrencies and ultimately replace fiat, as Bitcoin maximalists like to dream. *(89)* Or at least, if such a path exists, it hasn't been discovered yet.

Back to the Future?

So where does this leave us, in late 2017 looking toward the future? It's self-evident that wide global adoption is going to require serious scaling, coupled with low latency. It should also be clear by now that any solution providing adequate scaling is going to involve at least a certain amount of clearing centralization as a by-product, if not as a direct goal. This is true not only for the obvious reasons of

efficiency, but also because of the growing requirements of regulation. Authorities will want to be able to reject at the net any transaction of which they disapprove. Such an outcome is highly likely to result from lobbying efforts such as this one *(90)*, or from study committees like this. *(91)* In the past, regulators have been unable to exercise a veto over specific transactions, because the clearing mechanism was too decentralized. But once the need for clearing efficiency has leveraged enough centralization, such control may become much more feasible. Some national governments are mulling the creation of their very own cryptocurrencies (Estonia and Russia come to mind). In that case, censorship can be expected to be built-in, and competition from other blockchains will not be welcomed, and may be prohibited outright.

The other clear trend is the shift toward permissioned blockchains. *(222)* In any blockchain, there are three basic functional levels: the client can connect to the network and read data (it can download blocks); it can also submit transactions (meaning it has write access); and it can confirm transactions (by means of mining blocks). Put simply: read, write, and verify. In a permissioned blockchain, these functions can be accessed according to a node's possession of a certain private key, or by virtue of connecting from a certain IP address, through some type of login protocol, or by some other means specified in software. For example, anyone might be able to download the client and browse completed transactions (similar to search functions at blockchain.info *(92)* for example). But only authorized terminals would be able to submit spends, and only a strictly pre-specified list of miners would be able to confirm them.

This is fully consistent with the way existing fintech works. For example banks do not allow non-customers to initiate transactions across the banking system. A non-customer may be able to cash a check drawn on the bank (if they're willing to be fingerprinted), but only account holders may write checks, use an ATM machine, send a wire transfer or ACH payment, etc. Similarly while anyone can send money via Western Union or Moneygram, the customer has to take their money to an official terminal at a franchise office to submit their request. Transactions to certain recipients or regions are sometimes rejected by these money transmitters, allowing censorship. If banks and money transmitters ever adopted cryptocurrency, it stands to reason they would do so in a manner consistent with their existing model by deploying a permissioned blockchain. In such a system banks and franchised storefronts would have nodes with read and write privileges. Account holders would have wallets linked to their verified identities, and could submit payments only via a branch office node. Transaction verification would be done by mining pools controlled by the bank, or more likely by the banking cartel as a whole. (The Federal Reserve System is of course a banking cartel, not a government agency as such, no matter how much it may posture otherwise.)

No blockchain-based fintech could ever be acceptable to the existing financial system, or to its regulatory apparatus, which allowed any device with an internet connection, run by any anonymous geek anywhere in the world, to connect to the network and start broadcasting transactions, let alone validating them. Indeed there are reasons why even a privately owned network (as for a niche altcoin) might want to block that from happening – preventing DDoS attacks for instance. On a purely public permissionless blockchain, there is no way to prevent anything at all, from high velocity “dusting” spends of tiny amounts of coins simply to soak up block space maliciously, to frequent repetitive large

spends back and forth between wallets controlled by the same owner, made in an effort to bump up the calculated average transaction fees, to a full-blown 51% attack. (Bitcoin has already experienced all these kinds of attacks, and more, with the exception of a 51% attack.) For these reasons it's also fairly probable that many Lightning network operators will ultimately deploy permissioned blockchains, too.

So where does all of this get us, in the end? Regardless of what happens to "resolve" the Bitcoin scaling debate, it seems that we are headed for, at best, a federated network of mostly centralized clearinghouses operating in competition with each other. Ironically, this is not dissimilar to the status quo which existed before Satoshi ever published his paper, with one distinct difference: in the past there was no distributed ledger of all posted transactions which could be read by anyone with permission. *Thus the net effect of introducing blockchain tech into the mix will have been to reduce or eliminate privacy*. This is of course completely contrary to the vision which animated early Bitcoin adopters, but it was the obvious likely result all along, at least to those who read Satoshi's paper and thought about how the concepts *(93)* it discussed would eventually integrate into the real world.

The Future of Private Money

When Friedrich Hayek *(94)* published The Denationalization of Money *(95)* in 1976, and ***Denationalization of Money: The Argument Refined*** in 1978, he argued for privately issued money as opposed to money issued by governments (or by central banks to which a government has contracted out the issuance of its money). Hayek concluded that privately issued currencies, competing with one another for market share, would result in a stable system which would better protect the interests of the users of such currencies. Similar arguments *(96)* continue to be made by scholars today. Certainly central bank fiat currencies have done precisely the opposite, mainly because their management is actually serving the interests of governments -- and of the elites who own and operate those governments, of course -- against the interests of the populace.

When modern cryptocurrency made its debut in the form of Bitcoin in 2009, many hoped that such a currency would prove to be a fiat slayer, because it was deflationary (i.e. strictly limited in supply), whereas fiat currencies are always inflationary. (Inflation being one of the principal mechanisms through which the elites plunder the 99%.) However as Hayek pointed out, a deflationary (upward-valued) currency inherently favors creditors, just as an inflationary (downward-valued) currency inherently favors debtors. Neither policy is uniformly good over the long haul. But while central bank fiat leads to the tragedy of the tyrant *(97)*, decentralized cryptocurrency leads to the tragedy of the commons.

There is no inherent reason why a "fiat" monetary system (that is, one with an elastic, variable money supply, not "backed" by any asset other than its own utility) cannot serve the interests of its community of users in a balanced way. It's just that we are all accustomed to thinking of fiat systems, which are typically run by central banks, as having a built-in rate of inflation of 2% per year (or whatever). This inflation property is aimed squarely at alleviating the debt burdens of the biggest borrowers, who are almost always governments, and politically potent, giant corporations. But a privately issued fiat money which inflated perpetually without limit, without recourse to legal tender laws, and without due

regard for the true economic demand for its supply, would quickly lose market share to better managed, more stable competing currencies. Due to decades of severe mismanagement, the global regime of government fiat currencies is in serious trouble, and may be vulnerable in the near future to competition from better-managed cryptocurrencies. Even an analyst at Deutsche Bank thinks so. *(98)*

Is it possible for a privately managed currency to address such concerns in order to maintain its value? Plainly, yes: consider the recent example of Ripple. *(99)* Ripple's XRP currency had a market cap of around $11.4B, but the company also owned another $16B or so worth of XRP which it has not yet released into the market. Worried that such a large supply overhanging the market might depress the price, Ripple decided to deploy 88% of its remaining XRP inventory into a series of 55 smart contracts, which will release the currency into the market at a measured pace, on the first day of each month over the next 54 months. In other words, they committed to a specific rate of inflation over the next 4-1/2 years, based upon their estimates of the probable demand for their currency over that time as usage of their network expands. This is an example of exactly the kind of management for the benefit of users and other stakeholders that Hayek was talking about 40 years ago. Will it work? What will happen after 54 months? We don't know, but we can presume that Ripple will do its best to protect the value and utility of its private currency. (At this writing, Ripple's market cap is around $83B, so putting the monthly circulation increases on auto-pilot back in May seems to be working out very well.)

In regard to privacy however, Ripple is hardly a model to be emulated. Only duly KYC'd users can participate, and the company retains permanent records of all transactions. Moreover the target market for Ripple isn't really retail usage at all: they are angling to compete with the SWIFT wire system *(100)* to handle bank-to-bank and cross-border transactions, using their XRP currency as a common vehicle. All of the 50-odd validator nodes on their network are operated by big companies, mostly financial services firms. Nevertheless they've become the second largest cryptocurrency by market cap.

But what if an elastic-supply currency existed, managed by a private foundation, targeted at large existing niche markets, and issued onto a permissioned blockchain? What if this cryptocurrency provided its own built-in quasi-Lightning network to facilitate fast and truly private, anonymous and untraceable digital cash payments? What if the various components of this system utilized architectural data separation, and a partitioned business model combined with jurisdictional arbitrage, to provide a level of censorship resistance comparable to that of a widely distributed network of independent miners?

This vision is precisely our plan for the Ascension Project.

III. The Ascension Voucher Network Architecture (A Layer Above the Blockchain)

In addition to operating a future permissioned blockchain, the Ascension Foundation already operates a digital currency Issuer within the Voucher-Safe *(22)* / SilentVault *(25)* network architecture. This is a federated network built on top of XMPP (aka Jabber chat), in which wallet clients exist as specialized

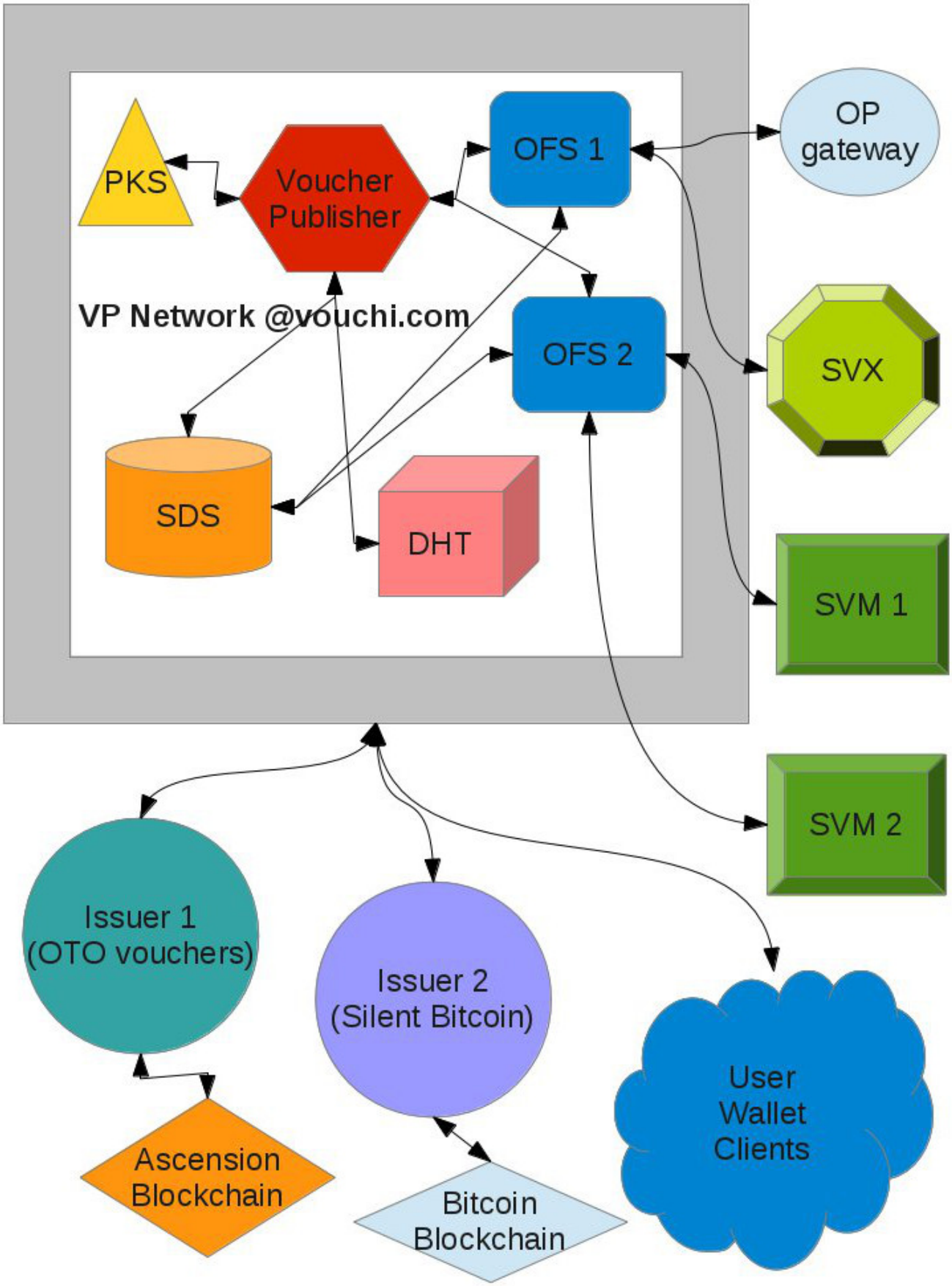


Illustration 2: Voucher-Safe / SilentVault Architecture

instant messaging clients, and value is represented via cryptographically signed XML objects called vouchers. A “voucher” is a digital bearer certificate representing a quantity of a valuable asset, held by its Issuer. This asset could be vaulted precious metals, stored fiat currency, or of course cryptocurrency, as is the case with OTO, SBC (Silent Bitcoin), and SLC (Silent Litecoin). The V-S/SV architecture is shown in Illustration 2 above.

Definitions:

VP: Voucher Publisher, is the centralized clearing engine which manipulates vouchers and clears payments. (There is presently only one VP in operation, but there could potentially be many. Since VPs are a profit center, is an opportunity for franchising.)

OFS: Openfire Server, the XMPP server gateway through which wallet clients access the VP, SVX, and SVM functionality. Acts as a proxy for end-to-end encrypted messages, as well as handling p2p and group chat messages. There can be multiple OFSs per VP, again offering a business opportunity since an OFS earns tokens through its operation.

SDS: Secure Data Store, the location for permanent storage of wallet data. Everything in its database is encrypted, and stored at anonymizing hashes. Each VP works with a single SDS, which earns tokens.

DHT: Distributed Hash Table, a place for temporary storage of encrypted messages at wallet hashes. Used for storing notifications to wallets about incoming payments and receipts. There is one DHT per VP network, which also earns tokens.

PKS: Public Key Server, which looks up the public key certificates of wallets (which are generated by clients and signed by the VP). A VP can operate multiple PKSen for redundancy, but they are house elves which do not earn tokens.

SVX: SilentVault Exchange *(101)*, a p2p escrow exchange where wallet users can anonymously trade vouchers of different asset types. By special arrangement with an Issuer, vouchers can also be purchased for external cryptocurrency payments. For example OTO vouchers can be purchased using BTC or LTC. Multiple exchanges can operate, competing on fees, allowing for a franchise model.

SVM: SilentVault Marketplace, a place for merchant stores or games where merchandize or services are offered for sale, accessible internal to the wallet client (i.e. not requiring the use of a browser or a domain name). There can/will be many such stores, most of them provided by independent entrepreneurs rather than by the Ascension Foundation itself.

Issuer: an entity which emits and redeems vouchers backed by assets it holds in trust. In the case of OTO, these assets would be Lyra coins which will exist on the Ascension blockchain. There are already a number of Issuers, such as Silent Bitcoin (SBC, shown) with more contemplated. As with SVM storefronts, Issuers are operated by independent businesses.

OP gateway: an OnionPay *(102)* franchise which provides a merchant interface (SCI) that allows websites to accept vouchers as payment for customer purchases. (There is currently just one of these, but multiples are possible.)

Achieving Performance, Privacy, and Business Opportunity (Lightning and then some!)

For Issuer asset types which are themselves cryptocurrencies, the voucher system acts like a "Lightning" network, in which coins that are moved into the custody of the Issuer cease to circulate on their blockchain, and thereafter circulate in digital voucher form instead. Unlike coins, vouchers are always destroyed and replaced in every transaction. And because the VP signs only vouchers and never wallet balances or receipts, this provides a means to circulate cryptocurrencies anonymously and untraceably, without leaving any "footprints" on the native blockchain. In this way a layer of privacy is provided, as well as efficient, instant, irrevocable settlement. In computer science lingo, voucher payments are "ACID," *(103)* that is: atomic, consistent, isolated, and durable. This deftly avoids the entire consensus problem arising from the need to make a decentralized blockchain consistent.

The SDS, DHT, and PKS nodes can exist logically independent of their underlying data storage mechanism, which can be anything from a standard relational database management system (RDBMS), *(104)* to a large distributed database, to a distributed "least authority" file system such as Tahoe *(105)*, to a distributed ledger such as Symbiont Assembly. *(106)* (Presently, a conventional RDBMS is utilized; Tahoe was also implemented.) Note too that because unique hashes are exclusively used as indexes, neither the SDS nor the DHT can know which records they are storing belong to which wallets. Also all data which they store is always encrypted to keys not accessible to them.

Like many centralized clearing systems, the V-S component nodes scale linearly, and load testing with robot clients has demonstrated that the network can support a transaction volume at least equal to that of the global Bitcoin network, even if all of the various nodes are running on but a single modern server! Hardware can be added as required to provide multi-server clustering for each individual component (VP, OFS, etc.). This makes linear scaling possible simply by deploying more hardware.

An Issuer keeps only a list of its circulating vouchers, by serial number and amount. It has no way to know which wallets contain any of those vouchers. The VP knows the public keys of the wallets involved in a given transaction, but has no list of valid vouchers for any Issuer. It cannot locate or decrypt the vouchers stored on the SDS or DHT for any given wallet, and signs only vouchers and tokens. (Tokens, in the V-S context are micro-vouchers expended to make payments.) Receipts are signed only by recipient wallets, never by the VP; and "memo" data in a payment or receipt is always encrypted end-to-end using the counter party wallet's public key, and therefore is not visible to the VP.

To pay for spends on this network, "tokens" are purchased from the VP using vouchers of the same asset type. Each Issuer sets the value of their tokens, and thus the cost of spending their vouchers. Tokens are earned by the OFS, VP, SDS, and DHT nodes whenever payments, receipts, and other operations with vouchers pass through them, or result in their being asked to store a datum. In this way each of these nodes becomes a profit center for its respective operator.

The VP's operator vets the Issuers, along with the operators of other nodes (such as OFSs or SVMs). These business arrangements can therefore exploit jurisdictional arbitrage, and enforce the compartmentalization of data about users and customers. This by itself facilitates censorship resistance and privacy. For example, note that the VP, SVX, and any SVM (app) will never see an IP address of a user client, since the OFS acts as a built-in proxy. (There is also a separate proxy layer above the OFS, which like the rest of the network does not have a public-facing IP address.)

In fact it doesn't require a massively decentralized network to protect users and their activities, so long as this simple rule is followed: *No entity which knows who or where a user is can know what they are doing; and conversely no entity which knows what a user is doing may know who or where they are*. For example, an SVM which supports online sports wagering will not be able to discern the country of origin of the players. In contrast, building such applications directly on the blockchain, which records the IP addresses of transaction submissions and posts everything to a permanent public ledger, depends wholly on the naive assumption that a given wallet address can never be associated with a player (ever!), in order to provide even a thin veneer of privacy.

Separating Issuance from Clearing

Quite significantly, this architecture also splits the function of minting or issuing money from the payment clearing system. Not only are these logically separate functions, it is also vital that they be legally separate. To see why, consider that if physical cash currency were used in the commission of a crime, no one arrests the officials at the mint where the currency was printed, or even the employees at the bank where the check was cashed, thus putting the bills into circulation. This is simply because those parties can have no possible knowledge about whose wallet those bills end up in, or of how they are spent once the bills have gone into circulation. In the same way, our digital cash vouchers circulate “in the wild,” as a digital analog to physical cash, without any ledger. This is in distinct contrast to blockchain currencies, which maintain a permanent and public ledger of all transactions, and where “miners” both validate transactions between wallets, and also mint new coins via block rewards.

In fact with the OTO currency there are two logical and legal firewalls: first between the OTO voucher Issuer (mint) and the VP (clearinghouse); additionally, the minting function is split between the OTO voucher Issuer and the Ascension Foundation's blockchain, where the Lyra coins backing the issued vouchers are created and will always reside. Those Lyra which are not currently backing vouchers may circulate freely on the Ascension blockchain itself. Moreover the blockchain can also be used for those functions and circumstances where a distributed public ledger is actually highly desirable, such as: documenting the total quantity of Lyra coins in existence; or the portion of Lyra which is presently circulating in OTO voucher form; or publishing the results of games having a random component, in order to render them provably fair.

The Best of Both Worlds

Through a licensing agreement, the Ascension Foundation is able to combine blockchain technology with the technology layer provided by Voucher-Safe and SilentVault. By means of this combination the most important benefits of a blockchain are preserved, while the drawbacks are mitigated. Viz.:

- Mining on the Ascension blockchain can be used to mint coins and validate transactions, including smart contracts. Because a permissioned blockchain will be utilized, the mining function will be contracted out to sufficient geographically dispersed pools to provide adequate decentralization. (User clients will be able to run full nodes that do not mine.) This eliminates problems with hard or soft forks, uptake of software updates, and the dreaded 51% attack. All mining pools will operate under a binding business contract with the Ascension Foundation.

- Blockchain cryptocurrencies are often called digital cash, but this is a misnomer as they do not exhibit the characteristics of physical cash, specifically fungibility and anonymity. But cryptocurrency circulating in voucher form (not just Lyra but also BTC, LTC, etc.) *is in fact true digital cash*, which works analogously to physical cash. Just like a billfold, a wallet can contain many different voucher types side by side. Wallets cost nothing to create, and absolutely no identifying information attaches to them, not even an email address.

- For a detailed list of further problems with Bitcoin (and other "raw" cryptocurrencies) which are solved by means of the digital cash voucher architecture, please see this essay. *(107)*

- Because the voucher network is already deployed, purchasers of OTO vouchers can take possession of their OTO immediately, and circulate them to others, before the Ascension blockchain is even initialized with its "genesis" block. (This is an ongoing project with a white paper, not a project consisting of a white paper.)

- The voucher network can scale as required simply through the addition of more hardware, and possibly also via future software changes to optimize clustering. In this characteristic it is similar to other systems with centralized clearing, such as PayPal or Visa.

- "DApps," or distributed applications, can be deployed right inside the wallet client by implementing to the SVM API, eliminating the need for websites which can be shut down, or domain names which can be seized, or external "app stores" where certain kinds of apps (e.g. crypto wallets) may not be welcomed. All client code has published source, including plugins to support the client side DApps. The Ascension Foundation may also permit certain DApps to create additional OTO supply (on the server side), and add it to the total in circulation according to stipulated rules.

- Most cryptocurrency wallet clients have no chat capabilities, or at best a crude one bolted on as an afterthought. The wallet clients used for OTO originated as open source instant messaging

clients, to which special-purpose plugins have been added in order to support wallet operations. This means that OTO users can not only spend to one another, they can also chat with one another, either one-on-one or in chat rooms. Secure chat is supported using OTR (Off The Record). Drag and drop file transfer, bookmarks and contact lists, and a host of other standard instant messaging features are also supported. (Even p2p voice chat can be supported, but isn't configured yet.) Our user community is meant to grow as a community, and our tools are designed from inception to facilitate this growth.

- Our network was not designed as a lab experiment, but rather from a business perspective, informed by the history of the digital gold industry in the 2000s, and earlier ledger systems such as Loom *(108)* and Truledger. *(109)* The fact that there are economic incentives for all of the entities, which have logically separate functions, allows for competition and decentralization via the business model, while still preventing the "tragedy of the commons" issues that have plagued Bitcoin. This avoids single points of failure or censorship, while allowing the Ascension Foundation to steer future technical development and monetary strategy for its own currency(-ies). Naturally, other currency Issuers on the platform can of course do likewise.

A Superior Hybrid Concept

Contrary to prevailing belief, completely decentralized cryptocurrencies lacking a proprietor to steer them and keep them competitive, are *not* inherently superior to systems utilizing centralized payment clearing. Not only are decentralized currencies necessarily less efficient, inevitably exhibiting scaling problems which are extremely hard to solve, but their need for broad consensus as a prerequisite to make any changes is clearly inhibiting their flexibility, and hence their growth. (Except for growth in price, as institutional money *(110)* begins to chase "alpha" into the cryptocurrency space.) *(111)* Moreover from a privacy perspective the blockchain spells the end of all financial and transactional privacy. It's been fairly called the beginning of the cashless control grid. This is a leading reason why governments and big banks love blockchain tech, and today are seen starting up their own blockchain projects. Potential solutions from within blockchain tech are perhaps possible *(112)*, but still years in the future.

Ascension offers a hybrid approach: issue the coins on a distributed private blockchain, but then add an application layer above the blockchain which provides the benefits of centralized clearing, along with strong privacy, plus the tools to support natively a community of users and merchants. This will allow the Ascension Foundation to construct the demand side for its currency, at the same time that the supply side is constructed, both via token sales and by other methods. Since the value of any currency – even the mighty US dollar – is predicated on achieving a balance between supply (money creation rate) and demand (level of economic activity using that currency), new OTO/Lyra released into circulation will be balanced by simultaneously providing markets and apps where it can be utilized by its holders. In this way a stable private ecosystem can be developed around a privately issued money, much as the brilliant Friedrich Hayek envisioned more than 40 years ago.

IV. Lightweight Client Architecture

Our existing wallet reference client for the V-S/SV system was first deployed in 2014 and has been maintained and enhanced ever since. It is based on the Spark *(113)* open source XMPP client, which supports a plugin architecture. We have forked the Spark 2.7.7 source tree, made some customizations for branding and login, improved support for anonymous users, and implemented the wallet and SVX/SVM API functionality as plugins. This means that our client is also a full-fledged Jabber chat client with an existing library of community-produced plugins, and a large user community. (Spark has seen nearly 7 million downloads in its 10+ year history.) All source, including for all plugins and libraries, is open source (published under the Apache 2.0 license), and we provide tools to build one's own client from source code if desired.

The footprint of our wallet client is therefore extremely light, requiring no large data downloads and synchronizing with the network in only seconds following login. While it is now possible to do Jabber chat using browser plugins – thus making a separate dedicated program unnecessary – we do not consider it possible to provide a truly secure wallet client, which controls and manipulates private keys, within a browser plugin context. This is because browsers are bloatware with large attack surfaces, and also because hostile plugins (aimed at stealing keys and passwords) may be running within the same process address space on the device. Operating systems typically provide better firewalls between processes than what is achievable within a single process (the browser).

There is also a benefit to having all of the client-side code running on the local device. It has become fashionable for Ethereum wallets to deploy some of their code as "libraries" on the blockchain, similar to Windows ".dll" or Linux ".so" files. This sounds good in theory, because blockchains are supposed to be immutable, but globally shared state and self-modifying code can bite back hard, as shown in this recent terrifying example with the Parity wallet. *(114)* (It now appears that this problem with coins lost due to a software error may be fixable only by means of another hard fork *(115)* of Ethereum.)

In keeping with security concerns, our clients generate all keypairs on the device, but do not store them there. Instead the private key (along with certain random hashes used as data storage indexes for wallet data) is wrapped up into a login data block, encrypted again using an input passphrase, and stored in the cloud at a hashed location. Unlike most cryptocurrency addresses, our wallet IDs are human-readable, resembling an email address, in the format <handle>-<sequence number>@VoucherPublisher. An example would be: *bob-8642@vouchi.com*.

The user picks the handle (e.g. "bob") while the system appends the differentiating sequence number, and the @publisher indicates the "domain" space in which the wallet was created. The user also selects a PIN, and two passwords: a "long-phrase" and a "passphrase." The wallet ID + PIN is used to build a hash which accesses the long-phrase storage, so that the OFS gateway server cannot determine which wallet is attempting to log in. The alphanumeric long-phrase is always entered via a drop-down menu, only for the three characters randomly selected on any given login attempt. The passphrase is never transmitted over the network at all, but is used to decrypt the login block once it has been successfully

retrieved using the long-phrase. This three-step login mechanism is more complex than a typical login/password procedure, but its very complexity removes any need for two-factor authentication. We consider two-factor wallet logins an unacceptable risk to privacy, because they link a wallet to an email address or phone number, which may itself be tied to a real life identity in third-party databases. Also, phones and email accounts can be hacked and taken over by a variety of methods, making two-factor security of limited actual value.

Wallets can contain and manipulate vouchers from any Issuer on the VP's network. Transaction fees are paid by means of “tokens,” micro-vouchers which are purchased and used automatically by the wallet as required. The network provides built-in pricing data in a large variety of national fiat currencies, precious metals, bitcoin, and litecoin, within a few minutes of the current global market. This makes it transparent for wallet users to spend an amount denominated in national currencies, e.g. US$19.95 worth of bitcoin, C$50 worth of OTO, etc.

A common problem with cryptocurrency wallet clients is that if the passphrase unlocking the wallet is lost, so are any coins in that wallet. There is essentially no recourse if this happens, unless your wallet client or hardware device has a known vulnerability which you can exploit. *(116)* (But in that case, so could somebody else.) We have solved this problem by means of implementing five recovery questions. Instead of picking one and asking for a duplicate answer, our technique hashes the wallet ID together with the user's answers, and encrypts a recovery block using the hash, which is then stored at the hash of that hash. The five questions are specified by the VP, and are thus the same for all wallets in its address space. The user can of course supply any answer to the questions, thus allowing one passphrase repeated five times (often called a “brain wallet” as it's easier to remember), or up to five distinct passphrases. Thus to recover wallet login credentials the user needs to remember only their wallet ID and their recovery passphrase(s). (It is also possible simply to give a “correct” answer to each of the five questions, but less secure wherever someone else could perhaps intuit the user's answers.)

There is also a test network publisher, “*@voucher-safe.org*” where practice wallets can be created and “play money” currencies can be obtained and spent at will. This network is also used for beta testing of server-side upgrades and enhancements, for demonstrating new Marketplace DApps, and the like. In function and intent it is similar to the TestNet offered by Bitcoin, Litecoin, and many other altcoins. However it does not require any blockchain downloads for access, merely that the “Test Network” box is checked on the client login screen.

User-configurable preferences are stored on the local device, as are any non-anonymous XMPP logins which the user may create on that device. (It is difficult to build a friends list to utilize the “presence” features of a chat network when everyone logs in with a random, not-repeated login handle every time.) However nothing wallet-related is ever kept stored on the local device, nor associated with any chat usernames. Because of this, our wallets can be accessed safely from multiple devices. (In fact the server side cannot even detect what kind of device the user is operating.) We consider this the best way to cross borders with cryptocurrencies. Making temporary, low-bandwidth connections using the XMPP protocol is hardly a red flag that one is a cryptocurrency user in the first place. Nor is having an

innocuous instant messaging client installed on your device.

In the cloud, all vouchers and receipts are stored at random hashes generated along with the wallet's private keys, and encrypted using the wallet's public key. This means that even someone who gained access to the SDS's database would be: 1) unable to identify which objects belong to which wallets; and 2) unable to read any of the data anyway. Even if a wallet's private key were compromised, that by itself would not enable the hacker to spend any of the wallet's contents. Wallets only have read-access permissions to their vouchers. Write access is only by the Voucher Publisher (VP), which requires the wallet's unique read-write capability passphrase, to supply to the SDS to gain folder update permission. This passphrase is stored in the wallet's login data block, but encrypted using the VP's public key, *not* that of the wallet. This means that a wallet's private key, by itself, cannot be used to steal from the wallet. Required is access to the *entire contents* of the login block, which can only be decrypted using the passphrase. Login blocks are stored at hashes which are not associated with the wallet ID by name, but can only be retrieved by building the proper hashes out of the wallet ID, PIN, and long-phrase. The net result of this is that a wallet can be pilfered only if the attacker has access to the wallet's complete login credentials – in which case they could just log in normally! Complete details can be found here. *(117)*

In the event that a wallet's owner believes that login data may have been compromised, the wallet can be evacuated of value and the wallet closed. Closing a wallet causes its public key to get added to a CRL (certificate revocation list) maintained by (and signed by) the VP. The key server (PKS) checks this list before returning public keys for wallet IDs. This means that one cannot accidentally spend to a closed wallet. It is of course impossible to spend to a wallet which does not exist at all.

One *can* spend to a wallet whose login credentials have been lost by its owner. However unlike in the blockchain world, where this is fatal and results in coins being lost forever (known as a “dead wallet” spend), in our system the spend becomes recoverable by the payer after a configurable 1-7 day pick-up window has elapsed. All voucher spends are made in two-phases: 1) the payer posts an encrypted voucher for the payee on the DHT (temporary storage hash table); and 2) the payee picks up the payment off the DHT by exchanging it immediately for a fresh voucher at the VP, and then generating a receipt for the payer, which is likewise posted on the DHT, encrypted for the payee to find and pick up. This mechanism makes dead wallet spends impossible, because they can always be recovered. Since receipts are generated and signed by the payee only (never by the VP), the VP which cleared the payment does not see any “memo” or “baggage field” items attached to the payment. Receipts do however serve as cryptographic proof that the payee received the payment. The DHT can be thought of as an inter-wallet message board, where all the messages auto-expire after at most one week.

Receipts retrieved from the DHT can be stored in the wallet, or optionally discarded. Stored receipts can be downloaded in XML or CSV formats, and permanently deleted at any time. Again, this is in stark contrast to a blockchain where wallet owners are not in control of their transaction history data, and cannot purge any records, ever. In our system only the payer and payee see the transaction details. The VP sees only the wallet IDs and the amount spent. (It stores only a hash of this information, which is purged once the payment has been either picked up or recovered.) The relevant voucher Issuer sees

only a request from the VP to exchange some number of input vouchers, listed by serial number and amount, for a number of new vouchers (usually two) which sum to the same amount. It has no idea which wallets are involved in the transaction. All VP<->Issuer communications take place using public key encryption (RSA-2048) over a RPC-JSON interface secured by TLS. (The TCP connection may be made over a VPN as well.)

All client connections to the network are always secured by mandatory TLS, and, where wallet-related messages are concerned, these are always end-to-end encrypted using 2048-bit RSA. The OFS (gateway) nodes act as a proxy to the VPs, to Exchanges, and to Marketplace DApps. Because of the end-to-end encryption, an OFS has no idea of the details of the messages it is proxying. Curiously, so-called “cryptocurrencies” actually aren't encrypted, in that network traffic is always sent in clear-text. In our voucher layer, everything is encrypted at least once, and then sent over a secure connection.

The overall intent of this robust design is to achieve these goals:

- To hide as much of the complexity as possible from users.
- To make wallets as reasonably hack-proof as possible.
- To minimize and compartmentalize the damage a hostile party can do, even if that party is a network “insider” such as the operator of a VP, Issuer, DHT, etc.
- To make network eavesdropping by third parties extremely difficult and not very rewarding.
- To make wallets friendlier than on blockchains, with human-readable addresses, lost credentials recovery features, and user control of transaction history.
- To lighten the footprint of blockchain clients so that wallets can be accessed safely on any device (even devices not belonging to the wallet's owner).
- To anticipate and circumvent potential protocol blocking and national firewalls during any future crackdown on cryptocurrencies.

We believe these goals have been achieved fairly well.

Future Client Plans

Having said all of this, it should be noted that our existing wallet client is merely a *reference* client. This means that it demonstrates and fulfills all of the requirements for a network client, with fully documented and commented code meant to serve as a functional example. For user friendliness and usability, we believe that it compares well with other popular wallets, such as Jaxx. *(118)* However this is not to say that it is the ultimate client, the best that could be conceived, or the like.

For one thing, the Spark client UI was originally designed some ten years ago, and despite our look and feel improvements, is beginning to look a little dated. However rather than abandoning Spark, it is our hope to provide it with a new skin, and thus contribute back to the Spark open source project in a major way. We also provide an older (but functionally equivalent) Java web-app version, which supports only the wallet-related functions but not the chat client functionality. (Basically, it's the plugins extracted

from Spark to run stand-alone.) There is also the original Voucher-Safe CLI client (command line interface). The CLI was used as the basis for creating the headless "cloud wallets" that are utilized for accessing escrow wallets in the SVX server and in the OnionPay merchant gateway.

Besides updating Spark, we plan to support the development of two entirely new wallet clients:

1. An Android application.
2. A web-based portal which can be accessed using any suitable browser.

Since the existing clients are written in pure Java, and the XMPP client library (Smack) *(119)* has been ported to Android already, the Android port should be mainly a matter of redesigning and replacing the UI entirely, according to best practices for wallet app UIs on Android.

While it must be observed that a web wallet version will inherently be less secure (both because it runs in a browser, and because as a thin client it may push certain sensitive operations up to the server-side), it should also be noted that most cryptocurrency users access their wallets by exactly this means. Comparatively few run Bitcoin Core or other heavy, native-mode clients. We consider that it is our job to provide options to users, not to dictate to them, and that our wallets will still have comparatively greater security that most others even when operated in this format. A web portal also gets us iOS device support, without needing to rewrite everything in Objective C.

Ultimately, it is our hope that open source third-party clients will eventually emerge that give any reference client produced by our in-house developers a run for its money. Indeed that would be a good criterion for the success of our wallet system.

V. In-wallet Exchanges and Marketplaces

Most cryptocurrencies rely upon external exchange platforms (example: ShapeShift) *(120)* in order to trade versus other cryptocurrencies, or against national fiat currencies. Because our technology is money agnostic, and therefore can make circulating digital value out of anything, we are able to achieve this capability internally. We have developed an anonymous p2p exchange API with escrow backing, and deployed it on a separate tab inside our existing wallet client. At present there is a single "SilentVault Exchange" operating (SVX1), so the drop-down list in the wallet offers but a single choice. In the future independent operators will be able to operate their own exchanges on this list. They will compete with each other on the basis of price (escrow fees) and voucher currencies supported. In this way the user community wins twice: first, by obtaining the best service for the lowest price; and second, by providing decentralization via the business model.

By agreement with cryptocurrency Issuers within our wallet system, an SVX can also sell (or repurchase) vouchers directly for other cryptocurrencies. For example the existing SVX1 sells SBC vouchers for BTC, SLC vouchers for LTC, and OTO vouchers for either BTC or LTC. This capability

to do automated voucher minting for suitably confirmed payments on one of several blockchains is an integral part of the SVX API. Future SVX franchises could in theory be dedicated to acting as a portal for conducting an ICO, even for a blockchain that (like Ascension) does not yet exist. The only implicit requirement would be that the vouchers so created would be redeemable for an equivalent quantity of coins on the blockchain once it is launched (as OTO vouchers are redeemable for Ascension's Lyra coins).

The SVX API can of course be extended in the future. In particular, once the Ascension blockchain has been initialized it will become possible to add support for "atomic swaps" between the Ascension blockchain and other blockchains. An atomic swap is a mechanism by which coins are spent on one blockchain, but cannot be spent by the recipient until a corresponding spend of coins has been made on the other blockchain (or a timeout occurs, reversing the spend). Basically, Alice spends coins to Bob on blockchain A, but Bob cannot move those coins until he makes a corresponding spend of coins on blockchain B to Alice. The main problem with this mechanism is that it isn't at all private; the spends on both blockchains are publicly associated. (For that matter, all exchanges performed via ShapeShift are published as well.) It is conceivable that protocol changes could be made to Bitcoin and other blockchain currencies, which would alleviate this concern. For example, MASTs (Merkleized Abstract Syntax Trees) could be deployed *(121)* to make atomic swaps have an acceptable level of privacy protection. But in the near term it seems clear that p2p exchanges will continue to play a major role *(122)*, even if fully decentralized exchanges *(123)* become a reality. Our SVX technology is p2p today and will evolve toward full decentralization in the future. (We consider decentralized exchange a "killer app" in itself.)

We have also developed a Marketplace API. The SilentVault Marketplace (SVM) API defines messaging protocol mechanisms for basic functions such as connecting to a Marketplace app, logging into it securely (via wallet ID + a PIN), and transferring value (in supported voucher types) between the wallet and an account in the Marketplace DApp. Each SVM DApp may extend this base set of message definitions to access its unique functionality. Client support is provided by a special plugin developed by the SVM DApp operator, who also creates the plugin for the server side. Source code for client plugins must be published; source publication is optional for the server plugin.

We have written and beta tested a coin-flipping game using a modified Martingale *(124)* wagering algorithm. This SVM DApp is called "ABC" (for Aleatoric Binary Challenge), and is presently deployed on our test network, with live deployment expected in the next few months. This is a complex but amusing betting game based around the concept of betting insurance, in which if you win you win bitcoin, but if you "lose" you win OTO. Significantly, OTO is created to "make whole" those who go bust under the Martingale strategy. ABC is thus an example not only of the sophistication that is possible using our in-wallet API, but also of the concept that expansion of the monetary base ought to occur from the bottom up (individual users), rather than from the top down (governments, banks). Naturally, there are built-in guardrails to ensure that monetary growth from this source will never become excessive.

We do not anticipate that the Ascension Foundation should or would develop the majority of future

SVM applications. On the contrary, the intention is for third-party vendors to purchase SVM franchises and develop their own applications: stores, other games, possibly trading and investment markets, various services, virtually any business proposition that can be represented in an electronic mall. As our user base grows, the value of an entry in our wallet Marketplace drop-down list will increase. Also note that more than just our own currencies such as OTO/Lyra are in play within the SVM. For example, SBC/BTC and SLC/LTC are already supported. OTO/Lyra is pegged to the current retail market price within SVM DApps. Our job is to provide the mall and maybe an anchor store or two, and then let other entrepreneurs do the rest. (Ideally, our "anchor stores" would themselves be spun off to independent owners in the future.) Nevertheless we do plan to develop in house a few more SVM DApps. These will include:

- Q13, a simplified ABC variant also using the InsurBucks insurance currency concept. (A simulator for this application already exists.)
- SportsTrader, a p2p sports betting app, featuring the SportsBucks currency.
- A Binary Options trading app, featuring the TradeBucks internal currency.
- A CFD (contract for difference) trading app, again utilizing TradeBucks for insurance.
- Other similar iGaming or trading concepts may be realized, depending upon the success of these.

Please see our Roadmap (Section XI) for the projected development schedule.

VI. The Ascension Blockchain: Private, Permissioned, and Performant

Consider the diagram below in Illustration 3, expanding the Ascension Blockchain component shown in Illustration 2.

Key:
The black arrows indicate public blockchain messaging.
The green arrows indicate private blockchain messaging, inside of a VPN.
The red arrows indicate legal contractual relationships.

The Ascension blockchain will be forked from the latest open source version of a first generation blockchain. The most likely candidates for this, in descending order are: Ethereum Classic (ETC), Ethereum (ETH), Bitcoin (BTC). ETC retains a PoW mining mechanism, and will not be transitioning to PoS through the adoption of Casper. Bitcoin does not support Turing-complete smart contracts, but basic contract types are available through Ivy. *(225)* However it does support recording non-transaction data in the public ledger (as exploited by Factom *(125)*, among others.) There are also projects meant to bring smart contracts capabilities into Bitcoin, such as RootStock. *(126)* Given that we are ambivalent about the wisdom *(127)* of supporting Turing-complete executable code on a blockchain to begin with, we may elect not to support smart contracts. At the very least they will be will be very tightly controlled (as described below), if they are supported at all. Even the adoption of

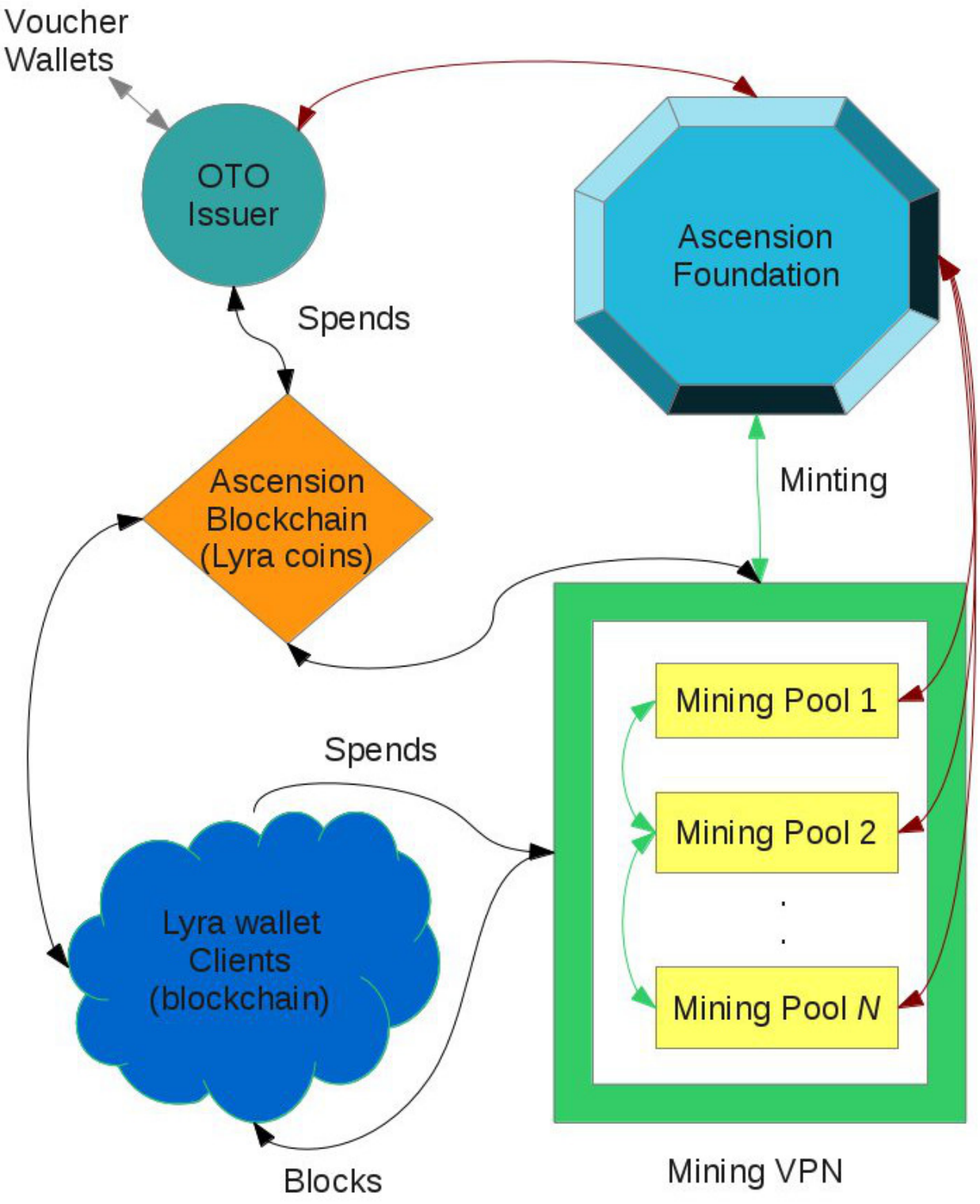


Illustration 3: Ascension Blockchain Architecture

SegWit presents a minor problem in that it makes it impossible to validate a blockchain transaction after the fact without reference to separately stored extension blocks. This is plainly sub-optimal unless block space limitation is a problem, as it was for BTC (but will not be for us). At least SegWit also

fixes transaction malleability. *(128)*

The reason for this fundamental uncertainty about blockchain source is quite simply that the industry is in such a state of flux that a choice made today may prove to be a foolish one only a few months from now. Since we do not intend to deploy the Ascension blockchain sooner than 4Q2018 at the earliest (and do not have to be in a rush to do so since we already have a working system above our future blockchain), making a final choice at the time of this writing strikes us as unwise and unnecessary. It is even possible that a dark horse platform such as EOS, BCH, or Omni *(129)* (or something else yet to be released!) may yet be adopted instead. (EOS however has a very naive and troubling attitude *(232)* regarding privacy.)

In any event, whichever starting point is ultimately selected, we will then customize the functioning of that blockchain's software to implement the following operational parameters:

1. The validation (mining) of blocks will only be accepted from network nodes which meet these criteria: a) are in possession of a signing key whose corresponding public key is on a list of authorized validators; and b) submit their block from an IP address on a private VPN.

2. All mining nodes will also offer public-facing IP addresses for connection by non-validator client nodes, discoverable via the usual DNS seeds mechanisms. Messages between validating nodes will always travel over the VPN, in order to improve security, and evade national firewalls and potential packet censorship. (A VPN failure fallback to public IPs is allowed.)

3. Mining pools (hereinafter just “miners”) will be under a legally binding contract with the Ascension Foundation (AF). Per the terms of this contract, they will provide to the network a specified minimum amount of hashing power, with a reasonable uptime guarantee. They will adopt and install software upgrades on a schedule stipulated by the AF. Miners will be established on all continents except Antarctica, in sufficient numbers to provide adequate redundancy and censorship resistance. VPN access will be provided to them by the AF.

4. Miners receive block transaction fees for the blocks they mine, but will not receive block rewards when they mine a block. Instead, each miner will be paid a fixed sum of Lyra (the coins used on the Ascension blockchain) each day they are online, calculated as a prorata share of the AF daily mining budget, based on the percentage of total network hashing power being provided by that miner. The AF will recalculate its mining budget periodically, based on such factors as changes in total hashing power, number of miners under contract, and the price history of Lyra versus a basket of other currencies.

5. Miners will agree not to mine any other cryptocurrency, including merged mining, using the same dedicated hardware they are providing to the AF network. They may mine other currencies as they like using entirely separate hardware. This proviso should eliminate the problem described here. *(130)*

6. Minting of new Lyra shall be conducted by the AF exclusively. This shall be done by means of a 'mint directive' message broadcast to miners, specifying the number of new coins to be created in an upcoming block (by default, the next block). This message must originate within the VPN and is a multi-signature transaction which must be signed by a majority of minting keys, established for this specific purpose, which are controlled by the AF board. This number of coins effectively becomes the “block reward” for the indicated block, with the distinction that the new coins will be paid to an address also belonging to the AF, instead of to the winning miner. (As noted above, miners do earn and retain the fees for transactions in a block.)

7. When the Ascension genesis block is created, the number of coins specified in the very first 'mint directive' will specify, at minimum, an amount of coins equal to the total quantity of OTO vouchers then in circulation, plus the required backing for any other voucher currencies backed wholly or fractionally by Lyra. Thereafter the quantity of Lyra minted over time will reflect increases in circulating OTO and related (Lyra-backed) currencies, together with the implementation of the monetary goals of the AF board. It is likely that most blocks will lack a minting directive associated with them, thus the number of new coins per block will often be zero.

8. Block size will initially be set at 1MB, with blocks occurring on average every 60 seconds. Given the available hash rate across all miners, the difficulty will be manipulated as required in order to maintain the desired block rate. Difficulty can be auto-adjusting, or explicitly set by AF. Block size can only be changed by means of a scheduled software update, to take effect as of a specific block number.

9. Blockchain wallet clients operated by users (defined as any node without validator permission) will connect to public-facing IP addresses of miners, and of one another. All TCP/IP connections will be secured via TLS using self-signed certificates. (The point here being to transmit data over encrypted connections rather than to authenticate anonymous parties.) TLS will also be supported for RPC/JSON connections. User clients will be able to download all past blocks, and submit transactions to the network, denominated in Lyra, with fees also offered in Lyra, in the usual manner. A suitable threshold for minimum spends and/or fees may be specified in the software, in order to prevent nuisance dusting attacks. While users will not be required to install every software update released by the AF, wherever the changes in a new release require it, the Satoshi number of releases below a certain level will no longer be accepted when connecting to other nodes which have upgraded. Users with too-old versions will be notified that they need to update their software.

10. Smart contracts (defined as any code posted to the blockchain meant for execution by other clients), can only be submitted into a block using a signing key duly authorized by the AF. Before authorization will be given, the smart contract code must be reviewed by AF staff, and a fee paid to the AF (in Lyra) for the code review and publication. Importantly, this will allow the AF to vet projects such as ICOs, hopefully preventing this problem *(131)* from occurring. Data publication in a block, other than of executable code, will not require any special

permissions.

11. In order to implement the permissions system outlined above, a versioned permissions block will be posted on the blockchain, and periodically updated. Each version of this JSON block will specify the list of public keys whose corresponding private keys are associated with particular permissions. For example, the keys belonging to the members of the mining pool, the keys permitted to publish smart contracts, the keys belonging to the AF for use in official mint directives, etc. Each permission block will specify the block number at which it becomes effective. Like mint directives, permission block updates must be signed by a majority of master keys belonging to the AF (whose fingerprints in this case are also hard-coded in the software). This mechanism allows for miners to enter or exit the system, for example.

12. The OTO voucher Issuer (OTO.Money) *(132)* manages ordinary client wallets holding at all times sufficient Lyra to back fully (100%) all OTO vouchers currently in circulation. When OTO is sold to the public, OTO.Money will purchase enough Lyra from the AF to cover any shortfall. The AF will satisfy the purchase either by transferring existing Lyra from wallets it controls to OTO.Money's wallets, or at its option create the new Lyra first via a mint directive, and then spend it to OTO.Money. Whenever a voucher wallet user redeems an OTO voucher for Lyra, OTO.Money will destroy (decirculate) the surrendered voucher and spend an equal amount of Lyra from its blockchain wallet to that of the redeeming user. Any additional voucher Issuers, now or in the future, who back their currency with Lyra, will operate in a similar manner. The AF will require periodic audits of Issuer reserves. Thus this is shown on the chart as a legal contractual relationship.

13. A voucher Issuer such as OTO.Money may utilize an SVX as a sales portal to privately receive BTC, LTC, or other cryptocurrencies as payment for vouchers sold. They may also designate independent sales agents, such as CryptoWealth.com *(133)*, to help them conduct their business. Regardless, the relationship at the blockchain level will remain between the Issuer and AF.

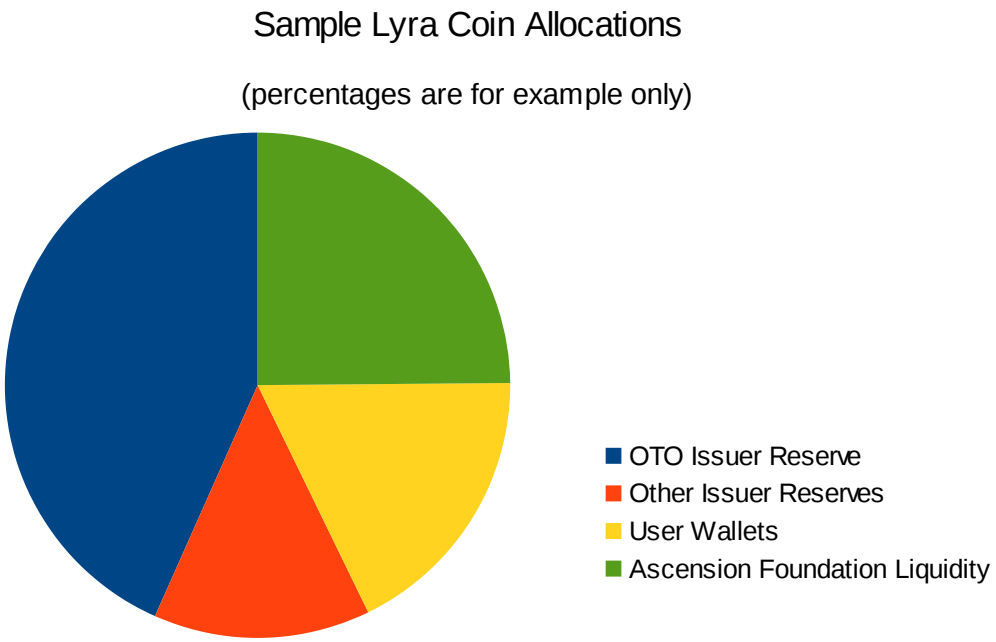
14. The AF will monitor market conditions in order to make periodic adjustments to hash rate, mining budget, difficulty, block size, and the Lyra growth rate. The goal is stable liquidity. A payment system needs stable liquidity, and that stability cannot be reached if you aim to be a payment network before you are an established asset.

Operating the Ascension blockchain and surrounding ecosystem according to these rules and guidelines should facilitate the fulfillment of our mission statement: "**To promote the growth of robust, borderless, wealth-generating, free market ecosystems**."

Once the blockchain is operation, the categories shown in the chart below describe the possible disposition of minted coins (note percentages are samples only).

The AF will of course maintain monetary reserves in currencies other than Lyra, including cryptocurrencies, precious metals, and fiat currencies.

An example of possible deployments of Lyra coins on the blockchain is illustrated in the chart below:



VII. Crypto-economic Monetary Engineering

The growing cryptocurrency market (now around US$600 billion in aggregate market cap) is much more than just a speculative craze. *(134)* It is rather the tip of the spear in a vast transformation *(135)* of the global economy, incorporating what can justly be described as the crypto-economy. The internet revolution of the 1990s successfully integrated the online economy into the global economy. Analogously, the cryptocurrency revolution of this decade will successfully integrate the crypto-economy into the sphere of global economic activity.

The crypto-economy represents the next generation of finance, destined to replace most current systems *(136)* for payments, banking, currency exchange, stock markets, credit and debt markets, commodities markets, international trade, shipping, warehousing, inventory control, even the issuance of currency itself -- traditionally the exclusive province of nation states. *(137)* The legacy system *(138)* is not only corrupt to the point of putrescence *(139)*, but is also centralized, anti-competitive, and top-down. The new crypto-economic system is decentralized, competitive, and bottom-up. The legacy system is highly politicized, while the new system is essentially post-political.

What are the monetary engineering goals for a privately issued currency in the crypto-economy? (We call it “monetary engineering” in preference to “monetary policy,” because policy sounds political,

implying decisions made for the benefit of some particular group, while engineering connotes rational decision-making based on specific facts and circumstances.) Goals should be simple, and non-conflicting. We've identified these goals:

1. Supply of the currency should be adequate to provide the float necessary for ongoing economic activity conducted in the currency, plus other uses such as loans, savings, investment, and R&D.
2. Demand for the currency should be adequate to allocate supply.
3. Net growth should occur from the bottom up, not from the top down.
4. Exchange rates, measured against a basket of fiat currencies, should exhibit long-term stability.

Supply is increased (new coins minted) in three ways: by coin sales into the market, in exchange for fiat currencies or other accepted cryptocurrencies; by coin creation in the context of the operation of certain DApps; and to pay for labor undertaken for AF projects. The first minting function, coin sales, is described in section VIII below. It is noteworthy that this is not an ICO, because there is nothing "initial" about it. The sale is uncapped and ongoing, limited only by market demand. The second function, minting in a DApp context, is limited in scope and typically tied to an insurance function.

For example, in the Q13 game a modified *(140)* Martingale wagering algorithm is used, in which wagers made in OTO are balanced by wagers made in an internal insurance currency called InsurBucks (IB), which is purchased with OTO using a fraction of the bankroll deployed. If you lose 13 tosses in a row, you have "gone bust" and so your bankroll will consist of zero OTO plus a quantity of IB. Your IB is then redeemed for fresh OTO out of the insurance pool. Whenever the pool's reserves are insufficient to make the losing player whole, new OTO is created by Q13 as needed.

Similarly in the ABC coin-tossing game, BTC is wagered in a Martingale *(141)* model (with a period of seven tosses compared to thirteen in Q13), balanced against OTO. If the player wins, they win more BTC; but if they lose, they win OTO equal to the BTC they lost. If there is a net deficit in OTO available to the ABC DApp, it creates fresh OTO as required. The net result of ABC's algorithm is thus that winners increase their bitcoin, but losers exchange bitcoin for OTO/Lyra. (Thus losing players merely sustained a conversion rather than a true loss.) More detailed information on the ABC game algorithm and its user-settable parameters is available separately.

These games are meant to implement the concept of economic mutualism *(142)*, but in a very different way than what is found in the current fiat monetary system. In that system, large politically-connected players are enabled to privatize their profits (winnings) while socializing their losses onto the public through bailouts and inflation. In our system, losses are "socialized" through inflation, but with the benefit flowing directly to individual users. Moreover this is not done by order, but only when a *bona fide*, quantifiable loss has occurred as a random event. This represents bottom-up currency creation in small increments, rather than top-down creation in large quantities offered only to privileged institutions. It is well known that those who are closest (i.e. get first access) to the new money being created reap the main benefits. *(143)* Keep in mind also that our blockchain system is *not* generating a supply of coins via block rewards to miners (who are paid differently). Applications such as Q13 and ABC are examples of what we intend to do instead. We anticipate other game developers (and non-

game app developers) to set in motion similar opportunities for creation of new coins. (Given appropriate guardrails of course.)

On the demand side, the AF will foster the development and deployment of DApps and other portals where OTO/Lyra can be utilized. Initially, some of these will be developed in-house; but it is intended that third party licensees will ultimately develop and operate the vast majority of them. We also expect that once there is a large quantity of our coins in circulation, it will become useful outside of our own wallet ecosystem, and thus become an accepted form of payment generally. At some point it may even become useful for modulating cross-border capital flows.

The AF will monitor all of these data points: rates of new sales, monetary growth in DApps, total coins deployed within DApps, currency velocity within both the voucher system (OTO) and the Ascension blockchain (Lyra), the willingness of users *(144)* to hold balances, and price history in secondary markets. It will then correlate these data with long-term exchange rates versus a basket of other cryptocurrencies (private or even government-issued), to use as a feedback signal in order to arrive at a bias for net expansion or contraction of the supply, and to determine the rate at which this should occur.

The AF will retain certain reserve levels in various currencies such as BTC, arising from the proceeds of its wholesale sales. Since on a blockchain coins are never actually removed from circulation, whenever the board determines that circulating Lyra should be reduced, the AF will tap these reserves to buy back coins, which it will then hold until circumstances warrant their resale into the market. Naturally the reserve buffer must be well diversified, in order to avoid a situation where a rapid change in market cap by one component asset would exert a disproportionate effect. For the same reason, rebalancing of the reserve components will be undertaken at regular intervals. Since the AF has no goal or mandate beyond relative price stability (for example, economic stimulus or full employment), its monetary engineering efforts will be steered exclusively by the market rather than by politics.

VIII. Ongoing Coin Sale (Uncapped)

Structure of Coin Offering

We are currently in our Presale phase, conducted in a “warm market” consisting solely of personal acquaintances and associates. This phase has already resulted in sales of approximately US $850K, and we intend to continue it until at least a further minimum of $500K has been sold, but not to exceed a total of $3M for the Presale. Buyers of OTO/Lyra in this phase get a price of $0.30 per coin if they purchase in bulk lots of $25K or more, or a price of $1 per coin for smaller quantities. In either case buyers are given a choice: add a 50% bonus in coins delivered immediately; or add a 100% bonus that does not vest until the start of Round 6, in which coins will be sold at $32 ($9.60 bulk rate, see Table 2 below).

Following the completion of our Presale phase, we will commence what we've designated as “Ground

Zero." In this phase a minimum of a further $3M worth of coins will be sold, up to a maxiumum of $30M. The price structure will be the same as for the Presale, but the coin bonus structure will be different, as follows:

Progress toward total sales of $30M	Bonus awarded for purchasers in this block
$0 – 3 M	50%
$3 – 6 M	45%
$6 – 9 M	40%
$9 – 12 M	35%
$12 – 15 M	30%
$15 – 18 M	25%
$18 – 21 M	20%
$21 – 24 M	15%
$24 – 27 M	10%
$27 – 30 M	5%

Table 1: Ground Zero Phase Bonus Structure

Following the completion of the "Ground Zero" phase, there will be at least six further numbered Rounds, depending upon demand. In these phases the discount will gradually be reduced from 96.88% offered in Presale and Ground 0, and be cut by half in each successive Round. Bulk prices will always be 30% of manufacturer's suggested retail price (MSRP). For its use in DApps, OTO/Lyra will be pegged at the MSRP. In addition, the quantity of coins available for sale will be doubled each round. There are no bonuses after Ground 0. At least two independent "funnels" will be utilized for Round sales, each with its own quota. These are: the bulk (or wholesale) funnel, for lots >$25K, and the retail funnel for lots <$25K. Retail packages will be defined at $500, $1500, $3000, $10K, and $25K, and possibly other price points.

In addition there may be a third funnel, for ERC20 tokens (Elyra). These will be sold for ETH on a sliding scale price based on the market price of ether. Elyra tokens will be interchangeable with OTO vouchers, as well as with Lyra coins on our blockchain. Once the Ascension blockchain has been launched, all Elyra ERC20 tokens will be converted to Lyra coins.

The structure of the Rounds envisioned is as follows:

Round	Coins (retail)	MSRP	Coins (bulk)	Bulk Price	Discount rate
1	1,000,000	$1	1,000,000	$0.30	31/32nds
2	2,000,000	$2	2,000,000	$0.60	15/16ths
3	4,000,000	$4	4,000,000	$1.20	7/8ths
4	8,000,000	$8	8,000,000	$2.40	3/4ths
5	16,000,000	$16	16,000,000	$4.80	1/2
6	32,000,000	$32	32,000,000	$9.60	-0-

Table 2: Round Structure

Therefore, a minimum of 126M Lyra coins will be minted between the start of Round 1 and the end of Round 6. This figure does not include those coins minted in the Presale or Ground 0 phases. That number will depend entirely upon the average price at which those early-phase coins are sold. (That is, it depends upon the quantity of sales that are made in bulk versus by means of packages at full retail price.) Our current estimate for Ground 0 mintage is ~60M coins. Any Lyra sold as Elyra ERC20 tokens will represent additional mintage. It will be observed that if one funnel sells out its Round allocation prior to another, it may create an arbitrage opportunity for alert speculators.

Additional sources of Lyra mintage are as follows:

Source of Mintage	*Quantity (range)*	*Special Conditions*
Presale buyers' bonus	0 – 10 M	Vests at $32, or 12/31/19
Staff and vendor compensation[1]	Indefinite (~500K to date)	Management discretion
Team bonus pool[2]	3,333,333	Vests at $16, or 12/31/19
Founder's bonus pool[3]	6,666,667	Vests at $32, or 12/31/19
Commissions on bulk sales	0 – 32.7 M	Requires $300K threshold[4]
Miners' compensation	Est. 1M per year	--
DApps	5% of coins deployed[5]	Requires use in DApp

Table 3: Additional Mintage

Table 3 Notes:
1 – This has become a common practice in the industry. The idea of course is to give paid staff and suppliers of other services a vested interest in the success of the project. Also, to allow contributors to demonstrate the value of their work before a standard paid position is offered. As long as the value of the goods or services provided exceeds the value of the coins, this dilution actually represents a net increase in value to all coin holders.

2 – This pool is meant as a retention incentive to full-time staff, who will receive a proporsional share. Because perhaps 90M coins will be in circulation by the time Round 5 begins, this dilution should not deleteriously affect market prices, even if team members promptly dump most of their coins.
3 – This pool is a reward to the founders for conceiving and successfully running the project. It is separate from the team coin pool, for which founders are ineligible. Because it vests only at $32 (Round 6), by which time at least 132M Lyra are expected to exist, again this should not represent a significant dilution. It will be noted that Founders + Team are together entitled to10M in bonus Lyra, which while significant, is a small percentage (on the order of 3%) of the total number of Lyra which are projected to exist by the end of Round 6 (200M+).
4 – Sales agents referring bulk purchases of >$25K are entitled to receive a commission in OTO/Lyra equal to 12% of the sale, which represents new mintage. However each individual agent must first reach a quota of $300K in total referred sales (excluding their own purchases) to become eligible. It is therefore impossible to predict with certainty how many coins will be minted for this purpose.
5 – As noted elsewhere, certain DApps such as Q13, ABC, etc. will be capable of minting additional coins based on the operating rules of the DApp. The 5% figure is a target only, e.g. if 1M coins were moved by their holders into an application, a target max of 50K new coins could be minted by the app. This figure therefore depends upon the quantity of coins deployed to (used in) any particular application over a period of time. Since we do not know how popular any given DApp will be, this cannot be calculated in advance.

It will be seen that the total number of Lyra introduced into the market from all sources cannot be determined definitively in advance. Our working estimate for the end of Round 6 is on the order of 200 – 250M coins. At a MSRP of $32 this projects a total market cap of between $6.4 and $8 billion. If this were achieved today, it would place Ascension in around 12th position for market cap, between EOS and Dash. Of course, we expect that selling this many coins will require a minimum of at least one year, while the top 10 list of cryptocurrencies changes extremely rapidly on a daily basis as the space grows. It is quite possible that in the event, our successful completion of Round 6 will not even place us in the top 50. In any event we will always publish accurate total circulation figures, via websites until our blockchain is launched, and via the blockchain itself afterwards.

Beyond Round 6, our plan is to continue to sell tokens at a premium price (>$32) to meet market demand, as may be needed. However our expectation is that after that point significant growth in circulation will be accomplished by means of DApps, which will have become much more numerous.

Offering Rationale

The customary practice in the world of Initial Coin Offerings (ICOs) has been to offer a capped quantity of tokens, typically at a sliding offer price, rewarding earlier buyers with a greater quantity of tokens. Open-ended, uncapped ICOs do exist but are widely derided *(145)* in the space. There are two main reasons for this disapprobation. First, raising “all the market will give us” rather than a specific fixed sum determined in advance is seen as evidence of either extreme budgetary ineptitude, or unbridled greed. Second, a non-deflationary currency is seen as monetary treason in the world of blockchain currencies, which as a rule are inherently deflationary. You will notice the Ascension

Foundation's coin sale does not have a predetermined overall cap, although individual Rounds are capped. We believe a hard cap is a poor choice for the kind of economic system we propose to develop, based on the following rationale.

Recall the views of the legendary Austrian school economist Friedrich Hayek, who argued for privately issued money as opposed to money issued by governments or central banks. Hayek concluded that privately issued currencies, competing with one another for market share, would result in a more stable system which would better protect the interests of the users of such currencies. Doubtless he would be pleased at the ease with which various non-governmental organizations are now able to issue what amounts to their own private currencies, using today's technology.

However as Hayek also pointed out, a deflationary (upward-valued) currency inherently favors creditors, just as an inflationary (downward-valued) currency inherently favors debtors. It could certainly be said that a deflationary supply favors *speculators* in that currency, since expanding demand meeting limited supply is bound to lead to a net rise in the price. But if we're talking about the currency being used as exchangeable value to support economic activity, beyond mere speculation and use as a reserve asset (which we must be, else there's little point to cryptocurrency on a long-term horizon), then a currency with an inherent deflationary bias is no better than (or just as bad as) a currency with an inherent inflationary bias.

Consider this question. If a cryptocurrency such as Bitcoin, Litecoin, or Ethereum were truly going to replace the dollar, euro, yen, or pound, then among other things it would need to be used to make loans. This is true even in a Rothbardian world entirely without fractional reserve banking. Looking at the past year's price charts of any of these currencies, who in their right minds would take out a loan (even a short-term interest-free one) payable in BTC, LTC, or ETH? Only a complete fool would do this, as they'd likely end up repaying a multiple of their principal on a purchasing-power basis. Speculators love these currencies today, but no sane person would ever use one of them to purchase anything which needed to be financed in that currency. Even providing intraday credit *(146)* for trading presents challenges. (Credit itself however, aka waiting to be remunerated, is a feature not a bug.) *(231)* Money holding substitutes for lending as a vehicle for savings (a problem long known to economists.) *(147)* Moreover, as the price consistently rises, holders become reluctant to spend that currency. This is the exact opposite of a currency experiencing hyperinflation, which people tend to convert to physical goods as soon as they receive it.

This illustrates how a deflationary currency can be quite unsuitable for actual economic activity *other* than investment. Even handling several months in the pipeline for goods could be highly problematic, given enough volatility, much like with a currency that's undergoing hyperinflation (such as the Venezuelan Bolivar). The difference is that the inflationary currency with the eroding value punishes manufacturers and wholesalers (leading to empty shelves), whereas the deflationary currency with the skyrocketing value punishes retailers (leading to no shelves at all), and even hurts customers who miss out on future gains by spending their coins today. Fortunately, at present everyone can convert in and out of fiat dollars, or other currencies, whenever they wish -- which is precisely the service provided by bitcoin merchant service providers such as Coinbase. *(148)* (Most online merchants don't “take

bitcoin," they take fiat into which bitcoin is instantly converted for them.)

Bitcoin's price trajectory since it's inception has been as follows (data courtesy of Zero Hedge):

- $0000 - $1000: 1789 days
- $1000 - $2000: 1271 days
- $2000 - $3000: 23 days
- $3000 - $4000: 62 days
- $4000 - $5000: 61 days
- $5000 - $6000: 8 days
- $6000 - $7000: 13 days
- $7000 - $8000: 14 days
- $8000 - $9000: 9 days
- $9000 - $10000: 2 days
- $10000 - $11000: 1 day
- $11000 - $12000: 6 days
- $12000 - $13000: 1 day
- $12000 - $13000: 17 hours
- $13000 - $14000: 4 hours
- $14000 - $15000: 10 hours
- $15000 - $16000: 5 hours
- $16000 - $17000: 2 hours
- $17000 - $18000: 10 minutes
- $18000 - $19000: 3 minutes

For use as a currency *(149)*, this is plainly not viable! *(150)* It's questionable even for serving as a reserve asset. We are not saying that "HODLing" is a hoarding, not that it is bad. (In fact it is good.) *(151)* The problem with a persistently increasing price is preventing the use of bitcoin as a medium of exchange, which was Satoshi's original purpose. *(152)* The nascent crypto-economy needs a medium of exchange in order to grow, and bitcoin is the best known cryptocurrency, hence the most able to fulfill this role. Yet this is what inevitably happens when spiking demand chases finite supply. Will the hard-coded limit of 21 million bitcoins someday be removed *(153)* in order to address this issue? Since we mean to create a next-generation cryptocurrency, these are problems for which we must offer solutions.

The solution to these problems is obvious: *a currency's supply must be managed to align with its demand*. This is what central banks such as the Federal Reserve are theoretically supposed to do given

their mandate to maintain stable prices, both in periods of economic expansion and contraction. In practice of course, they always err on the side of inflation, often explicitly targeting a certain figure such as 2% annually. Why? Because an inflation bias benefits the biggest debtors in the economy, who are almost always governments and politically powerful giant corporations. Interest rates (except for consumer credit of course!) are consistently kept low for the same reason. Savers and those on fixed incomes are harmed by inflationary policies, often forcing the elderly back into the work force. Central banks get away with this behavior largely because of legal tender laws, coupled with a complete lack of accountability. Thus, the ability to manage the money supply is a deadly defect only in the absence of competition.

Obviously the AF cannot deploy legal tender laws to force people to use Lyra in the marketplace. We can only earn the trust of the global market by managing our currency intelligently. As described above, we plan to begin by building both the demand and supply sides simultaneously. By creating DApps such as ABC, Q13, and SportsTrader (with others to follow), we will create practical uses for the coins in circulation. By selling OTO vouchers into existence to interested buyers, we will mint initial supply. We believe in an honest free market capitalist approach. This means that the purpose of offering coins is to generate revenue through presales, while the purpose of trading on the secondary market is to create liquidity for them, and to provide a forum for honest price discovery.

To insure that too many coins are not sold, they are offered in progressively larger blocks at escalating MSRPs. Existing holders always have the ability to step in front of retail sales to sell at a price between the current retail price and the previous one. (Or indeed, at any price.) New retail sales thus occur only when demand at the new price level exceeds available existing supply. As the number of holders grows, they therefore acquire a kind of collective veto against the AF's ability to continue the expansion of the monetary base by means of new sales, should enough existing holders choose to exercise it.

This factor is the reason why cryptocurrencies (including ours) are not “Ponzi schemes,” despite the frequency of this accusation from establishment mouthpieces. Earlier buyers are not being paid by the purchases of later buyers. Instead, later buyers need to pay higher prices to earlier buyers to induce them to part with an appreciated asset. Actually it is fiat monies and government social insurance programs that are the true Ponzis, as discussed here. *(154)*

The flip side of this is that we cannot even estimate the total amount of OTO/Lyra which will ever be issued. To attempt to do so would be to assert knowledge not only of our projected development and other fixed costs (which, naturally, *are* estimable), but also knowledge of the future demand for our DApp services, our future market share of p2p sports betting and other large, complex markets, future demand for use of OTO/Lyra in cross-border transfers, the amount of reserve assets which should be held in order to insure liquidity and implement monetary engineering goals, etc., all necessarily *a priori*. This is simply not possible; and to make the effort would be to commit what Hayek called “the knowledge fallacy” – the presumption that perfect information exists which makes efficient central planning possible. (Satoshi Nakamoto fell into this trap when he decided arbitrarily ahead of time that 21 million bitcoins is the ideal quantity.)

The AF cannot and will not attempt to centrally plan the Lyra-backed economy. What it can do is use the long-term price of Lyra (against a basket of assets) as a feedback signal to indicate when the coin supply should expand or contract. Beyond minting more Lyra to expand supply, excess supply can be addressed either by deploying more use cases for Lyra, through marketing, or by buying it back in the secondary market (as described above in section VII).

In conclusion, we're not merely catering to speculators, or aiming just to line our own pockets. Recall that our mission statement is: "**To promote the growth of robust, borderless, wealth generating, free market ecosystems."** This goal simply cannot be achieved by means of an ICO with a forever-fixed quantity of tokens issued. We are different, because we're thinking much bigger and further ahead. Our vision is for long-term parallel economic development, not merely for short-term development funding and purely speculative gains.

IX. Proposed Ascension Foundation Price List

The following is a provisional list of items which we anticipate will be sold by the AF to interested buyers. This is not necessarily a complete list, and all prices shown are estimated and may be subject to future revision, or negotiation in individual cases. All prices are shown quoted in US dollars; however payment must be tendered in OTO/Lyra. Certain items may not be available until the Ascension blockchain has been launched.

- Permission to operate a DApp in the SilentVault Marketplace (SVM franchise): $50K (plus review of business plan and server-side code written by purchaser). Renewals $10K / year.

- Permission to publish and operate a smart contract on the Ascension blockchain: $10K (plus prior review of smart contract code written by purchaser). [Assumes that we deploy suitable smart contracts in the Ascension blockchain.]

- Permission to operate an additional Openfire Gateway (OFS) within the existing wallet network: $20K. Renewals $2K / year.

- Independent SilentVault Exchange (SVX) franchise: $500K. Renewals $50K / year.

- Permission to operate a voucher Issuer within the existing wallet network: $250K (plus due diligence on operators and regular audits of asset reserves). Renewals $25K / year. (Note this could be used to conduct a pre-blockchain ICO, as we ourselves are using it with OTO.)

- Non-exclusive license for operating an independent Voucher Publisher (VP) network with its own Issuers: $5M (plus due diligence on operators and a contract for software maintenance).

- Annual subscription to a premium multi-hop VPN service which accepts OTO: $300.
- Permission to operate a retail sales portal for OTO and/or Lyra: negotiable.
- Contract custom software development by our engineers: $300 / hour, or negotiated fixed bid.

X. Legal Challenges

The legal status of cryptocurrencies and ICOs around the world is, frankly, an utter and complete mess. Blockchain digital currencies are at once a brand new kind of money, and a new type of asset. Due to the rapid appreciation in their exchange rates versus legacy national fiat currencies, it's also tempting to see them as some new kind of investment vehicle. Bureaucracy being the slowest and stupidest of all human institutions, unsurprisingly this situation has led to responses by authorities that are as all over the map as are the countries themselves.

Some countries have tried to ban Bitcoin, such as Morocco. *(155)* Malaysia is studying *(156)* the matter, with a decision on a ban anticipated by the end of the year. South Korea banned ICOs *(157)*, along with margin trading of cryptocurrencies. China likewise banned ICOs, and then went further by shuttering all of the crypto exchanges *(158)* within China. (South Korea has indicated *(159)* they don't plan to go that far, but has also made some recent threatening noises.) *(235)* The Philippines is mulling new rules *(160)* on both ICOs and exchanges. France is working on a regulatory framework *(227)* for ICOs. Russia appeared to be on track to ban Bitcoin in 2016, then went all in on bitcoin mining. *(161)* This didn't stop them from simultaneously blocking access *(162)* to crypto-to-fiat exchanges. The rationale behind Russia's strategy became clear with the announcement of their own state-run Bitcoin competitor, the CryptoRuble. *(163)* Estonia has pondered the idea of doing a national ICO, and tying it to its e-residency program. *(164)* Catalonia (assuming it separates from Spain) is considering something similar. *(165)* India is said to be planning a crypto rupee. Dubai announced in September its intention to launch a blockchain currency called emCash. The nation of Georgia uses a blockchain for its land title database *(166)*, for which Sweden also has a pilot project. *(226)* Belarus recently made both cryptocurrencies and ICOs explicitly legal. *(233)* Iran is proactively preparing the infrastructure *(167)* for adopting Bitcoin, perhaps because it worked so well for WikiLeaks. *(168)* Due to the growing involvement in the sector by large fintech firms in the USA and Canada, it seems unlikely *(169)* that an outright ban on Bitcoin or other cryptocurrencies will ever take place in those two countries. Nevertheless it would require a degree of naivete not to perceive that establishment concern about cryptocurrencies is growing. *(170)* It is likely that action will be taken by governments, if for no other reason than to protect big banks. *(228)*

In addition to the wide range of reactions by government agencies, there is also considerable confusion and contradiction. Just within the USA, the IRS (tax agency) issued guidance *(171)* in 2014 saying that cryptocurrencies are analogous to commodities, rather than being true currencies, and consequently should be taxed as property. The Commodities Futures Trading Commission (CFTC) appears to agree

-- which implies that cryptocurrencies are outside its purview, since it regulates only derivatives (such as futures and options), and not the trading of the commodities themselves. *(172)* In 2013, the Financial Crimes Enforcement Network (FinCEN) published guidance about how and when the Bank Secrecy Act *(173)* of 1970 should be applied to virtual currencies (blockchain, crypto, or otherwise). A detailed discussion of the implications of this guidance can be found here. *(174)* Meanwhile the Securities Exchange Commission (SEC) has issued guidance *(175)* in 2017, plus more guidance here *(223)*, claiming that cryptocurrency tokens (particularly ICOs) might actually be securities. The result is a looming potential turf war *(176)* between agencies with differing perspectives on the nature of these new beasts, now that bitcoin futures trading has become a reality. *(177)* The US Congress is currently considering an expansion of money laundering definitions *(178)* to include digital currencies explicitly, a change which would primarily impact exchanges.

In Canada, the Ontario Securities Commission (OSC) has likewise provided guidance *(179)* on the subject of ICOs. A discussion of the rationale behind their guidance can be found here. *(180)* Carolyn Wilkins, Senior Deputy Governor of the [central] Bank of Canada, asserts in this interview *(181)* that cryptocurrencies are not money, but "look to me more like a security." Previously, at the Sibos banking and financial conference, Ms. Wilkins had characterized bitcoin more as a commodity than a currency. In Canada's Globe & Mail, she was quoted as saying: "We don't consider them [cryptocurrencies] to be money because they don't meet the fundamental qualities of that." So this one central bank official has said at various times that cryptocurrencies are not money, but may be a commodity, or may be a security. Her comments were made in response to demands by Mr. Jeff Kehoe, the OSC's director of enforcement, that the central bank should provide some guidance as to whether bitcoin is a currency or some other type of entity. The obvious inference is that nobody knows for sure. It's noteworthy that the OSC seems to want cryptocurrency to be money, while the Bank of Canada wants it to be a security. Each institution thus seems to be hoping that the other will have to deal with it. (In Europe, the European Central Bank (ECB) doesn't seem to want the responsibility *(182)* either.) The Bank of Canada nonetheless is studying the idea of issuing its own blockchain currency. *(183)* The US Federal Reserve also has a study project *(184)*, as does the National Bank of Ukraine. *(185)*

For both Canada and the USA, the underlying legal principles for considering an investment a security were established in a US Supreme Court (SCOTUS) case from 1946. *(186)* The eponymous Howey Test *(187)* asserts that an offering is an investment contract (and hence a security) if it involves: (1) an investment of money (2) in a common enterprise (3) with the expectation of profit (4) to come significantly from the efforts of others. This is of course a litmus test, not a bright line classification; the actual facts and circumstances in each particular case must control the determination, not merely the outward form which they may have been given.

This has led to a distinction being drawn between "securities tokens" and "utility tokens," where the former clearly represent equity, debt, or profit entitlement within the common enterprise, while the latter, being analogous to mere "tickets to ride" in a theme park (that may not be built yet), are not automatically deemed to be securities – but *might* be, depending upon the particular circumstances. Even in the absence of any possible certainty, platforms have been introduced which claim (somewhat disingenuously) to have all of this worked out, so that someone doing a token offering can rest easy,

knowing that their legal ducks are all in a row. These include examples such as StartEngine *(188)*, ICOBox *(189)*, Medici's ATS *(190)*, and the Canadian ICO platform TokenFunder *(191)*, which recently won the approval *(192)* of the OSC.

Veteran fintech attorneys have designed something called the Simple Agreement for Future Tokens (SAFT), *(193)* based on the Simple Agreement for Future Equity (SAFE) used with incubator startups. (Note the SEC has been somewhat skeptical *(194)* of SAFEs.) This device is aimed at "removing ICO complexities" by conceding the argument that tokens are investment contracts. But even this strategy has not been met exclusively with plaudits: one law school in New York City actually thinks it increases legal risks *(195)* from token sales, rather than the reverse. Two other attorneys who work in the space believe that any regulation has to be applied only on a case-by-case basis, simply because there is no one-size-fits-all solution *(196)* for dealing with ICOs to begin with.

Stepping back for a moment from all the confusion and conflicting interpretations, the fundamental problem comes into sharp focus: *cryptocurrencies are a new thing*, completely unprecedented in the history of financial technology. Viewed as currencies, they are certainly very peculiar. They are privately issued, supported by no legal tender laws, and unlike barter scrip and earlier so-called community currencies, they are purely digital in nature, generally being backed by nothing tangible, and without a physical cash form. They circulate between wallets, not between accounts like digital fiat monies, and can do so on a person-to-person (p2p) basis without an intermediary. There has never before been a type of money like this!

Viewed as securities, they are also very peculiar. They do not generally represent equity in an enterprise, nor debt, nor a derivative wager placed on the future price of something. They are unregistered (without CUSIP numbers), *(197)* and are digital bearer instruments controlled by means of private encryption keys. (A point noted here *(198)* by investor and PayPal co-founder Peter Thiel.) Although they can be bought and sold, they are not physical commodities like metals or agricultural products. They can be subdivided almost infinitely. Their price is determined by supply and demand *(199)*, but market demand may be due to the burgeoning sector *(200)* as much as to the individual cryptocurrency. Some of their value is clearly speculative *(201)*, while some of it also arises from functional utility as a new type of circulating value. Some portion of the speculative value (often mocked and derided) *(202)* of the overall cryptocurrency market is actually without doubt attributable to hedging against a lack of confidence *(203)* in the broader financial sector. In this sense cryptocurrency resembles precious metals. *(204)*

What then is to be done with this new hybrid animal that's not really a currency, not really a security, not really a commodity, and definitely not a share, bond, futures contract, or option? The answer is obvious: being an entirely new financial creature, a category creator like the platypus *(205)*, entirely new positive law must be enacted by congresses and parliaments, before any kind of legitimate and efficacious regulatory enforcement becomes possible, let alone appropriate. All the legal confusion stems from wild extrapolation of cases from more than half a century ago, straining to apply laws written in the 1930s or 1970s concerning stocks, bonds, pork bellies and bank accounts, to a 21st century set of objects and circumstances that could not possibly have been imagined when those laws

were written or those cases adjudicated. When all becomes extrapolation and arbitrary interpretation based on demonstrably weak analogies, the rule of law may fairly be said to have been extinguished.

In our view, it is not the place of agencies which were set up to regulate matters quite distinct from modern cryptocurrencies, to usurp the place of elected representatives to enact new laws. It appears that some of these agencies may actually agree with this view. This may be why they have issued "guidance" rather than rules, since any rule-making needs to implement specific legislation. To the extent that such guidance actually reflects the ultimate shape of future legislation, it may prove worthwhile. However it appears quite likely, given the conflicting guidance offered by agencies even within the same country, that the cart may be way out in front of the horse here.

In which case, programs dreamed up by lawyers, such as the SAFT, have the cart at least two lengths in front of the horse. The attorneys are offering legal advice based on guidance issued by relevant enforcement agencies, who in turn issued their guidance based on their best speculations about the ultimate shape of some hypothetical future legislation. Given that legislators still haven't figured out how to tax the internet yet (in more than two decades!), that legislation may be a long time coming, and may well take a very different form from what's currently expected. More importantly, cryptocurrencies are global by nature, while law is almost always specific to particular countries. Therefore those countries which enact new laws the quickest may end up hurting themselves profoundly, if those laws are perceived as poorly conceived or needlessly onerous. This factor may lead to long delays in crafting new legislation, as it probably has for laws dealing with taxation of internet sales. *(206)*

It may be objected that enforcement agencies such as the SEC have already begun prosecuting (civilly or criminally) various people and businesses in the cryptocurrency space. This is true; however these cases have involved cryptocurrency only incidentally. For example two ICOs were recently charged *(207)* with fraud in the USA. Last May, the SEC settled a $9M civil case *(208)* against GAW Miners, again for fraud. The SEC has filed a civil lawsuit against the operators of PlexCoin *(209)*, for making a "fraudulent and unregistered offer" to investors – again, due to "materially false and misleading statements," aka fraud. Certain "dark web" marketplaces dealing in prohibited goods have been shut down. *(210)* Various independent bitcoin exchangers have been convicted of selling bitcoins *(211)* to undercover agents for use on such dark markets. The important point to note here is that both constructive fraud and facilitating the sale of prohibited drugs *are already illegal*. These defendants would have been convicted whether they had used cash, bitcoin, money market certificates, or sea shells in the commission of these crimes. The mere use of cryptocurrencies was hardly the basis for the offense. Joining "fraudulent" with "unregistered," as in the PlexCoin case, is lily painting aimed at giving "unregistered" a penumbra of legitimacy on its own. Of course none of this prevents the SEC (or any government agency) from resorting to intimidation and threats *(212)* even where actual legal enforcement action may be impractical.

We believe it would be fairly trivial to demonstrate on the record in court the many differences between cryptocurrencies and other forms of money or securities. For one thing, the list of expert witnesses who could be called upon to support the contention that cryptocurrencies represent a whole new world

is practically endless. (Pretty much everyone who could be deemed to be an expert in the space holds this view.) It follows that the direct application of antique existing laws to activities within this entirely new space is beyond the current legal mandate of the various enforcement agencies. In the USA, acting "under color of law" outside of one's legal authority is actually a criminal offense, under 18 U.S. Code § 242 *(213)*, as is conspiring to do the same. *(214)* Of course the chance of persuading a government to prosecute one of its own agents for exceeding their legal authority is probably remote *(215)*, but the possibility does illustrate a potential reason for the restraint shown by the SEC *et al* in prosecuting cryptocurrency defendants, which thus far has been limited to cases where violations of existing laws on other subjects plainly occurred.

All of this being said, what is the position of the Ascension Foundation regarding the nature of our Lyra coins, the OTO vouchers backed by them, and our responsibility for legal compliance? Our position is that we are simply selling a product, which happens to be a digital coin having particular use cases. The material facts in view are these:

- We sell our Lyra coins, currently represented by OTO vouchers redeemable for Lyra, to meet demand. They are not marketed as an ICO, token generation event (TGE), or crowdfunding investment. No specific return or price appreciation is guaranteed, or even offered.

- While the Ascension blockchain is not yet launched, our voucher network that sits on top of it is fully functional today. Moreover this network is not going away once our blockchain is deployed; rather, it represents an integral part of our market solution for scalability and privacy.

- In addition to selling OTO/Lyra, we are also selling (for Lyra) certain licenses and franchises within our technological ecosystem. (See Section IX above.) Purchasers of many of these items will be able to earn profits directly attributable to their own efforts, and commensurate with their respective success. Purchasers may freely pool their coins to form joint enterprises to acquire and exploit such licenses.

- Certain use cases are/will be provided, some by us and some by others, for OTO/Lyra. These "DApps" require our vouchers or coins for access by users/customers. This provides a non-speculative reason to purchase and hold the coins. Note that at least two such applications will be released almost immediately (see Section XI below), and that OTO vouchers are fully functional today, and indeed have been in limited private circulation since 4Q2016.

- As with many other digital products and services, our digital coins are sold through one or more retail portals, to which the AF provides coins in bulk at wholesale prices. These retailers are free to employ commissioned salespeople, and to design their own unique affiliate sales programs, provided they comply with our MSRP guidelines. (See Section VIII above.)

- The only secondary market for our coins that is currently available is the p2p escrow market provided through the SVX API, where OTO can be swapped for bitcoin, litecoin, and other

assets. The AF does not make a market in the SVX, and any trading it does there (or anywhere) is exclusively for its own account. Prices from trades made therein are kept private between the parties to the trade, and are not automatically published externally.

- Our OTO vouchers are not currently listed on any third-party centralized exchanges, and the AF is not actively seeking such listing. Once Lyra coins are circulating on our blockchain, we cannot of course prevent any third-party exchange from listing them on its platform, using the blockchain reference client supplied by us. (In fact it is possible that this could be done today using our OTO voucher client, but since this would involve a lot of custom development by the exchange, we regard such support as unlikely to occur at this time.) Our ultimate intention is to provide wholly decentralized marketplaces where Lyra, and other assets, can be traded freely.

We believe that these facts argue strongly against *(216)* our coins being construed as a security in most jurisdictions. A widely-used worksheet for determining the applicability of the famous Howey Test is available here. *(217)* Without stipulating that we believe our coins are subject to existing securities or other regulations, we have completed the worksheet in light of the facts stated above, with these results. *(218)*

Having said all this, we do not consider it appropriate to dictate to others concerning the legal risks to which they may be subject. For this reason, we do not for example take a position on whether a particular voucher system Issuer would be considered a virtual currency administrator, or the like, requiring licensing. That would depend upon a number of factors, including the jurisdictions in which that Issuer did business, and the manner in which they handled in and out fiat exchanges (internally or externally). Compliance is thus left as an exercise for the operator of that Issuer. We believe that the compliance obligations of any business component should be dealt with at the level of that component. In this way regulatory risks are “laid off” onto the lowest level where the rubber really meets the road.

XI. Roadmap

As noted above, the Ascension project builds upon work done by Voucher-Safe (2008-2013) and SilentVault (2014-present). Significant milestones beginning within the SilentVault period include:

2Q14: Aleatoric Binary Challenge (ABC) algorithm simulator developed
3Q14: SilentVault reference wallet client released
SilentVault Exchange (SVX) deployed with SBC/SLC/SSV asset types
4Q14: Mac port of reference client
SilentVault Marketplace (SVM) API released
1Q15: ABC development (server and client)
2Q15: First ABC beta test
3Q15: Added RGOLD asset type
Updated reference clients, released separate ABC plugin

[4Q15:Hiatus]
1Q16: Mark II and III ABC algorithm simulators and tests
2Q16: Second round of ABC development (with VFQ integration)
3Q16: Added VFQ (Value Flow Quantification) asset type
4Q16: Second ABC beta test
    Upgraded test network
    Updated reference wallet client plugins
    Added OTO asset type
1Q17: Upgraded reference wallet client releases
    Added SCA (Silent Canadian dollars) and SUS (Silent US dollars) asset types for future use
    Q13 (Quantz) algorithm simulator developed
2Q17: Planning for OTO voucher offering, website design and content drafts
3Q17: Development of Managed Account backend for holders of OTO
4Q17: Ascension white paper produced (this document)
    Deploy Managed Account backend

The following represent future goals with target dates for completion (subject to change):

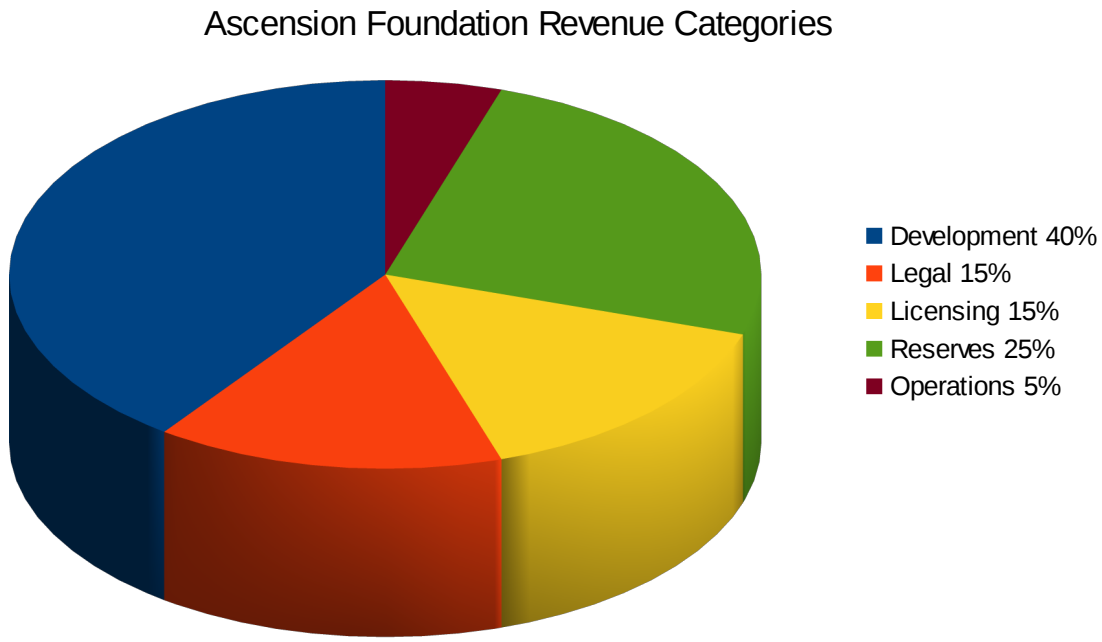
1Q18: Deploy pooled lodgements of OTO into Q13 simulator via Managed Account backend
    Update all reference user wallet clients and deploy initial website content
    Continue Presale phase
    Deploy ABC as live SVM app
    Develop and beta test Q13 SVM app (with InsurBucks integration)
    Launch “Ground Zero” Phase; Round 1 commences immediately upon its completion
2Q18: Native Android wallet client release
    Deploy Q13 SVM app
    Develop and beta test SportsTrader SVM app (with SportsBucks integration)
    Select source base for Ascension blockchain and begin development
3Q18: Web-based wallet client release (also provides iOS thin client)
    Deploy SportsTrader SVM app
    Develop and beta test Binary Options SVM app (with TradeBucks integration)
    Deploy testnet for Ascension blockchain
4Q18: Deploy Binary Options SVM app
    Develop and beta H[0]/T[1] “Hot One” SVM app (with InsurBucks integration)
    Develop and beta CFD (Contract for Difference) SVM app (with TradeBucks integration)
    Ascension blockchain launch (OTO becomes redeemable for Lyra; Lyra can be bought directly)

Further than one year out, we do not consider it wise to project a detailed release schedule, given the especially rapid pace of change in the crypto-economy space.

XII. Use of Funds

As noted above, the Ascension Foundation will be contracting out its coin sales to others: the first identified sales outlet is CryptoWealth.com. It will presell its Lyra coins in bulk at wholesale prices to the OTO voucher Issuer (OTO.Money), which will sell the vouchers representing those coins to the distributor CryptoWealth for the same price per unit. (NB: the OTO.Money issuer earns fees when OTO vouchers are purchased or exchanged in the SVX.) CryptoWealth will apply a retail markup in exchange for performing all sales and marketing functions. Additional competing sales portals may be established in the future.

The AF intends to accept a list of national fiat and crypto currencies for its Lyra coins. These payments may be held in the forms in which they were received, or converted to other forms or used to purchase other assets, depending upon the category to which the funds are allocated. The relevant categories and their respective percentages are as shown in the following chart:



Notes:
Development (40%) refers to funds expended to develop and deploy technology. This would include paid technical staff, contracted mining pools, hardware, equipment, bandwidth and other services.
Legal (15%) relates to funds expended for the creation and maintenance of business entities and accounts, hiring attorneys, accountants, trustees and directors, fees for any required licenses or legal permissions, as well as building a war chest in the event of any future legal attack by state agents.

Licensing (15%) refers to funds paid to acquire the lawful use of technology produced by others. Initially, this will include the phased purchase of an exclusive license of existing Voucher-Safe and SilentVault technology, but may also include any other proprietary tech deemed vital to AF's operations. In respect of V-S and SV tech, this category is subject to a hard cap of US$10 million. Should this milestone be reached, future revenue falling into this category will be allocated to establish a venture capital fund for investing in new technologies in the crypto-economic space generally.
Reserves (25%) are monies set aside for implementing monetary engineering goals. These funds may be highly static, and held mainly in bitcoin or other "hard" cryptocurrency assets.
Operations (5%) expenses are those for day-to-day operations such as office expenses, customer support staff, web design services, insurance, bookkeeping and the like. There is a possible overlap here with the Development and Legal categories.
NB: Sales & Marketing is not shown as a category because those expenses have been out-sourced to retailers.

Disclosures:

All team members and contractors will be paid at appropriate market rates out of the Development, Legal, or Operations budgets above. Any bonus compensation will be paid in the form of OTO/Lyra in bonus incentive pools. The total OTO paid to team members past and present to date is approximately 500,000. A further pool of 3,333,333 Lyra is earmarked for future team bonus compensation, and vests at a price of US$16 (Round 5).

A quantity of OTO has been presold to seed round buyers between 2014 and today. This includes the seed sources for SilentVault. (Yes, we were selling "tokens" way before it was cool to do so.) The total amount of OTO already sold to our various presale buyers is approximately 2.8M. This is vested immediately.

Lastly, we have allocated a founders pool totaling 6,666,667 Lyra. These Lyra cannot be claimed until the price of OTO/Lyra reaches US$32 (Round 6) *and* the Lyra blockchain has been deployed, *or* the end of 2019, whichever comes first.

XIII. About the Authors

Sean Daley, Founder and CEO

Retired criminal defense lawyer, former digital gold trader
Sean has a law background, with deep experience in the cryptocurrency and online sports betting worlds. He practiced for over 20 years as a criminal defense lawyer. Sean was also one of the first

movers in the e-gold space, which ultimately lead him into Bitcoin and the cryptocurrency world. Add in his experience in the sports betting world, and you get Ascension.

Kevin Wilkerson, Founder and CTO

Principal Implementer of the Voucher-Safe technology, Founder of the Digital Cash Alliance

Kevin has been involved with software development for more than 30 years, as a coder, a systems architect, and technical team lead. He has worked in areas as diverse as mechanical CAD/CAM, interactive cable television, e-commerce, and private communications technologies. He was involved in the digital gold industry in the 2000s, the predecessor to today's cryptocurrencies. Kevin is the co-architect and principal implementer of the Voucher-Safe digital cash technology, which allows OTO and other assets to circulate privately off-chain. He is a former freedom movement political activist, science fiction author, and classical musician. Kevin founded the Digital Cash Alliance in 2015, and has been involved in a number of free market business enterprises.

XIV. Conclusion

Thank you for reading through to the end of this paper. Despite the many criticisms we have made herein regarding existing blockchain technologies, such criticism is not the point of this paper. This is not a time for tearing down, but for building up a next generation of crypto-economic tools and businesses. We feel privileged to be able to work and contribute in such a dynamic, disruptive industry which has the potential to transform the world economically. Accordingly, this paper is not merely about what we ourselves can do, or what our own plans are. It's also in no small part about providing an infrastructure in which other entrepreneurs will likewise be able to contribute for our mutual benefit.

We do expect that our own ideas presented here will come in for considerable criticism from the community. In particular, we anticipate that we will be criticized both for utilizing a centralized payment clearing mechanism, and for refusing to specify a hard limit on the ultimate number of Lyra coins to be issued. Our reasons for making these decisions are explained above. Here in closing we'd like to observe that after the long blockchain scaling debate (still ongoing), and the various hard forks, we expect that the criticism about locally centralized clearing will be a lot less loud than it would have been several years ago. In view of the parabolic valuation growth of cryptocurrencies going on at present, especially in bitcoin, we likewise expect that the ability to increase supply as needed, which is

today a radical notion, will gain growing acceptance in the months and years to come. Our proposal is to follow the guidance of the free market, rather than the hubris of designers – not excluding ourselves.

This is a time to get real, to reassess, and to make sober adults-in-the-room plans for how to build on top of the first generation crypto technology to continue to develop the crypto-economy. In this effort it is neither necessary nor desirable to discard everything that is known and done in the legacy, pre-crypto economy. On the contrary, it's about learning what we can from history, and designing solutions to tough problems arising in both the legacy economy and in the new one.

One of the prerequisites for doing this is to recognize the importance of decentralizing the crypto-economic business model, not just certain functions such as mining. This involves asking questions like: where are the profit centers? Who pays for those profits? Who is in competition with whom, and how can competition be harnessed to reward innovation and better service? How can every vital element be made self-supporting? How can those who perhaps are not themselves radical innovators participate through operating crypto-businesses, beyond mere passive investment? How do we create a better, fairer, post-political economic order in the crypto-economy, without repeating the mistakes and pitfalls of the old order? Such considerations on decentralizing the business model by means of competition and profit incentives are seldom talked about when decentralization is discussed, even by the brightest people. Our business model attempts to take all of these kinds of questions into account.

The time has come to focus on the larger perspective of what we are enabling as we build for the future. *(219)* Bitcoin has been called “a hole in a burning building,” and the developing crypto-economy represents an escape hatch *(220)* from the imploding debt-based legacy economy, which continues to disintegrate. A global asset bubble of approximately $250 trillion *(224)* has been inflated by central banks since 2005. When this bubble begins to collapse, an unknown portion of it will flow into the crypto-economy.

We'll leave you with an updated version of a quotation taken from a book by Norm Franz *(221)*:

> *GOLD is the money of kings; SILVER is the money of gentlemen; BARTER is the money of peasants; and DEBT is the money of slaves; but CRYPTO is the money of the free.*

We hope you will join us in building the next phase of the crypto-economy!

XV. Bibliography

(1) - *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto, October 2008, https://bitcoin.org/bitcoin.pdf

(2) - Wikipedia entry: *Satoshi Nakamoto*, https://en.wikipedia.org/wiki/Satoshi_Nakamoto

(3) – CoinMarketCap website, list of all known cryptocurrencies, https://coinmarketcap.com/all/views/all/

(4) – Investopedia entry: S*mart Contracts*, https://www.investopedia.com/terms/s/smart-contracts.asp

(5) – Ethereum Project website, https://ethereum.org/

(6) – RippleNet website, https://ripple.com/

(7) – Chainalysis website, https://www.chainalysis.com/

(8) – *Visualizing the transactions behind the $31m Tether hack*, Elementus.io blog, 22 November 2017, https://elementus.io/blog/tether-hack/

(9) – Bitcoin.org, definition of a "full node," https://bitcoin.org/en/full-node#what-is-a-full-node

(10) - *Who is Moving 750 BTC Worth of Coins on the Bitcoin Network Every 5 Seconds?*, NewsBTC, 10 March 2017, http://www.newsbtc.com/2017/03/10/moving-750-btc-worth-coins-bitcoin-network-every-5-seconds/

(11) - *Empty Block Data by Mining Pool*, BitMEX blog, 17 October 2017, https://blog.bitmex.com/empty-block-data-by-mining-pool/

(12) – Ethereum Classic website, https://ethereumclassic.github.io/

(13) – EOS Dawn 2.0 website, https://eos.io/

(14) – EOS Gold website, https://eosgold.io/

(15) – Wikipedia entry: *Smart Contract*, https://en.wikipedia.org/wiki/Smart_contract

(16) – *What is Turing Completeness?*, wiseGEEK, 13 November 2017, http://www.wisegeek.com/what-is-turing-completeness.htm

(17) - *The Road Ahead for Ethereum: Three Hard Problems*, Muneeb Ali, 17 June 2016, https://medium.com/@muneeb/the-road-ahead-for-ethereum-b5b090bcd1a

(18) – Video presentation at the ETC Hong Kong Summit, Meredith Patterson, 29 November 2017, https://youtu.be/rqqdFufARXA

(19) - *Ethereum ERC20 Tokens Explained*, James Seibel, 21 July 2017, https://medium.com/@james_3093/ethereum-erc20-tokens-explained-9f7f304055df

(20) - *Ethereum's Creator Proves Blockchain Scaling Vision is No Joke*, CoinDesk, 19 September 2016, https://www.coindesk.com/ethereum-creator-vitalik-buterin-scaling-devcon2/

(21) - *What You Need to Know About the Future of Bitcoin Technology*, Subhan Nadeem, 2 December 2017, https://medium.freecodecamp.org/future-of-bitcoin-cc6936ba0b99

(22) – P2P Voucher Payment Project website, https://www.voucher-safe.org

(23) – Bitcoin Wiki entry: *Lightning Network*, https://en.bitcoin.it/wiki/Lightning_Network

(24) - *Rootstock is Fusing Lightning With On-Chain Scaling – On a Sidechain*, CoinDesk, 8 March 2017, https://www.coindesk.com/lumino-bitcoin-lightning-network-scaling-sidechain/

(25) – SilentVault Project website, https://silentvault.com

(26) - *U.S. Entry Into World War I Was a Disaster*, David Stockman, 13 November 2017, https://dailyreckoning.com/u-s-entry-world-war-disaster/

(27) – PayPal website, https://www.paypal.com/

(28) - *How ACH works: A developer perspective*, Gusto Engineering Blog, 23 April 2014, http://engineering.gusto.com/how-ach-works-a-developer-perspective-part-1/

(29) – clearXchange (Zelle) website, https://www.clearxchange.com/

(30) – CHIPS information page, Federal Reserve Bank of New York, https://www.newyorkfed.org/aboutthefed/fedpoint/fed36.html

(31) – SWIFT system website, https://www.swift.com

(32) – Wikipedia entry: *FedWire*, https://en.wikipedia.org/wiki/Fedwire

(33) – Wikipedia entry: *Cheque Clearing*, https://en.wikipedia.org/wiki/Cheque_clearing

(34) - *Taiwan AML reforms & USD/Crypto Drama*, WhaleCalls, 18 April 2017, https://medium.com/@whalecalls/taiwan-aml-reforms-usd-crypto-drama-15417cbcdf7b

(35) – Wikipedia entry: *Double-entry bookkeeping system*, https://en.wikipedia.org/wiki/Double-entry_bookkeeping_system#History

(36) – DASH website, https://www.dash.org/

(37) – PIVX website, https://pivx.org/

(38) – Bitcoin Wiki entry: *CoinJoin*, https://en.bitcoin.it/wiki/CoinJoin

(39) - *Ripple's Distributed Ledger Network Passes 50-Validator Milestone*, CoinDesk, 17 July 2017, https://www.coindesk.com/ripples-distributed-ledger-network-passes-50-validator-milestone/

(40) - *List Of High Profile Cryptocurrency Hacks So Far*, Store of Value blog, 24 August 2017, https://storeofvalue.github.io/posts/cryptocurrency-hacks-so-far-august-24th/

(41) – Visa fact sheet, June 2015, https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf

(42) - *Dear Bitcoin: I'm Sorry, Fees Will Rise*, Rusty Russell, 7 August 2017, https://medium.com/@rusty_lightning/dear-bitcoin-im-sorry-fees-will-rise-b002b1449054

(43) – Tool listing unconfirmed transactions, blockchain.info, https://blockchain.info/unconfirmed-transactions

(44) – Wikepedia entry: *Byzantine fault tolerance*, https://en.wikipedia.org/wiki/Byzantine_fault_tolerance

(45) – *Compact Blocks FAQ*, Bitcoin Core, https://bitcoincore.org/en/2016/06/07/compact-blocks-faq/

(46) – FIBRE website, http://bitcoinfibre.org/

(47) – *Improving Transaction Rate*, Hyperledger Fabric, 11 October 2016, https://lists.hyperledger.org/pipermail/hyperledger-fabric/attachments/20161012/4b7b62f6/attachment-0001.pdf

(48) – *Ethereum Platform Review*, Vitalik Buterin, see page 22 https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57506f387da24ff6bdecb3c1/1464889147417/Ethereum_Paper.pdf

(49) - *Loveable Digital Kittens Are Clogging Ethereum's Blockchain*, CoinDesk, 4 December 2017, https://www.coindesk.com/loveable-digital-kittens-clogging-ethereums-blockchain/

(50) – Apache Kafka project website, https://kafka.apache.org/

(51) – Wikipedia entry: *CAP theorem*, https://en.wikipedia.org/wiki/CAP_theorem

(52) - *'A Modest Proposal': Vitalik Unveils Multi-Year Vision for Ethereum*, CoinDesk, 2 November 2017, https://www.coindesk.com/modest-proposal-vitalik-unveils-multi-year-vision-ethereum/

(53) – *On Stake*, Vitalik Buterin, 5 July 2014, https://blog.ethereum.org/2014/07/05/stake/

(54) - *Segregated Witness: A Fork Too Far*, Jaqen Hash'ghar, 21 December 2016, https://medium.com/the-publius-letters/segregated-witness-a-fork-too-far-87d6e57a4179#.obdmk8ru0

(55) – Ethereum Classic project website, https://ethereumclassic.github.io/

(56) - *The DAO Attacked: Code Issue Leads to $60 Million Ether Theft*, CoinDesk, 17 June 2016, https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/

(57) – Why the Wrong Response to The DAO Attack Could Kill Ethereum, CoinDesk, 20 June 2016, http://www.coindesk.com/ethereum-response-dao-kill/

(58) - *Understanding Bitcoin's Scaling Debate: Politics Comes First*, CoinDesk, 21 July 2017, https://www.coindesk.com/understanding-bitcoins-scaling-debate-politics-comes-first/

(59) – Hyperledger Linux Foundation Project website, https://hyperledger.org/

(60) - *A Case for Permissioned Blockchains*, IBM Developer Works, 29 April 2016, https://www.ibm.com/developerworks/community/blogs/gcuomo/entry/A_Case_for_Permissioned_Blockchains?lang=en

(61) - *Bitcoin versus American Express: a normal person's reaction to $7 transaction fees*, David Gerard, 27 August 2017, https://davidgerard.co.uk/blockchain/2017/08/27/bitcoin-versus-american-express-a-normal-persons-reaction-to-7-transaction-fees/

(62) - *2x or NO2X: Why Some Want to Hard Fork Bitcoin — and Why Others Do Not*, Bitcoin Magazine, 6 October 2017, https://bitcoinmagazine.com/articles/2x-or-no2x-why-some-want-hard-fork-bitcoin-november-and-why-others-dont/

(63) – Bitcoin Capacity increases FAQ, Bitcoin Core, 23 December 2015, https://bitcoincore.org/en/2015/12/23/capacity-increases-faq/

(64) - *Bitcoin Realism or: How I Learned to Stop Worrying and Love 1MB Blocks*, Jimmy Song, 6 March 2017, https://medium.com/@jimmysong/bitcoin-realism-or-how-i-learned-to-stop-worrying-and-love-1mb-blocks-c191c35e74cb

(65) – SegWit Charts tool, http://segwit.party/charts/#

(66) – Wikipedia entry: *Lightning network*, https://en.wikipedia.org/wiki/Lightning_Network

(67) - *Mathematical Proof That the Lightning Network Cannot Be a Decentralized Bitcoin Scaling Solution*, Jonald Fyookball, 26 June 2017, https://medium.com/@jonaldfyookball/mathematical-proof-that-the-lightning-network-cannot-be-a-decentralized-bitcoin-scaling-solution-1b8147650800

(68) - *Continued Discussion on why Lightning Network Cannot Scale*, Jonald Fyookball, 28 June 2017, https://medium.com/@jonaldfyookball/continued-discussion-on-why-lightning-network-cannot-scale-883c17b2ef5b

(69) – Wikipedia entry: *Non-uniform memory access*, https://en.wikipedia.org/wiki/Non-uniform_memory_access

(70) - *Dear Bitcoin, This is How You Can Beat Visa*, James Hudon, 27 August 2017, https://medium.com/@hudon/dear-bitcoin-this-is-how-you-can-beat-visa-b5ee857cf193

(71) – *What is Bitcoin?*, Roger Ver, March 2017, https://www.docdroid.net/NG1sbVq/pantera-march-2017.pdf

(72) - *Economics of Bitcoin as a settlement network*, The Saif House, 19 May 2017, https://thesaifhouse.wordpress.com/2017/05/19/economics-of-bitcoin-as-a-settlement-network/

(73) - *2x Called Off: Bitcoin Hard Fork Suspended for Lack of Consensus*, CoinDesk, 8 November 2017, https://www.coindesk.com/2x-called-off-bitcoin-hard-fork-suspended-lack-consensus/

(74) – Bitcoin Cash project website, https://www.bitcoincash.org/

(75) - *Bitcoin Cash: What You Need to Know*, Jimmy Song, 24 July 2017, https://medium.com/@jimmysong/bitcoin-cash-what-you-need-to-know-c25df28995cf

(76) – Bitcoin Gold project website, https://bitcoingold.org/

(77) - *Bitcoin Gold: What to Know About the Blockchain's Next Split*, CoinDesk, 23 October 2017, https://www.coindesk.com/bitcoin-gold-know-blockchains-next-split/

(78) - *Relief and Disbelief: Bitcoin Reacts to Sudden '2x' Suspension*, CoinDesk, 8 November 2017, https://www.coindesk.com/relief-disbelief-bitcoin-reacts-sudden-2x-suspension/

(79) - *Bitcoin Gold or Comedy Gold? Bitcoin Diamond Launches With 4.2 Bln Coins*, The CoinTelegraph, 24 November 2017, https://cointelegraph.com/news/bitcoin-gold-or-comedy-gold-bitcoin-diamond-launches-with-42-bln-coins

(80) – *Revived Bitcoin Hardfork Bitcoin2x Scheduled For Tomorrow*, Coinivore, 27 December 2017, http://coinivore.com/2017/12/27/revived-bitcoin-hardfork-bitcoin2x-scheduled-tomorrow/

(81) - *There can only ever be 21 million forks of Bitcoin: a survey so far*, David Gerard, 20 November 2017, https://davidgerard.co.uk/blockchain/2017/11/20/there-can-only-ever-be-21-million-forks-of-bitcoin-a-survey-so-far/

(82) - *Why Bcash Mining Shouldn't Affect Bitcoin Much (But Bitcoin Mining Could Ruin Bcash)*, Bitcoin Magazine, 22 August 2017, https://bitcoinmagazine.com/articles/why-bcash-mining-shouldnt-affect-bitcoin-much-bitcoin-mining-could-ruin-bcash/

(83) - *Beware of Bitcoin's possible incompatibility with some major services*, Bitcoin Core alert, 11 October 2017, https://bitcoin.org/en/alert/2017-10-09-segwit2x-safety

(84) - *To B2X or Not to B2X: How Exchanges Will List the SegWit2x Coin*, Bitcoin Magazine, 28 October 2017, https://bitcoinmagazine.com/articles/b2x-or-not-b2x-how-exchanges-will-list-segwit2x-coin/

(85) - *A Bitcoin Beginner's Guide to Surviving the Bgold and SegWit2x Forks*, Bitcoin Magazine, 13 October 2017, https://bitcoinmagazine.com/articles/bitcoin-beginners-guide-surviving-bgold-and-segwit2x-forks/

(86) - *Bitcoin Surges To New Record High $6600 On Futures Hope & Fork Dividends*, Zero Hedge, 1 November 2017, http://www.zerohedge.com/news/2017-11-01/bitcoin-surges-new-record-high-6600-futures-hope-fork-dividends

(87) - *Understanding Segwit2x: Why Bitcoin's Next Fork Might Not Mean Free Money*, CoinDesk, 1 November 2017, https://www.coindesk.com/understanding-segwit2x-bitcoins-next-fork-might-different/

(88) - *Lightning Only? Scaling Bitcoin Might Require A Whole 'Nother Layer*, CoinDesk, 16 November 2017, https://www.coindesk.com/lightning-scaling-bitcoin-might-require-whole-nother-layer/

(89) - *Blockchain's killer app is bitcoin, the rest is mostly 'pure marketing', says MaidSafe's David Irvine*, V3, 25 September 2017, https://www.v3.co.uk/v3-uk/news/3017991/blockchains-killer-app-is-bitcoin-the-rest-is-mostly-pure-marketing-says-maidsafes-david-irvine

(90) - *World's Biggest Tech Giants Could Boost Bitcoin in Regulatory Push*, CoinDesk, 16 May 2017, https://www.coindesk.com/worlds-biggest-tech-giants-boost-bitcoin-regulatory-push/

(91) - *China sets up fintech committee at central bank*, CNBC, 15 May 2017, https://www.cnbc.com/2017/05/15/china-sets-up-fintech-committee-at-central-bank.html

(92) – Blockchain.Info website, https://blockchain.info/

(93) – *Fiddling on the Blockchain While Privacy Burns*, Justin Turrell, 15 February 2014, https://silentvault.com/tiki-read_article.php?articleId=1

(94) – Wikipedia entry: *Friedrich Hayek*, https://en.wikipedia.org/wiki/Friedrich_Hayek

(95) – Wikipedia entry: *The Denationalization of Money*, https://en.wikipedia.org/wiki/The_Denationalization_of_Money

(96) - *Free Market Money: On The Separation of Banking and State*, Richard Ebeling, 21 August 2016, https://www.nassauinstitute.org/article1415/

(97) - **The Creature from Jekyll Island: A Second Look at the Federal Reserve**, G. Edward Griffin, 11 September 2010, https://www.amazon.com/Creature-Jekyll-Island-Federal-Reserve/dp/091298645X

(98) - *Deutsche Asks A Stunning Question: "Is This The Beginning Of The End Of Fiat Money?"*, Zero Hedge, 2 November 2017, http://www.zerohedge.com/news/2017-11-01/deutsche-bank-asks-shocking-question-beginning-end-fiat-money

(99) - *Ripple Pledges to Lock Up $14 Billion in XRP Cryptocurrency*, CoinDesk, 16 May 2017, https://www.coindesk.com/ripple-pledges-lock-14-billion-xrp-cryptocurrency/

(100) - *American Express Opens First Blockchain Corridor With Ripple Tech*, CoinDesk, 16 November 2017, https://www.coindesk.com/american-express-opens-first-blockchain-corridor-ripple-tech/

(101) – *The SilentVault Exchange (SVX)*, SilentVault, https://silentvault.com/tiki-index.php?page=SVExchange

(102) – OnionPay website, http://onionpay.to/

(103) – Wikipedia entry: *ACID*, https://en.wikipedia.org/wiki/ACID

(104) – Wikipedia entry: *Relational database management system*, https://en.wikipedia.org/wiki/Relational_database_management_system

(105) – Tahoe Least Authority File Store project website, https://tahoe-lafs.org/trac/tahoe-lafs

(106) – Symbiont website, https://symbiont.io/

(107) - *Bitcoin: Architectural Problems and Limitations*, Digital Cash Alliance, https://digitalcash.to/bitcoinIssues.html

(108) – Loom project website, https://loom.cc/

(109) – TruLedger project website, http://truledger.com/

(110) - *Mysterious Bitcoin Dip-Buyer Identified*, Zero Hedge, 14 November 2017, http://www.zerohedge.com/news/2017-11-13/mysterious-bitcoin-dip-buyer-identified

(111) - *Massive Hedge Fund CEO "Ready To Add Bitcoin To Investment Universe"*, Zero Hedge, 14 November 2017, http://www.zerohedge.com/news/2017-11-14/massive-hedge-fund-ceo-ready-add-bitcoin-investment-universe

(112) - *Developers Discuss the State of Bitcoin Privacy at Baltic Honeybadger Conference*, CryptoDaily, 29 November 2017, https://cryptodaily.co.uk/2017/11/developers-discuss-state-bitcoin-privacy-baltic-honeybadger-conference/

(113) – Spark IM Client project website, https://igniterealtime.org/projects/spark/index.jsp

(114) - *With deletion of one wallet, $280M in Ethereum wallets gets frozen*, Ars Technica, 7 November 2017, https://arstechnica.com/information-technology/2017/11/with-deletion-of-one-wallet-280-m-in-ethereum-wallets-gets-frozen/

(115) - *Parity Urges 'Rescue' Fork to Reclaim Frozen Millions*, CoinDesk, 11 December 2017, https://www.coindesk.com/parity-proposes-hard-fork-to-reclaim-frozen-160-million/

(116) - *'I Forgot My PIN': An Epic Tale of Losing $30,000 in Bitcoin*, Wired Magazine, 29 October 2017, https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/

(117) – *VS Login Protocol*, Voucher-Safe Project, 27 January 2014, https://www.voucher-safe.org/tiki-index.php?page=VS+Login+Protocol

(118) – Jaxx Cryptocurrency Wallet website, https://jaxx.io/

(119) – Smack project website, https://igniterealtime.org/projects/smack/index.jsp

(120) – ShapeShift Cryptocurrency Exchange website, https://shapeshift.io/

(121) - *Making MAST Meaningful; Bitcoin Atomic Swaps Become Private*, HackerNoon, 3 October 2017, https://hackernoon.com/making-mast-meaningful-bitcoin-atomic-swaps-become-private-ff003f7c2b7a

(122) - *Will Decentralized Exchanges Replace Peer-to-Peer Exchanges Completely?*, The CoinTelegraph, 20 October 2017, https://cointelegraph.com/news/will-decentralized-exchanges-replace-peer-to-peer-exchanges-completely

(123) – Bisq Network website, https://bisq.network/ See also Ox, Kyber, and Oasisdex.

(124) – Wikipedia entry: *Martingale (betting system)*, https://en.wikipedia.org/wiki/Martingale_(betting_system)

(125) – Factom Harmony website, https://www.factom.com/

(126) – RootStock (RSK) project website, https://www.rsk.co/

(127) – Peter Todd on Twitter, 7 December 2017, https://twitter.com/petertoddbtc/status/938868037691822080

(128) - *What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability*, CoinDesk, 12 February 2014, https://www.coindesk.com/bitcoin-bug-guide-transaction-malleability/

(129) – Omni Layer project website, http://www.omnilayer.org/

(130) – Ari Paul on Twitter, 14 November 2017, https://twitter.com/AriDavidPaul/status/930582723193958401

(131) - *Ethereum to ICOs: You're Doing It Wrong*, CoinDesk, 10 November 2017, https://www.coindesk.com/ethereum-icos-youre-wrong/

(132) – OTO.Money (voucher Issuer) website, https://oto.money

(133) – CryptoWealth website, https://cryptowealth.com

(134) - *My Crazy $17,000 Target for Bitcoin Is Looking Less Crazy*, Charles Hugh Smith, 27 November 2017, https://charleshughsmith.blogspot.de/2017/11/my-crazy-17000-target-for-bitcoin-is.html

(135) - *Bitcoin Futures Are a Bet That Digital Money Will Take Over the World*, Bloomberg Technology, 1 December 2017, https://www.bloomberg.com/news/articles/2017-12-01/bitcoin-futures-seen-as-bet-digital-money-will-take-over-world

(136) - *Max Keiser: Banks Will Fail Trying to Compete with Bitcoin*, Binary District, 4 November 2017, https://journal.binarydistrict.com/max-keiser-banks-will-fail-trying-to-compete-with-bitcoin/

(137) - *Stiglitz Says Bitcoin 'Ought to Be Outlawed'*, Bloomberg Technology, 29 November 2017, https://www.bloomberg.com/news/videos/2017-11-29/joseph-stiglitz-bitcoin-ought-to-be-outlawed-video

(138) - *JPMorgan Guilty of Money Laundering, Tried To Hide Swiss Regulator Judgement*, The CoinTelegraph, 17 November 2017, https://cointelegraph.com/news/jpmorgan-guilty-of-money-laundering-tried-to-hide-swiss-regulator-judgement

(139) - *Is it Tuesday? Time for another banking scandal*, Simon Black, 28 November 2017, https://www.sovereignman.com/trends/is-it-tuesday-time-for-another-banking-scandal-22657/

(140) – Wikipedia entry: *Optional stopping theorem*, https://en.wikipedia.org/wiki/Optional_stopping_theorem

(141) – Wikipedia entry: *Martingale (probability theory)*, https://en.wikipedia.org/wiki/Martingale_(probability_theory)

(142) – Wikipedia entry: *Mutualism (economic theory)*, https://en.wikipedia.org/wiki/Mutualism_(economic_theory)#Mutualism_today

(143) - *Census Bureau: 5 Richest Counties Are D.C. Suburbs*, CNS News, 7 December 2017, https://www.cnsnews.com/news/article/terence-p-jeffrey/census-bureau-5-richest-counties-are-dc-suburbs

(144) - *Money does not circulate*, Oleg Andreev, 26 November 2017, https://oleganza.com/all/money-does-not-circulate/

(145) - *Let's boycott uncapped ICOs*, Vasja Veber, 13 July 2017, https://medium.com/viberate-blog/why-we-should-boycott-uncapped-icos-999a5fab7916

(146) - *Credit for Cryptos: Leverage Trading Is Coming to Bitcoin*, CoinDesk, 29 November 2017, https://www.coindesk.com/credit-cryptos-better-worse-leverage-trading-arriving/

(147) – Wikipedia entry: *Inflation*, https://en.wikipedia.org/wiki/Inflation#Positive

(148) – Coinbase exchange website, https://www.coinbase.com/

(149) - *Bitcoin Loses Steam as Steam Loses Bitcoin*, Mises Institute, 8 December 2017, https://mises.org/power-market/bitcoin-loses-steam-steam-loses-bitcoin

(150) - *Made money in bitcoin? Well done. Here's what you must do now*, MoneyWeek, 6 December 2017, https://moneyweek.com/bitcoin-exit-strategy/#.WifA4xrxPGA.twitter

(151) - *In Defense of Bitcoin Hoarding*, Jeffrey A. Tucker, 6 December 2017, https://fee.org/articles/in-defense-of-bitcoin-hoarding

(152) - *Bitcoin's rocketing value is undermining its original purpose*, The Spectator, 8 December 2017, https://blogs.spectator.co.uk/2017/12/bitcoins-rocketing-value-is-undermining-its-original-purpose/

(153) - *The Three Economic Eras of Bitcoin*, Rusty Russell, 30 November 2017, https://medium.com/@rusty_lightning/the-three-economic-eras-of-bitcoin-d43bf0cf058a

(154) - *This Time Is Different Part I: What Bitcoin Isn't*, Mark E. Jeftovic, 30 November 2017, https://medium.com/@markjeftovic/this-time-is-different-part-i-what-bitcoin-isnt-eb9f645239b1

(155) - *Bye-Bye Bitcoin: Morocco Bans Cryptocurrencies*, Morocco World News, 21 November 2017, https://www.moroccoworldnews.com/2017/11/234382/bitcoin-morocco-cryptocurrencies-economy/

(156) - *Malaysia's Central Bank to Decide on Crypto Regulation at Year's End*, Bitcoin News, 8 October 2017, https://news.bitcoin.com/malaysias-central-bank-signals-year-end-bitcoin-ban/

(157) - *Cryptocurrencies Drop as South Korea Bans ICOs, Margin Trading*, Bloomberg Technology, 29 September 2017, https://www.bloomberg.com/news/articles/2017-09-29/cryptocurrencies-drop-as-south-korea-bans-icos-margin-trading

(158) - *Bitcoin Crashes 35% In China: Beijing To Shut All Local Exchanges By End Of September*, Zero Hedge, 14 September 2017, http://www.zerohedge.com/news/2017-09-14/bitcoin-crashes-chinese-trading-second-largest-exchange-halt-all-trading

(159) - *South Korean Finance Watchdog Has 'No Plans' to Regulate Bitcoin Trading*, CoinDesk, 23 November 2017, https://www.coindesk.com/south-korean-finance-watchdog-has-no-plans-to-regulate-bitcoin-trading/

(160) - *Philippine Regulators Eye New Rules for Bitcoin Exchanges and ICOs*, CoinDesk, 22 November 2017, https://www.coindesk.com/philippine-regulators-eye-new-rules-for-bitcoin-exchanges-and-icos/

(161) - *Russia is going all in on bitcoin — and everyone's got a theory*, VICE News, 31 October 2017, https://news.vice.com/story/russia-is-going-all-in-on-bitcoin-and-everyones-got-a-theory

(162) - *Breaking: Russia Rejects Cryptocurrency as Authorities Block Access to Exchanges*, The CoinTelegraph, 10 October 2017, https://cointelegraph.com/news/breaking-russia-rejects-cryptocurrency-as-authorities-block-access-to-exchanges

(163) - *BREAKING: Russia Issuing 'CryptoRuble'*, The CoinTelegraph, 15 October 2017,

https://cointelegraph.com/news/breaking-russia-issuing-cryptoruble

(164) - *We're planning to launch estcoin—and that's only the start*, Kaspar Korjus, Managing Director at e-residency, 18 December 2017, https://medium.com/e-residency-blog/were-planning-to-launch-estcoin-and-that-s-only-the-start-310aba7f3790

(165) - *Bitcoin Just Spiked Back Above $6000 As Catalan Considers Blockchain-Backed e-Residency Program*, Zero Hedge, 29 October 2017, http://www.zerohedge.com/news/2017-10-29/bitcoin-just-spiked-back-above-6000

(166) - *The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project*, Forbes, 7 February 2017, https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#2deed9df4dcd

(167) - *Iran Is Preparing Infrastructure For Bitcoin Adoption*, Zero Hedge, 1 November 2017, http://www.zerohedge.com/news/2017-11-01/iran-preparing-infrastructure-bitcoin-adoption

(168) - *Julian Assange Thanks US Government, Senators, For Forced Bitcoin Investment*, The CoinTelegraph, 15 October 2017, https://cointelegraph.com/news/julian-assange-thanks-us-government-senators-for-forced-bitcoin-investment

(169) - *Why Governments Will Not Ban Bitcoin*, Charles Hugh Smith, 22 October 2017, https://charleshughsmith.blogspot.de/2017/10/why-governments-will-not-ban-bitcoin.html

(170) - *Crypto Surge Sparks Establishment Panic: Bans, Crackdowns, & Fatwas As Bitcoin "Undermines Governments, Destabilizes Economies"*, Zero Hedge, 4 December 2017, http://www.zerohedge.com/news/2017-12-03/crypto-surge-sparks-establishment-panic-bans-crackdowns-fatwas-bitcoin-undermines-go

(171) - *The IRS Just Made A Crucial Ruling About Bitcoin*, Business Insider, 25 March 2014, http://www.businessinsider.com/irs-bitcoin-is-property-not-currency-full-release-2014-3?IR=T

(172) - *CFTC Chairman: Cryptocurrencies Are 'Unlike Any Commodity' We've Seen*, The CoinTelegraph, 13 December 2017, https://cointelegraph.com/news/cftc-chairman-cryptocurrencies-are-unlike-any-commodity-weve-seen

(173) – Wikipedia entry: *Bank Secrecy Act*, https://en.wikipedia.org/wiki/Bank_Secrecy_Act

(174) - *The Bank Secrecy Act, Cryptocurrencies, and New Tokens: What is Known and What Remains Ambiguous*, Coin Center, 20 May 2017, https://coincenter.org/entry/aml-kyc-tokens

(175) - *Investor Bulletin: Initial Coin Offerings*, U.S. Securities Exchange Commission, 25 July 2017, https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings

(176) - *LedgerX and CBOE: The CFTC's Trojan Horse in an SEC Turf War*, CoinDesk, 13 August 2017, https://www.coindesk.com/ledgerx-cboe-cftcs-trojan-horse-sec-turf-war/

(177) - *Bitcoin Soars After CFTC Approves Futures Trading: First Trade To Take Place Dec.18*, Zero Hedge, 1 December 2017, http://www.zerohedge.com/news/2017-12-01/bitcoin-jumps-above-10k-after-cftc-approves-futures-trading-first-trade-take-place-d

(178) - *Congress and the Fed Take Aim at Bitcoin*, Mises Institute, 29 November 2017, https://mises.org/power-market/congress-and-fed-take-aim-bitcoin

(179) - *CSA Staff Notice 46-307: Cryptocurrency Offerings*, Ontario Securities Commission, 24 August 2017, http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm

(180) - *Decoding when Canadian securities law applies to cryptocurrencies*, Financial Post, 12 September 2017, http://business.financialpost.com/legal-post/decoding-when-canadian-securities-law-applies-to-cryptocurrencies

(181) - *Carolyn Wilkins: Bitcoins are securities not money!*, Kamal Glover YouTube channel, 20 November 2017, https://youtu.be/KrdetxUHyc0

(182) - *Investors Taking a Risk Buying Bitcoin, Says ECB Vice President*, CoinDesk, 30 November 2017, https://www.coindesk.com/investors-taking-a-risk-buying-bitcoin-says-ecb-vice-president/

(183) - *Central Bank Digital Currency: Motivations and Implications*, Bank of Canada, November 2017, https://www.bankofcanada.ca/wp-content/uploads/2017/11/sdp2017-16.pdf

(184) - *Federal Reserve starting to think about its own digital currency, Dudley says*, CNBC, 29 November 2017, https://www.cnbc.com/2017/11/29/federal-reserve-starting-to-think-about-its-own-digital-currency-dudley-says.html

(185) - *The Ukrainian Central Bank Is Expanding Its Blockchain Team*, CoinDesk, 4 December 2017, https://www.coindesk.com/ukrainian-central-bank-expanding-blockchain-team/

(186) - *How A 1920s Florida Citrus Land Baron Created The Acid Test For Crypto Tokens*, Forbes, 14 November 2017, https://www.forbes.com/sites/chitraragavan/2017/11/14/how-a-1920s-florida-citrus-land-baron-created-the-acid-test-for-crypto-tokens/#4bb5f1e74a3c

(187) - *What Is the Howey Test?*, FindLaw, http://consumer.findlaw.com/securities-law/what-is-the-howey-test.html

(188) - *StartEngine Rolls Out Regulated Initial Coin Offerings*, Early Investing, 13 October 2017, https://earlyinvesting.com/startengine-to-offer-legal-and-regulated-icos/

(189) – ICO Box website, https://icobox.io/

(190) - *Regulated ICOs Arrive: Overstock to Open Exchange for Legal Token Trading*, CoinDesk, 27 September 2017, https://www.coindesk.com/regulated-icos-arrive-overstock-open-exchange-legal-token-trading/

(191) – TokenFunder website, https://www.tokenfunder.com/

(192) - *TokenFunder Wins Approval to First OSC Regulated ICO Launch*, Bitcoin Magazine, 25 October 2017, https://bitcoinmagazine.com/articles/tokenfunder-wins-approval-first-osc-regulated-ico-launch/

(193) - *SAFT Arrives: 'Simple' Investor Agreement Aims to Remove ICO Complexities*, CoinDesk, 2 October 2017, https://www.coindesk.com/saft-arrives-simple-investor-agreement-aims-remove-ico-complexities/

(194) - *Investor Bulletin: Be Cautious of SAFEs in Crowdfunding*, U.S. Securities Exchange Commission, 9 May 2017, https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_safes

(195) - *Report Warns SAFT May Increase Legal Risk of Token Sales*, CoinDesk, 21 November 2017, https://www.coindesk.com/report-warns-saft-may-increase-legal-risk-token-sales/

(196) - *Why there is no "one-size-fits-all" regulation for ICOs*, BetaKit, 3 October 2017, https://betakit.com/why-there-is-no-one-size-fits-all-regulation-for-icos/

(197) – *Fast Answers: CUSIP Number*, U.S. Securities Exchange Commission, https://www.sec.gov/answers/cusip.htm

(198) - *Peter Theil "People are under estimating Bitcoin"*, Kamal Glover YouTube channel, 27 October 2017, https://youtu.be/0yHhwhvoB0w

(199) - *What Gives Cryptocurrencies Their Value*, Mises Institute, 1 December 2017, https://mises.org/wire/what-gives-cryptocurrencies-their-value

(200) - *Ethereum Surges To New Record Highs - Bigger Than Capital One, ICE, & eBay*, Zero Hedge, 24 November 2017, http://www.zerohedge.com/news/2017-11-24/ethereum-surges-new-record-highs-bigger-capital-one-ice-ebay

(201) - *Riding The Blockchain Train: These Companies Changed Their Name, And Their Stock Price Soared*, Zero Hedge, 24 December 2017, http://www.zerohedge.com/news/2017-12-24/riding-blockchain-train-these-companies-changed-their-name-and-their-stock-price-soa

(202) - *Bitcoin Tumbles After Jamie Dimon Calls It A Fraud: "Would Fire Anyone Trading It"*, Zero Hedge, 12 September 2017, http://www.zerohedge.com/news/2017-09-12/bitcoin-tumbles-after-jamie-dimon-calls-it-fraud-would-fire-anyone-trading-it

(203) - *Macquarie Lashes Out At Dimon: "Modern Finance", Not Bitcoin, Is The Real Fraud*, Zero Hedge, 28 September 2017, http://www.zerohedge.com/news/2017-09-28/macquarie-lashes-out-jamie-dimon-modern-finance-not-bitcoin-real-fraud

(204) - *With Bitcoin's Adolescence Comes Real Competition*, Tom Luongo, 11 November 2017, https://tomluongo.me/2017/11/11/with-bitcoins-adolescence-comes-real-competition/

(205) - *Bitcoin Is A Platypus: The Story Of Category Creators*, Forbes, 3 December 2017, https://www.forbes.com/sites/spencerbogart/2017/12/03/bitcoin-is-a-platypus-the-story-of-category-creators/2/#33364bd9625e

(206) - *Just in Time for the Holidays, Reckless States Are Coming for Your Online Purchases*, Mises Institute, 24 November 2017, https://mises.org/wire/just-time-holidays-reckless-states-are-coming-your-online-purchases

(207) - *ICOs and a soon-arriving flood of SEC enforcement investigations*, Bankless Times, 14 October 2017, https://www.banklesstimes.com/2017/10/14/icos-and-a-soon-arriving-flood-of-sec-enforcement-investigations/

(208) - *SEC Obtains Final Judgment Against GAW Miners CEO Josh Garza for $9 Million Fraud*, Cryptocoins News, 10 May 2017, https://www.cryptocoinsnews.com/sec-obtains-final-judgment-against-gaw-miners-ceo-and-admitted-fraudster-josh-garza/

(209) - *SEC takes PlexCoin scammers to court over securities laws violations*, Finance Feeds, 2 December 2017, https://financefeeds.com/sec-takes-plexcoin-scammers-court-securities-laws-violations/

(210) - *Dark web's largest illegal marketplace, founded by Canadian, shut down by U.S.*, CBC, 20 July 2017, http://www.cbc.ca/beta/news/technology/alpha-bay-doj-us-illegal-online-marketplace-dark-web-1.4213901

(211) - *Bitcoin's 'First Felon' Charlie Shrem Begins 2-Year Sentence*, CoinDesk, 30 March 2015, https://www.coindesk.com/bitcoins-first-felon-charlie-shrem-begins-2-year-sentence/

(212) – *SEC blocks restaurant app's 'initial coin offering'*, New York Post, 11 December 2017, https://nypost.com/2017/12/11/sec-blocks-restaurant-apps-initial-coin-offering/

(213) - *Deprivation Of Rights Under Color Of Law*, U.S. Department of Justice, https://www.justice.gov/crt/deprivation-rights-under-color-law

(214) - *18 U.S. Code § 241 - Conspiracy against rights*, Cornell Law School, https://www.law.cornell.edu/uscode/text/18/241

(215) – *Under color of law*, TRAC, Syracuse University, http://trac.syr.edu/tracreports/civright/107/

(216) - *Investment Tokens vs. Product-Use Tokens in ICOs*, Blockmason, 17 August 2017, https://medium.com/@BlockMason/three-weeks-ago-the-ethereum-community-was-rocked-by-an-unexpected-report-the-sec-had-finally-90814e8ca4d

(217) – *A Securities Law Framework for Blockchain Tokens*, Debevoise & Plimpton, 5 December 2016, https://www.coinbase.com/legal/securities-law-framework.pdf

(218) – Completed Howey Test worksheet, The Ascension Foundation, 24 November 2017, https://oto.money/docs/ascension-howey.html

(219) - *Think people got rich from Bitcoin? We haven't seen anything yet.*, Simon Black, 12 December 2017, https://www.sovereignman.com/investing/think-people-got-rich-from-bitcoin-we-havent-seen-anything-yet-22758/

(220) - *This Time is Different Part 2: What Bitcoin Really Is.*, Mark E. Jeftovic, 12 December 2017, https://guerrilla-capitalism.com/articles/this-time-is-different-part-2-what-bitcoin-really-is/

(221) - *Money & Wealth in the New Millennium Quotes*, GoodReads, https://www.goodreads.com/work/quotes/496004-money-and-wealth-in-the-new-millennium

(222) - *Where Have All the Private Blockchains Gone?*, CoinDesk, 18 December 2017, https://www.coindesk.com/private-blockchains-gone/

(223) - *Statement on Cryptocurrencies and Initial Coin Offerings*, U.S. Securities Exchange Commision, 11 December 2017, https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11

(224) - Regulating Cryptocurrencies--and Why It Matters, Charles Hugh Smith, 18 December 2017, https://charleshughsmith.blogspot.de/2017/12/regulating-cryptocurrencies-and-why-it.html

(225) - *Ivy for Bitcoin: a smart contract language that compiles to Bitcoin Script*, Chain, 18 December 2017, https://blog.chain.com/ivy-for-bitcoin-a-smart-contract-language-that-compiles-to-bitcoin-script-bec06377141a

(226) - *Sweden is trialling a blockchain-powered land registry – which could save taxpayers $100 million*, Business Insider Nordic, 4 April 2017, http://nordic.businessinsider.com/sweden-is-pioneering-a-blockchain-run-land-registry---which-could-save-taxpayers-$100-million-2017-4/

(227) - *French Regulator Launches 'UNICORN' ICO Support Project*, CoinDesk, 26 October 2017, https://www.coindesk.com/french-regulator-launches-unicorn-ico-support-project/

(228) - *'EU crackdown on bitcoin is attempt to protect banks'*, RT, 18 December 2017, https://www.rt.com/news/413517-bitcoin-cryptocurrency-eu-crackdown/

(229) - *A Deeper Dive Into Dash and Its Explosive Year*, CryptoSlate, 20 December 2017, https://cryptoslate.com/deeper-dive-dash-dynamite-year

(230) – Investopedia entry: *Net settlement*, https://www.investopedia.com/terms/n/net-settlement.asp

(231) – *Cryptos Fear Credit*, Perry G. Mehrling, 29 September 2017, http://www.perrymehrling.com/2017/09/cryptos-fear-credit/

(232) - *Does Freedom Require Radical Transparency or Radical Privacy?*, EOS blog, 16 December 2017, https://steemit.com/eos/@dan/does-freedom-require-radical-transparency-or-radical-privacy

(233) - *Belarus Legalizes Cryptocurrencies and ICOs – Tax-Free for Five Years*, Bitcoin.XYZ, 23 December 2017, http://bitcoin.xyz/belarus-legalizes-cryptocurrencies-icos-tax-free-five-years/

(234) - Why Lightning and Raiden Networks Will Not Work, Egor Homakov, 16 December 2017, https://medium.com/@homakov/why-lightning-and-raiden-networks-will-not-work-d1880e4bc294

(235) - *South Korea "Shutdown" Threat Sparks Crypto Carnage 2.0*, Zero Hedge, 28 December 2017, https://www.zerohedge.com/news/2017-12-27/south-korea-shutdown-threats-sparks-crypto-carnage-20

(236) - *Fundamental challenges with public blockchains*, Preethi Kasireddy, 10 December 2017, https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428