MYBIT

A Decentralized Asset Management Platform

Version 0.7

Authors: Ian Worrall
January 2017

Abstract

In an interconnected, open digital world it does not make sense that ownership is still fragmented in outdated, closed systems. The reason ownership management has not progressed is that it cannot be securely stored in a centralized system. It must be decentralized. In the past few years, technological advancements have made decentralization possible utilizing various Blockchain technologies.

This paper describes our implementation to securely create a digital footprint of product registration (to rightful owners), authenticate high-valued merchandise, and transfer ownership (Bills of Sale) in an immutable, transparent, cryptographically secured, and highly auditable Blockchain Ledger application.

The approach has four core components: 1) The ability for users to register and transfer ownership of their assets on the Blockchain with no technical knowledge, 2) the ability to secure these assets in a Smart contract powered Trust, 3) the ability for high-end product manufacturers to authenticate their merchandise in a golden source ledger, and 4) the ability to vastly reduce the complexity and cost to query ownership rights and authenticity for buyers of these products.

The Blockchain is used to securely record ownership transactions that are impossible to later repudiate or manipulate. Later in this paper we will discuss the various Blockchain protocols chosen for the initial MyBit application.

Table of Contents

1. Centralized vs Decentralized 5
   1.1. Centralized model 5
   1.2. Decentralized model 6
   1.3. Centralized vs Decentralized Comparison 7
   1.4. When does Decentralization make sense? 8
   1.5. Why is our platform better suited for a Decentralized model? 9
2. Intro to Blockchain 10
   2.1. Bitcoin 11
   2.2. Bitcoin 2.0: Blockchain application Layer 11
   2.3. Decentralized Applications (DApps) 12
   2.4. Decentralized Consensus 13
3. Ethereum 14
   3.1. What is Ethereum 14
   3.2. Functionality 14
   3.3. Resource Efficiency 15
   3.4. Security 18
4. Internet of Value 18
5. The Problem 20
   5.1. Fragmentation and Opaqueness in asset ownership. 20
   5.2. Reliance on Third Parties 20
   5.3. Not a secure way to manage records 21
   5.4. Lack of transparency creates auditing and compliance issues 22
6. The Solution 23
   6.1. Application Overview 23
   6.2. Technical flow of Asset life cycle 25
   6.3. Process Example 26
   6.4. Architectural Flow 28
   6.5. Scope of Improvements 29
   6.6. Tech Stack 29
   6.7. Transactional Security 30
   6.8. Compliance 31
   6.9. IP Protection 32
   6.10. Integration Examples 32

6.10.1. Smart Trusts 32
6.10.2. Rating System 33
6.10.3. Insurance Claims 33

7. The Market 34
7.1. Securing Commerce 34
7.2. Value Lost through Fraud 34
7.2.1. Counterfeit 35
7.2.2. Supply Chain 35
7.2.3. Healthcare 36
7.2.4. Insurance 36

8. Monetization 37
8.1. Profit Sharing 37
8.1.1. Active Profit Sharing 38
8.1.2. Passive Profit Sharing 38
8.2. Token Pricing Model 38

9. Team 39

10. Milestones Timeline 41

11. Community Driven Development 41

12. Conclusion 42

13. References 43

1. Centralized vs Decentralized

1.1. Centralized model

Centralized models rely heavily on one party (company, individual, server, etc.) to manage and make core decisions.

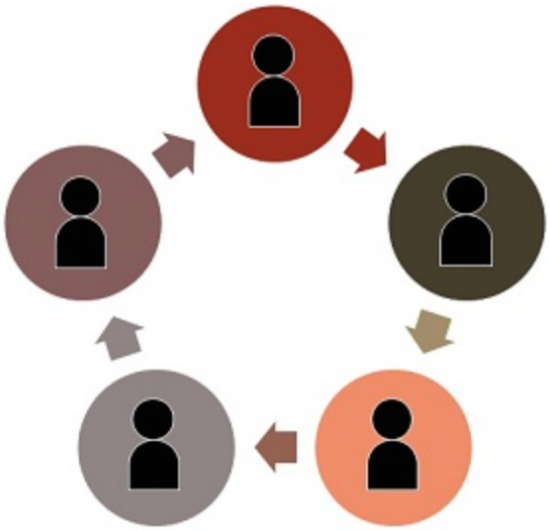
A large majority of models today are centralized (some may include decentralized components but as a whole do not fit the criteria of a truly decentralized model). **Examples of centralized models** include businesses where the owners (or managers) make the core decisions, government organizations, and IT systems that hold all user information and company data. Even peer to peer companies such as Uber and AirBnB do not fit under the decentralized classification because all users are routed through the service provider for all activity.

The largest **advantage of the centralized model** is the ability for highly efficient decision making. This is due to owners typically deciding the vision, operations, and all other aspects of business while employees follow these objectives. If a mission critical issue arises, core decision makers can meet, discuss, and implement a resolution strategy rather quickly and efficiently.

Flaws of the centralized model include a) bureaucracy in decision-making which slows down innovation. If a majority of the employees or customers want to see a change, it is ultimately up to the owners (or managers) to make the final decision. b) single point of failure risk. If something happens to the service provider it affects employees, customers, and other affiliated parties which creates unnecessary risk for participants. c) the model is not designed for innovation. Due to the bureaucratic structure where employees lack the ability to partake in the decision making process it creates obstacles for implementing innovative updates.

1.2. Decentralized model

Truly decentralized models rely on the entire network of participants to make decisions and run the business.



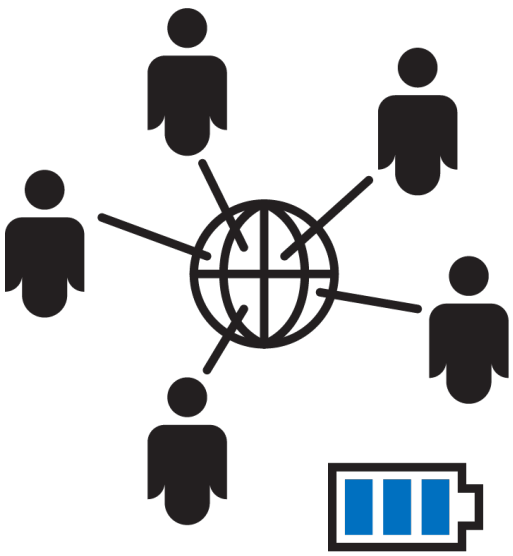
Very few organizations follow truly decentralized models to date. Prior to the recent emergence of Smart Blockchain Technology decentralization was not feasible. Over the upcoming years you will most likely see a massive shift into decentralized models. According to Johnston's Law, "Everything that can be decentralized, will be decentralized." Current **examples of decentralized models** include Bitcoin, Ethereum, Augur, Steem, Iconomi, and Waves. The foundational structure of these will be explained in the Blockchain 2.0 and decentralized application sections further in this paper.

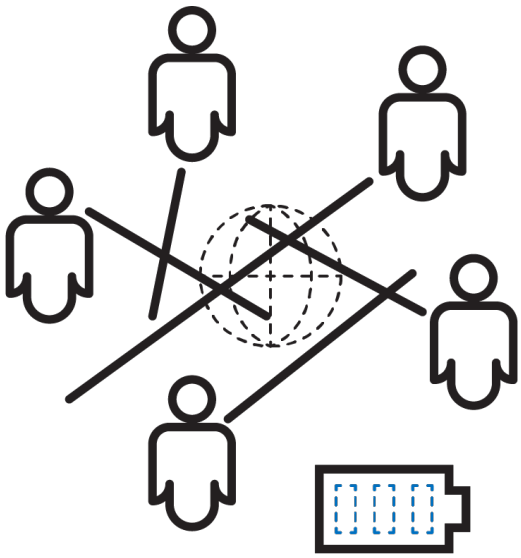
The biggest **advantages of the decentralized business model** are a) no single point of failure risk. Since there is no service provider (or centralized party) which the network relies on to function properly, if one (or several) network participants are corrupted or leave the network it will not affect functionality nor the other participants. b) incorporates truly democratic principles by providing every participant an equal say in the vision, development, and objective of the organization. c) fuels innovation via the enablement of experts from a variety of verticals to equally participate in operations and suggest changes.

A **disadvantage of the decentralized model** is that organizational issues have the potential to arise during the decision-making process if there is a lack of agreement among members. This issue is addressed and made much more manageable with **Blockchain Consensus Technology**.

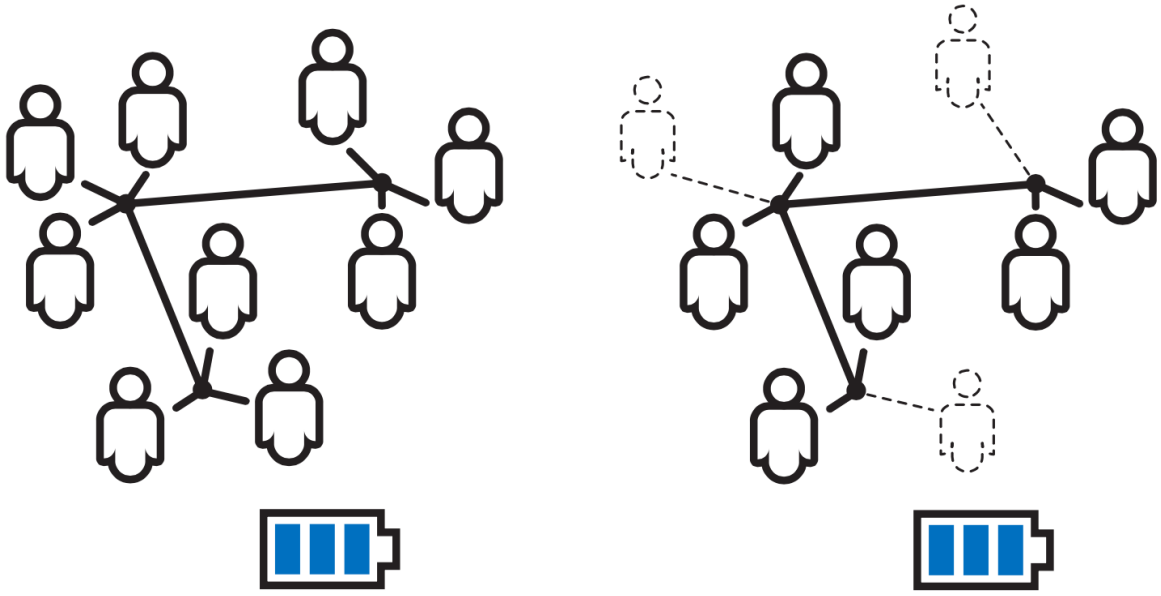
1.3. Centralized vs Decentralized Comparison

If the service provider (AirBnB platform for example) is removed, all of the users are affected and unable to continue utilizing the service. This creates a single point of failure risk.





In the decentralized model there is not a reliance on a single service provider in which all users must be routed through for the system to function thus eliminating a single point of failure risk. The actions, roles, and responsibilities of the service provider are written in computer code therefore ensuring execution according to community dictated decisions (commonly referred to as Consensus).



Consensus is a vital characteristic of decentralized application architecture which requires that a majority of users must agree on any core change to the business model before it can be implemented. Whereas, in a centralized model, if a company decided to update an aspect of their business operations such as raising fees, changing terms and conditions, or altering their model in any way, it could be completed without the approval of users.

1.4. When does Decentralization make sense?

Not all models would benefit from a fully decentralized structure. It may not be optimal for a large multi-national corporation that has investment holdings, manages supply chains for computer component distribution, provides consulting services, and has thousands of businesses relying on their services. If something were to go wrong, it is critical that the MNC is able to react as quickly and efficiently as possible. This requires a core (centralized) group to handle these

important decisions. While this approach is usually more viable, it still has the single point of failure risk if decision makers do not act in the best interest of the company or "go rogue."

While organizing the multi-national corporation itself with a decentralized model does not usually make sense, it may streamline operations to implement a decentralized model to some lines of business within the MNC. The MNC could decentralize their investment technology and protocols to increase transparency, streamline processes such as dividends and other disbursements, and eliminate a single point of failure risk such as an upset employee intentionally making adverse investment decisions to damage the company. Supply chains and inventory management could also be decentralized to cut costs and open the doors to innovation. The people who usually are most knowledgeable about specific problems and inefficiencies are not typically the business owners and decision makers, but rather the employee(s) who work directly in the respective sector. This creates a conundrum where the decision makers often are not fully aware nor experienced in the field, yet the employees who have experience usually do not have a voice in the outcome. Decentralized models work to bridge this gap via streamlined communication and consensus protocols.

In the majority of circumstances, it would be in the best interest of an organization with multiple lines of business to take a centralized model approach. Decentralized models are most viable for specific applications and departments where achieving objectives is more reliant on transparency, innovation, and risk-aversion, and not as reliant on fast decision making.

1.5. Why is our platform better suited for a Decentralized model?

Centralization creates a single-point of failure risk. When you are dealing with potentially billions, if not trillions, of asset and ownership records, the data becomes vulnerable to fraud and mismanagement if one entity controls it all. It also creates security flaws that can (and statistically will) be exploited.

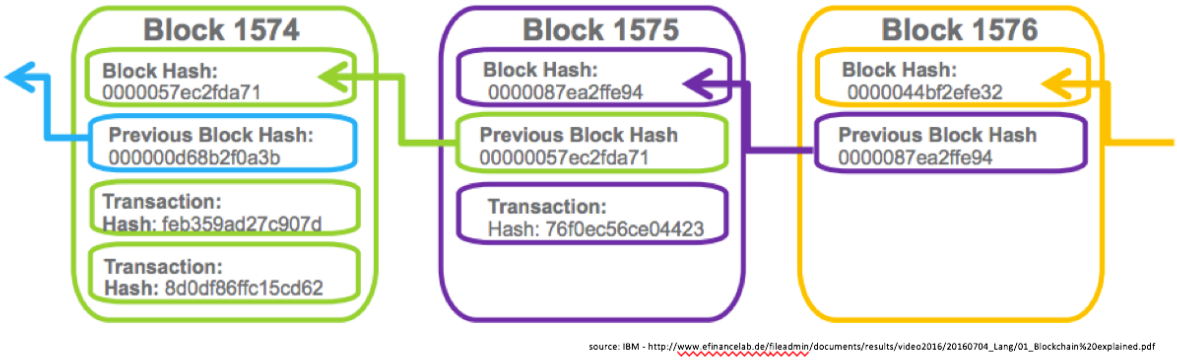
By utilizing a decentralized model, a single point of failure risk is removed. Data is governed and maintained by network participants (nodes) and all data is fully replicated across all network peers. Also, Democratic principles are ingrained in the core (code) of the platform providing all participants with a voice regarding

the future of the application. This results in innovation at the foundational level. This creates a unique opportunity for managing assets and ownership that is more secure, efficient, and reliable than any other solution for digitalizing assets and ownership.

2. Intro to Blockchain

A Blockchain is a data structure that makes it possible to create a tamper-proof digital ledger of assets and transactions which are shared among a distributed network of users. Blockchains utilize advanced cryptography to allow each participant on the network to interact with the ledger in a secure way without the need for a central authority.

Once a block of data is recorded on the Blockchain ledger it is often referred to as immutable in that it is extremely difficult to change or remove due to the fact that all past transactions are continuously revalidated before an addition can be added. When a user wants to add to a Blockchain, participants in the network (all of which have copies of the current Blockchain) run algorithms to evaluate and verify the proposed transaction (all of this happens in the background in a matter of seconds). If a majority of nodes agree that the transaction looks valid, (identified information matches the Blockchain's history) then the new transaction is approved and written to the Blockchain.



source: IBM - http://www.efinancelab.de/fileadmin/documents/results/video2016/20160704_Lang/01_Blockchain%20explained.pdf

Transactions are grouped into 'blocks', then stored forever in a 'chain' by linking each new block chronologically with the hash of the preceding block

2.1. Bitcoin

Bitcoin is often referred to as the first "killer" decentralized (Blockchain) application. Since it was launched in 2009, it has had 100% uptime with zero network breaches which is remarkable. A common misconception regarding major Bitcoin hacks is the Bitcoin network itself that was exploited; that was not the case. The hacks that have gained much attention were Bitcoin exchanges starting with Mt. Gox and including Bitstamp, Bitfinex, as well as other small platforms. These hacks, which lead to millions of dollars worth of Bitcoin being stolen, had nothing to do with the security of the Bitcoin network, but rather how the exchanges managed user account access and private keys.

2.2. Bitcoin 2.0: Blockchain application Layer

Commonly referred to as Bitcoin 2.0 technology, the Blockchain application layer is a set of bitcoin-derived technologies designed to further the functionality, scalability, and performance of the Bitcoin Blockchain.

With Blockchain application layer technology, we have seen the emergence of smart contracts. **Smart contracts** are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary. Smart contracts usually have a user interface and often emulate the logic of contractual clauses which can be partially or fully self-executing, self-enforcing, or both. Smart contracts aim to provide security superior to traditional contract law and to reduce other transaction costs associated with contracting.

Other innovations that have accompanied Blockchain application layer technology are increased performance such as faster block processing times, ability to process more transactions in a single block (blocksize), and more efficient algorithms to secure the network that are not as resource heavy as Bitcoin's proof of work algorithm. Other application layer technologies facilitate interacting with the Blockchain such as easily deploying on various environments, SDKs to interact with common application programming languages, and advanced consensus technologies to manage organization of network participants. New applications are constantly emerging that cater to a specific need or area.

2.3. Decentralized Applications (DApps)

DApps are decentralized ledgers that enable efficient value transfers and trustworthy storage because they are secure even in the face of actively malicious attackers. These systems are distributed, massively redundant, fault-tolerant databases.

Below is a diagram of a generalized **Decentralized Application Stack**. Our stack slightly differs for reasons of stability and performance which we outline in detail in the "Tech Stack" section further in this paper.

For an application to be considered a DApp it must meet the following criteria:

1) The application must be completely open-source, it must operate autonomously, and with no entity controlling the majority of its tokens. The application may adapt its protocol in response to proposed improvements and market feedback but all changes must be decided by consensus of its users.
2) The application's data and records of operation must be cryptographically stored in a public, decentralized blockchain in order to avoid any central points of failure.

3) The application must use a cryptographic token (bitcoin or a token native to its system) which is necessary for access to the application and any contribution of value from miners should be rewarded in the application's tokens. The application must generate tokens according to a standard cryptographic algorithm acting as a proof of the value nodes are contributing to the application (Bitcoin uses the Proof of Work Algorithm).

2.4. Decentralized Consensus

Decentralized consensus breaks the old paradigm of centralized consensus when one central database rules transaction validity. A decentralized scheme, on which the bitcoin protocol is based, transfers authority and trust to a decentralized virtual network and enables its nodes to continuously and sequentially record transactions on a public "block," creating a unique "chain": the Blockchain. Each successive block contains a "hash" (a unique fingerprint) of the previous code; therefore, cryptography (via hash codes) is used to secure the authentication of the transaction source and removes the need for a central intermediary. The combination of cryptography and Blockchain technology together ensures there is never a duplicate recording of the same transaction.

There are two common **mechanisms by which DApps can establish consensus**: the **proof of work**, PoW, mechanism and the **proof of stake**, PoS, mechanism.

With the proof of work mechanism, decisions about changes in a DApp are made based on the amount of work that each stakeholder contributes to the operation of the DApp. Bitcoin uses this approach for its daily operations. The mechanism for establishing consensus through PoW is commonly referred to as mining.

With the proof of stake mechanism, decisions about changes in the DApp are made based on the percent ownership that various stakeholders have over the application. For instance, the vote of a stakeholder who controls 10% of the tokens issued by a DApp carries a 10% weight.

These two mechanisms can be used in parallel. Such a combination allows a DApp to operate with less energy consumption than proof of work alone and allows it to be more resistant to 51% attacks.

DApps have the potential to become self-sustaining because they empower their stakeholders to invest in the development of the DApp. Because of this, it is conceivable that DApps for payments, data storage, bandwidth, and cloud computing may one day surpass the valuation of multinational corporations like Visa, Dropbox, Comcast, and Amazon that are are currently active in the space.

3. Ethereum

3.1. What is Ethereum

Ethereum is an open source public blockchain-based distributed computing platform, featuring smart contract functionality. It provides a decentralized virtual machine, the **Ethereum** Virtual Machine (EVM), that can execute peer-to-peer contracts using a token called ether.

Smart contracts are applications that run exactly as programmed without any possibility of downtime, censorship, fraud, or third party interference.
These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions and many other things that have not yet been invented, all without a middle man or counterparty risk.

Effectively, Ethereum aims to take the promise of decentralization, openness, and security that is at the core of blockchain technology and integrate with nearly everything that can be computed.

3.2. Functionality

Ethereum enables developers to build unstoppable applications with smart money and smart execution of tasks. On traditional server architectures, every application has to set up its own servers that run their own code in isolated silos, making sharing of data difficult. If a single app is compromised or goes offline, many users and other apps are affected. On a Blockchain, anyone can set up a node that replicates the necessary data for all nodes to reach an agreement and

be compensated by users and app developers. This allows user data to remain private and apps to be decentralized which is how the Internet was supposed to be designed.

3.3. Resource Efficiency

Ethereum has plans to migrate the network from proof of work to proof of stake in the near future. Proof of stake provides a large resource efficiency over proof of work since it does not rely on specialized supercomputers (ASIC Miners) to secure the network and validate transactions.

Proof of work is extremely inefficient in terms of energy which makes it very expensive. This incentivizes miners to centralize the hashing power in what is referred to as mining pools. This is clearly not desirable for a network whose goal is to minimize the need to trust third parties and centralized powers.

Proof of stake is not reliant on mining; its focus is validation.
In PoS, each validator owns a stake in the network (ether in the case of Ethereum) that they bond. Bonding stake means you deposit money into the network, which is used as a form of collateral to vouch for a block. In PoW a chain is valid because of workloads behind it, while in PoS you trust the chain with the highest collateral.

Consider Bitcoin as an example of a Blockchain secured with **a proof of work algorithm**. Each block in Bitcoin consists of two parts:

• block header of key parameters, including block creation time, reference to the previous block and the Merkle tree root [4] of the block of transactions
• block list of transactions.

To reference a specific block, its header is hashed twice with the SHA-256 function [5]; the resulting integer value belongs to the interval [0, 2^256 − 1]. To account for different possible implementations, we will use a generic hashing function hash(·) with a variable number of arguments and range [0, M]. For example, arguments of the function can be treated as binary strings and merged together to form a single argument that can be passed to the SHA-256 hashing

function. The block reference is used in the proof of work protocol; in order for a block to be considered valid, its reference must not exceed a certain threshold:

$$\text{hash}(B) \leqslant M/D,$$

where $D \in [1, M]$ is the target difficulty. There is no known way to find B satisfying (1) other than iterating through all possible variables in the block header repeatedly. The higher the value of D, the more iterations are needed to find a valid block; the expected number of operations is exactly D.
The time period T (r) for a miner with hardware capable of performing r operations per second to find a valid block is distributed exponentially with the rate r/D (see Appendix A):

$$P\{T(r) \leqslant t\} = 1 - \exp(-rt/D).$$

Consider n Bitcoin miners with hash rates r1, r2, ..., rn. The period of time to find a block T is equal to the minimum value of random variables T (ri) assuming that the miner publishes a found block and it reaches other miners immediately2. According to the properties of the exponential distribution, T is also distributed exponentially:

$$P\{T \stackrel{\text{def}}{=} \min(T_1, \ldots, T_n) \leqslant t\} = 1 - \exp\Big(-\frac{t}{D}\sum_{i=1}^{n} r_i\Big);$$

$$P\{T = T_i\} = \frac{r_i}{\sum_{j=1}^{n} r_j}.$$

The last equation shows that the mining is fair: a miner with a share of mining power p has the same probability p to solve a block before other miners.
In proof of stake algorithms, inequality (1) is modified to depend on the user's ownership of the particular PoS protocol cryptocurrency and not on block properties. Consider a user with address A and balance bal(A). A commonly used proof of stake algorithm uses a condition as

$$\text{hash}(\text{hash}(B_{\text{prev}}), A, t) \leqslant \text{bal}(A)M/D,$$

where
• Bprev denotes the block the user is building on,
• t is the current UTC timestamp.

For various reasons, some cryptocurrencies use modified versions of (2) which we discuss in the corresponding sections. Unlike (1), the only variable that the user can change is the timestamp t in the left part of equation (2). The address balance is locked by the protocol; e.g., the protocol may calculate the balance based on funds that did not move for a day. Alternatively, a **PoS** cryptocurrency may use unspent transaction outputs as Bitcoin does; in this case, the balance is naturally locked. A proof of stake protocol puts restrictions on possible values of t. For example, if t must not differ from the UTC time on network nodes by more than an hour, then a user can attempt no more than 7200 values of t. Thus, there are no expensive computations involved in proof of stake.

Together with an address A and a timestamp t satisfying (2), a user must provide a proof of ownership of the address. To achieve this, the user can sign the newly minted block with his signature; in order to produce a valid signature, one must have a private key corresponding to the address A.
The time to find a block for address A is exponentially distributed with rate bal(A)/D. Consequently, the (2) implementation of proof of stake is fair: the probability to generate a valid block is equal to the ratio of user's balance of funds to the total amount of currency in circulation. The time to find a block for the entire network is distributed exponentially with rate Σ bal(a)/D.

Thus, if the monetary supply of the currency Σ bal(a) is fixed or grows at a predictable rate, the a difficulty D should be known in advance:

$$D = \frac{1}{T_{ex}} \sum_{a} \mathbf{bal}(a),$$

with Tex denoting the expected time between blocks. In practice, D needs to be adjusted based on recent blocks because not all currency owners participate in block minting.

3.4. Security

In the event of a major hack, Ethereum has proved to be successful at mitigating risk to network participants. Ethereum itself has never been hacked, only services built on it have, very similar to the misconception of the Bitcoin network being hacked (discussed previously in this paper) when in fact, it was security issues with exchanges that held Bitcoin and the private keys of users.

4. Internet of Value

Similar to how the internet streamlined and secured the transfer of information (communication technologies), Blockchain enables for asset ownership (and transfer) & core business functions. The Blockchain is often heralded as the world's first internet-scale open platform for value-exchange.

"Blockchain can bring the experience of a continuously connected, seamless, multi-device computing layer, with an overlay for payments —not just basic payments, but micropayments, decentralized exchange, token earning, digital asset invocation and transfer, and smart contract issuance and execution — as the economic layer that the Web never had."
- Melanie Swan 1

Transferring money was solved by Bitcoin and surrounding technologies; however, Blockchain can open up doors for ownership and asset management. Bitcoin was an audacious idea. Until cryptocurrencies came along, no one had the ability to transmit value at a distance without the permission and support of a third party. This revolutionary idea of instant value transfer is the core of what blockchain technology makes possible. The blockchain is being heralded as the fifth disruptive computing paradigm, which would bring with it an ubiquitous experience of value exchange on the web.

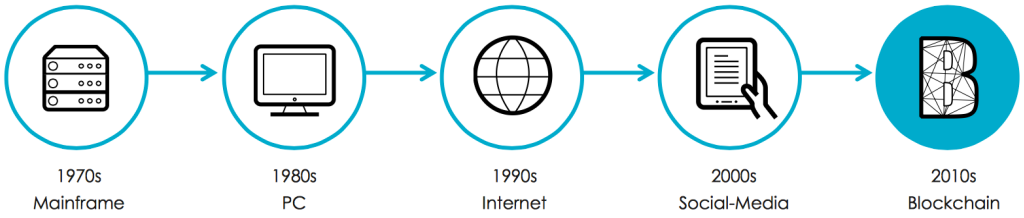


Figure 1: A new paradigm for computing

In an increasingly digital age it is imperative that money and assets can flow freely and securely on a global scale transcending borders. This streamlines business functions creating unparalleled efficiencies. Think about how communication was first revolutionized through the transition from physical mail services to electronic communication with email and instant messaging & collaboration platforms such as Slack. These innovations enabled individuals and companies to securely communicate and transact on a global scale in a fraction of the time. Electronic trading and transfers were other examples of large accomplishments that increased the speed and accessibility of financial services. As Bitcoin (or other Blockchain-derived means of monetary exchange) begins to play a bigger role in the world economy, it further increases ones' ability to securely transact quickly and affordably. The next piece of the puzzle is enabling the same for the transfer of assets. With the combination of communication, money, and assets flowing freely on a global scale it unlocks further potential of the internet and fundamentally changes economics as we know it.

Figure (Left): A trusted third-party actually controls the ownership rights of your asset and you must go through them to do anything with it (typically with a fee involved). If you want to transfer money, stock, or a commodity, a fee is involved for having the "manager" of the asset complete the transaction as instructed.

Figure (Right): The owner has full control of the asset and can do with it as he/she pleases without going through a third-party. The computer code executes the desired transaction instantly for free (or an extremely minimal platform fee compared to traditional transfer methods) without the need for paying someone to complete it.

5. The Problem

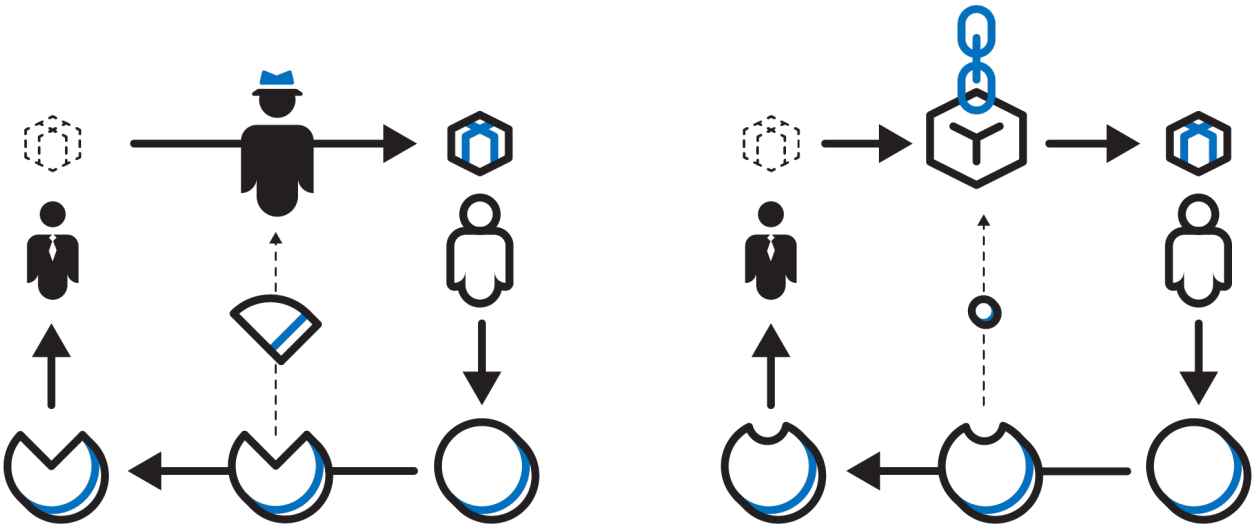
5.1. Fragmentation and Opaqueness in asset ownership.

The absence of efficient technology solutions surrounding Asset Management hinder the ecosystem. The current systems do not adequately facilitate asset management making the process unnecessarily time consuming and expensive for all parties involved. Lack of transparency and counterparty risk adversely affect secondary market transactions, securing assets (in Trusts or Wills), and insurance claims procedures. Nearly all facets of business are moving to a digital environment to provide an easier and cost-effective solution for both individuals and companies alike, yet the Asset Management industry is finding it difficult to keep pace with the transformation.

Communication transcends borders, mobile money and electronic banking enable the instant transfer of funds, FMCGs and services can be easily purchased online, yet the process of managing (transact, protect, etc.) high-valued assets remains expensive and cumbersome.

5.2. Reliance on Third Parties

Trusted third-parties have existed for decades to facilitate and secure transactions while keeping a piece of it for themselves. With Ethereum smart contract technology a majority of these roles can be replaced with computer code that is guaranteed to be executed as written, without error. It is important to understand that Blockchain does not completely eliminate the need for oversight or a third-party in every situation; however, it changes how a lot of business models in the future will need to function to remain relevant and profitable. Models that include brokers, escrow agents, or other third-parties that currently profit from facilitating a transaction will have to transition into providing an actual service of value rather than being able to “skim” percentages of each transaction. This is due to Blockchain technology providing a faster, cheaper, and more secure method of transfer.



As you can see above in the above figure, increased automation in a particular transactional process (the fewer human hands it needs to touch to be completed) results in more money being retained by buyers and sellers.

5.3. Not a secure way to manage records

Records are held by trusted-third parties and are not continuously audited or checked for validity. This creates an unsecure method of managing these ownership rights as well as an inefficient way to retrieve the data for verification and/or transfer purposes. A common "hack" in today's society is data manipulation, the altering of records (data) to produce a different outcome. For example, if a financial analytics firm had even a small fraction of their data altered it could completely change the output of their algorithms. Another example is where record ownerships are altered enabling an individual or group to fraudulently sell the asset. These cyber attacks go largely unnoticed because there are not many cost-effective nor efficient solutions for countering them.

With Blockchain technology you have a preventative measure against these data manipulation attacks built directly into the functionality in that each transaction is revalidated before the next one can be written to the chain. This is a core reason why we believe Blockchain technology to be the optimal solution for implementing a digital asset (and ownership) platform.

5.4. Lack of transparency creates auditing and compliance issues

Since data is often kept in closed-systems unavailable to the public, people must rely on third-parties to correctly (and regularly) conduct audits. Unfortunately, if it is not mandated from a regulatory body, audits are very rarely conducted because they do not provide tangible economic value. It would be too time consuming (with no clear cash value) for auditors to analyze records of entities that were not mandated to do so.

If the records were easily available to the public, it would resolve much of this issue. There is also potential for problems to arise from lack of transparency and accessibility of data for governing bodies. For this reason (and lack of adequate reporting tools), peer to peer commerce is one of the leading issues to regulators. If a transparent and auditable Blockchain ledger solution was implemented and became the standard in transactional reporting, it would increase both the accuracy and efficiency of the entire process while not requiring additional reporting work to be completed by the users of peer to peer services.

6. The Solution

Our Vision is a secured global system of ownership governed by the people for the benefit of the people. The MyBit platform is striving to bridge the gap between real-world (physical) assets and Blockchain technology by becoming the world's first Decentralized Asset Management initiative to run on both web (MIST) and mobile (Status.im).

6.1. Application Overview

This application is designed to demonstrate how assets can be modeled on the Blockchain using the scenario of Asset Management. Various scenarios can be incorporated such as physical products (Rolex watch, designer apparel, etc.), automobiles, hardware, edible items, FMCG, etc.

Let's assume in our scenario Assets are modeled using Blockchain technology with the following attributes:

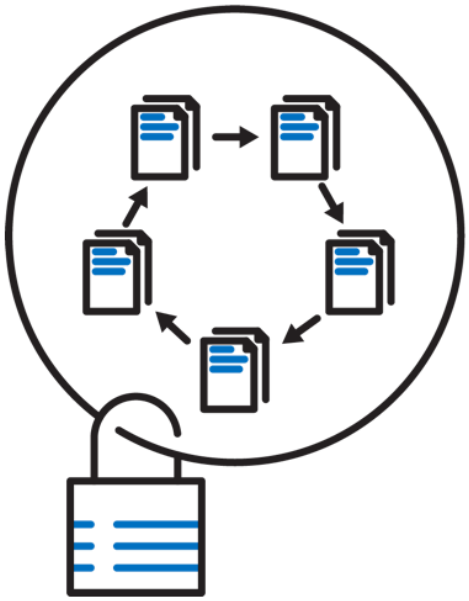
Type	**Attribute**
Alphanumeric	AID (Asset ID)
Unsigned int	AIN(Asset Identification Number)
Name of the asset	Asset
String	Description
String	Date of Registration
Identity of genesis owner	Registered by
Identity of current owner	Current Owner
Identity of beneficiary	Beneficiary (if any)
Cryptographic hash of the supporting document	Identification Document (optional*)

The application is designed to allow participants to interact with the Assets by creating, updating, storing, querying, and transferring them as their permissions allow.

Technical Execution	Contracts needed	Permissions	Participants
Refer to Section 6.2	TrustManager*	Read, trigger events	Insurance Regulator
Refer to Section 6.2	AssetManager	Trigger events	Validating Authority*
Refer to Section 6.2	AssetManager, IdentityManager	Create	Initiator
Refer to Section 6.2	AssetManager, IdentityManager	Read(Verify ownership), Update, Transfer	Seller
Refer to Section 6.2	AssetManager, IdentityManager	Read(Verify ownership)	Buyer
Refer to Section 6.2		Transfer, Decommission	Current Owner
Refer to Section 6.2	AssetManager, IdentityManager	Read(Own Assets)	nth Buyer (Next Buyer)
Refer to Section 6.2	AssetManager, IdentityManager	Read, Update, Transfer	Beneficiary

The concept taken here (as an example of asset management) allows a view of the ledger that stores all the interactions/transactions of which the above participants have completed in relation to their assets. The ledger view shows specific details of every transaction including parties involved, time, assets involved, terms, and cryptographic signatures.

While this is all happening, every action is logged in a tamper-proof global database and replicated across all nodes on the network to ensure data integrity.



Asset lineage is another vital component which enables users to trace the history of assets (they own, have sold, or are enquiring about in relation to a potential purchase). This creates a transparent view of asset ownership by increasing the accessibility of both pre-purchase and post-purchase data.

6.2. Technical flow of Asset life cycle

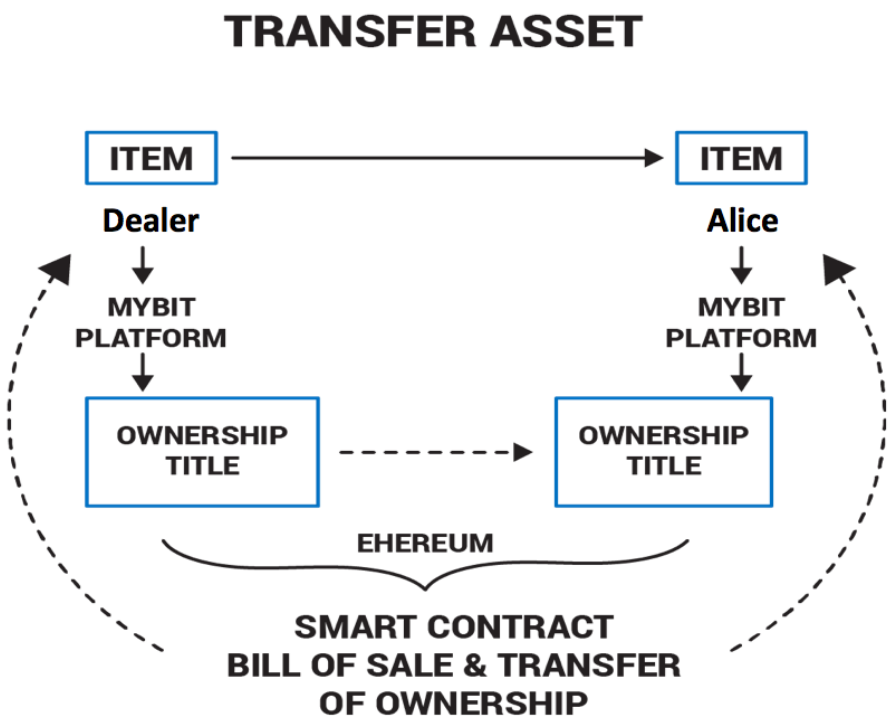
1. Asset is created by the Initiator using the Asset Management contract. Details of the Initiator are recorded on the Blockchain using our Unique Blockchain Identifier (UBI) contract. These contracts develop two sandboxed containers (like a table) on the Blockchain which are linked by public address (hash) of Initiator account. In this step the Initiator can also elect to register his/her beneficiary with our Trust Manager contract.
2. In case of an error in asset creation, the Initiator will be able to update the asset, but a trail of updates will still be recorded on the ledger.
3. Details of the Asset should contain a unique identifier that can distinguish the asset. Supporting documents can also be uploaded.

4. Initiator (as a seller now) can decide to transfer the asset to a buyer.
5. Buyer has the capability to verify the ownership of the asset and identity of the owner from the Blockchain using our contract logic.
6. Assuming each buyer will check with the system to verify asset ownership, fraud will be easily detected.
7. Trail of ownership will be updated on the Blockchain with each transfer transaction. Current owner and beneficiary information will also be updated.
8. Validated Authority may or may not be implemented for each transaction as it depends on the level of control required for Business logic.
9. With each completed transaction a Bill of Sale will be generated by Backend Server. Required data will be pulled directly from the ledger.
10. In case of untimely death, on submission of required documents with regulator, it can trigger an event on the ledger which would execute the Trust smart contract and transfer the ownership seamlessly to the beneficiary.
11. If an asset's life is expended, the current owner can also decommission the asset on the ledger.

6.3. Process Example

Alice is buying a Rolex watch from a Dealer and then reselling it to Bob in the secondary market.

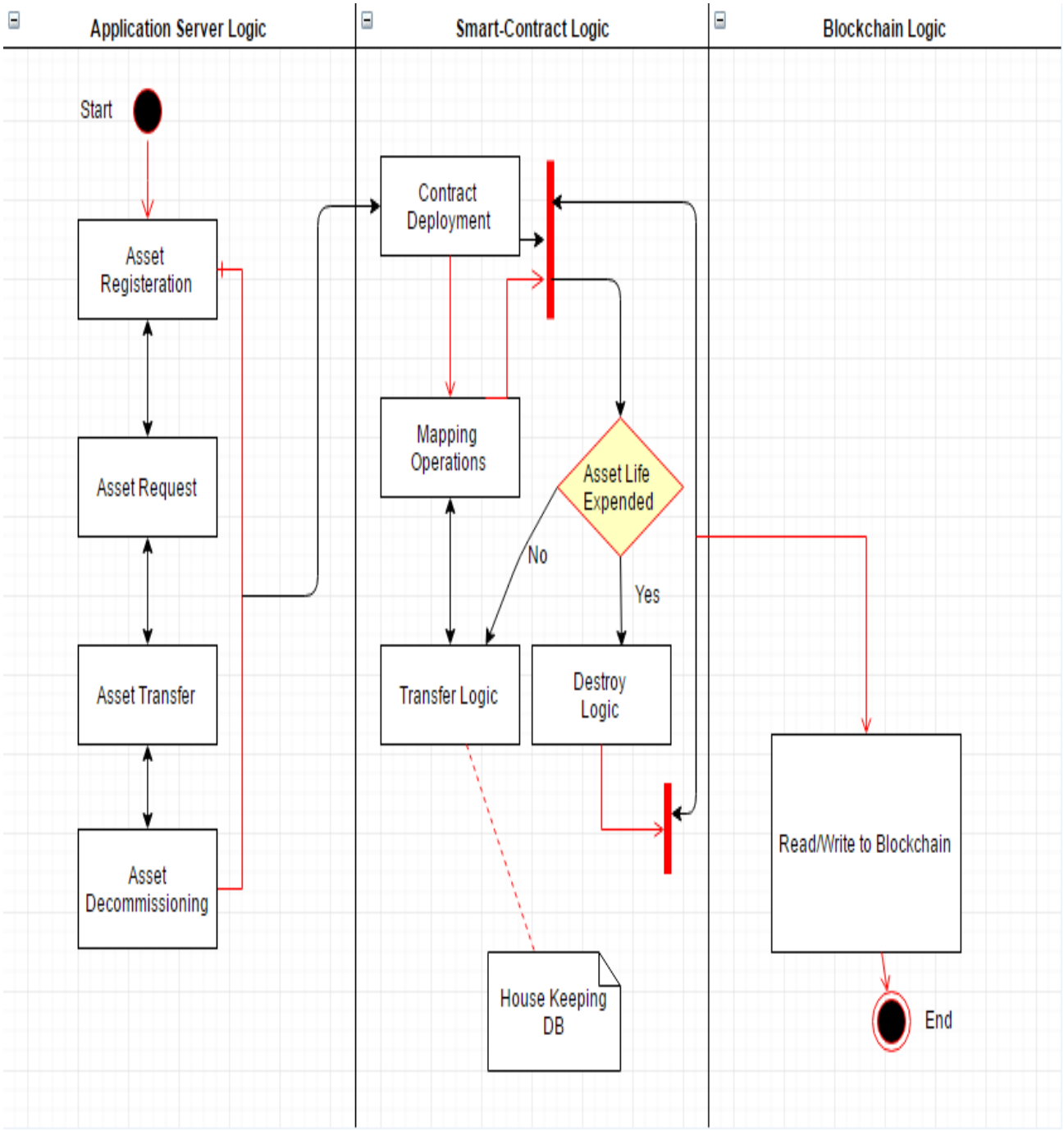
1. Upon receipt of payment (Alice to Dealer), physical asset is received by Alice, and asset ID (AID) is transferred from UBI of Dealer to UBI of Alice.



2. A Record is registered and stored in the database of the backend server and hash of the transaction will be stored in the Ethereum Blockchain which can be used to trace asset lineage.
3. Now Alice sells the Rolex watch to Bob (in person) in exchange for cash and transfers the ownership title to Bob. Bob has the ability to pull information about the watch from the Blockchain to verify that Alice is the (current) rightful owner as well as any past ownership history. This feature can be used to trace assets back to the point of production (assuming the manufacturer is utilizing the platform) to verify authenticity. Following completion of the interaction the hash of the transaction is recorded on the Blockchain.
4. Bob has decided to keep the watch and protect his asset by placing it in his Will (utilizing the Trust contract) with his father registered as the beneficiary of the Rolex. If the Will remains unchanged until the time of his death, the ownership of the Rolex will be transferred to Bob's father

6.4. Architectural Flow

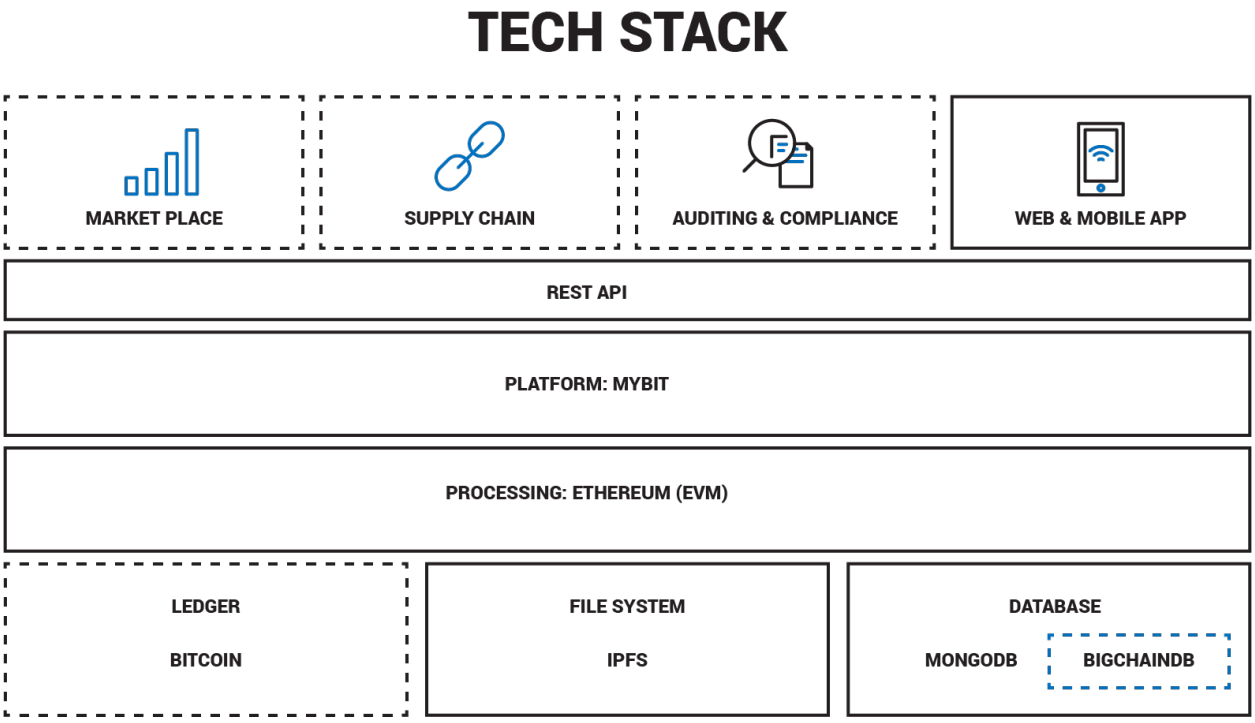
All Application interactions occur over REST protocol. The application interacts with smart contracts over RPC using an HTTP endpoint.



6.5. Scope of Improvements

- Multi-party asset ownership
- Scale application to include other phases of asset life cycle
- Trigger death problem in a more decentralized manner.
- Analytics dashboards to be placed on top for monitoring Blockchain performance.

6.6. Tech Stack



At the **Database** level of our technology stack our end goal is to integrate BigchainDB, an enterprise grade decentralized Blockchain Database. However, we must wait for a stable release so we are planning to use MongoDB as a housekeeping database until Bigchain is production ready. We chose MongoDB since they are a top-tier and highly reliant distributed database (the next best thing to decentralized) and Bigchain is developing their solution in cooperation with MongoDB so the transition from MongoDB into BigchainDB will be much easier than if we chose another database solution from the start. For BigchainDB to be decentralized, nodes must be maintained by various sources so we will be

highly selective on the Blockchain foundations we choose as candidates, with final approval deriving from MyBit network consensus of all our participants.

For our **file system** we have chosen the inter-planetary file system (IPFS) as it is the most notable decentralized file storage initiative with founders visions' that align much with those of our team.

We may elect to use the Bitcoin Blockchain as a **ledger** where transactional data is hashed and stored since it is the oldest, most secure, and trusted Blockchain to date. Limitations may arise due to Bitcoin's throughput capacity and high latency, which is the reason we are not planning to include in our MVP release, but may choose to incorporate as its technology advances to manage scale.

For **processing** we are using Ethereum as our platform's engine to enable rich and highly functional smart contract logic which is a backbone of our platform. We are keeping in mind that Ethereum has plans in the near future to migrate to proof of stake (from proof of work) with their Casper release and are developing our solution to easily adapt to that transformation.

The MyBit **platform** will expose a rich **Rest API** to enable the development of **services** utilizing MyBit's functionality. The Web and Mobile interfaces we are developing will rely on this API as well as provide the community options to develop solutions such as advanced analytics, market places, supply chain applications, and much more. We will utilize the Mist Browser for the MyBit web application and status.im OS for mobile to enhance user experience and accessibility.

6.7. Transactional Security

A safeguard is created in the world of commerce as two forms of verification are easily accessible. 1) Does the person physically have possession of the item and 2) Does the person have control of the private key for the item? With basic commerce transactions this is relatively easy to enforce. If the seller does not have both 1 and 2 then there is an increased chance the seller is not the rightful owner and the transaction needs to be further evaluated prior to completing.

If a situation arises where ownership rights for a specific asset are disputed, our platform has a built in mechanism (consensus) to resolve the dispute by requiring a majority of the network to make the final decision. To manage this at scale (so millions of network users do not need to vote for every dispute), the process can be completed by an unbiased user or group of users for a small network fee similar to the OpenBazaar implementation. The number of peers required to achieve consensus in these isolated situations can be based on the level of security required which is typically in direct relation to asset value.

The process becomes slightly more complicated when dealing with Titles. Real estate transactions are a perfect example where this platform makes it easier to securely purchase foreign property and have ownership transferred; however, since the buyer and seller will most likely not be interacting face to face, there are measures that need to be taken to ensure an asset Title was not added fraudulently. This can be addressed by having a verification service (approved by the majority of the network) review and validate submissions. If there is ever a discrepancy, consensus can be used to resolve the situation. While this process may seem like it relies on third-parties, it is only a small portion of the platform. This provides market potential for verification service companies to enter the market quickly and effectively. The most important aspect to take away from this is the elimination of traditional escrow services which are costly and time consuming. As Blockchain and smart contract services around asset management evolve, human reliance will slowly be phased out all together.

6.8. Compliance

With every disruptive technology, compliance and governance is always a factor that needs to be kept in mind. A large and ever-growing issue is the loss of tax revenue through peer to peer (p2p) commerce. This is a result of outdated systems and toolsets, lack of transparency, reporting tools, and ability to audit.

With a Decentralized Asset Management platform, all transactions are recorded in an immutable and transparent ledger that can have real-time accounting and reporting applications built on top of it to not only increase the accuracy of p2p tax revenue figures, but also automate a large majority of the processes, thus saving government and regulatory bodies tons of money.

Pulling vs. Pushing records for auditing. Under current systems data of records must be requested, pulled, aggregated, and then analyzed which is very time consuming. Blockchain enables the pushing of data to a real-time system where an algorithm can automatically keep fully-updated records 24/7 without the extensive overhead costs associated with the manual "pull and analyze" process. In summation, our platform is striving to be fully compliant by enabling government and regulatory bodies to have a way to trace and audit p2p commerce.

6.9. IP Protection

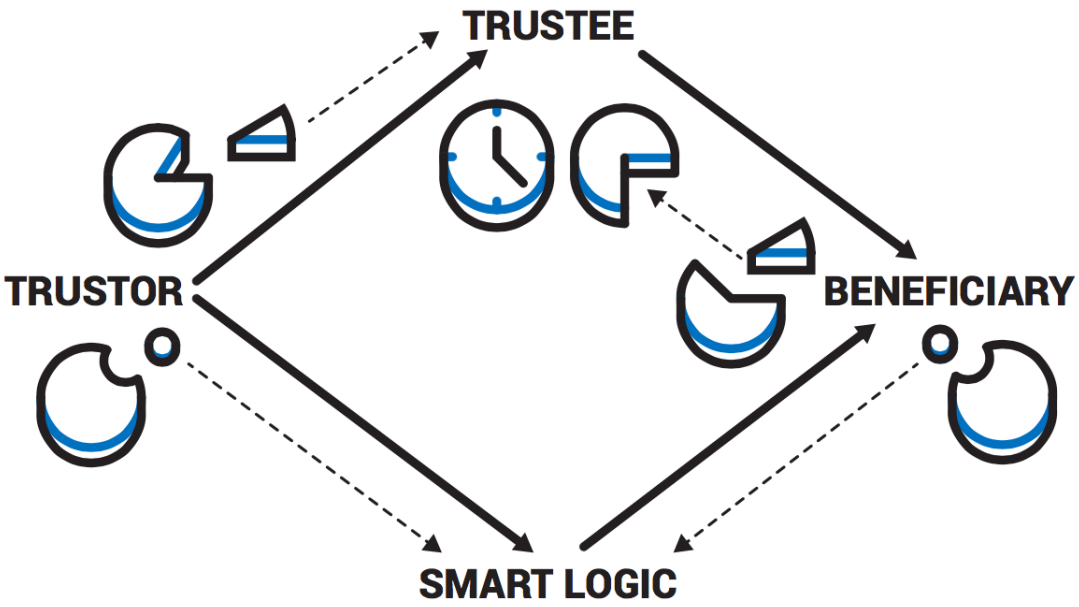
True Blockchain Technology is open sourced (publicly available for people to review). Decentralized Applications MUST be open sourced to function appropriately and provide the necessary levels of transparency; therefore, the structure of this DApp will be open source. What enables us to protect our platform from replication will be the proprietary integration that facilitates (and largely automates) the registration process of physical assets onto the Blockchain in a seamlessly fluid user experience.

6.10. Integration Examples

The following are a few examples of simple, current use cases of the extended MyBit platform which provide real-world value. There are countless additional use cases to be explored, as well as many that have yet to be thought of or implemented.

6.10.1. Smart Trusts

Overhead maintenance expenses of traditional Trusts can be extensive to have trustees (administrator of the Trust) manage and govern them based on provided terms. Smart Trusts are governed by irrefutable computer code to make the process much cleaner, affordable, and manageable.



The trustee's role can be replaced by smart computer code (Trust contract) that is guaranteed to execute as instructed by the trustor (creator of the trust) without the exorbitant fees and reliance on a third-party.

6.10.2. Rating System

By leveraging UBI and singularity in unique asset registration, there is potential for a cross-platform rating system to be put into place to prevent fraudsters from jumping from one commerce platform to the next, continuously ripping off customers. Since an asset registry is immutable and linked to their unique Blockchain Identifier, transactional history both good and bad will follow users, further securing peer to peer commerce.

6.10.3. Insurance Claims

Policy terms and procedures could be transformed into smart contract logic to remove the friction during claims processes. The ownership titles of insured assets could be placed into a smart contract which is governed by policy terms such as remaining active as long as premiums continue to be paid on time, (or a set expiration date) and upon termination of the policy the associated smart contract is automatically destroyed. If a trigger event occurs resulting in the

policy to be paid out the asset titles could automatically be transferred to the UBI of the insurance provider and insurance money sent to the policy holder. Human interaction could be in the form of oversight, rather than actually completing the claims process and interacting regularly with the policy holder saving insurance companies Billions of dollars.

7. The Market

7.1. Securing Commerce

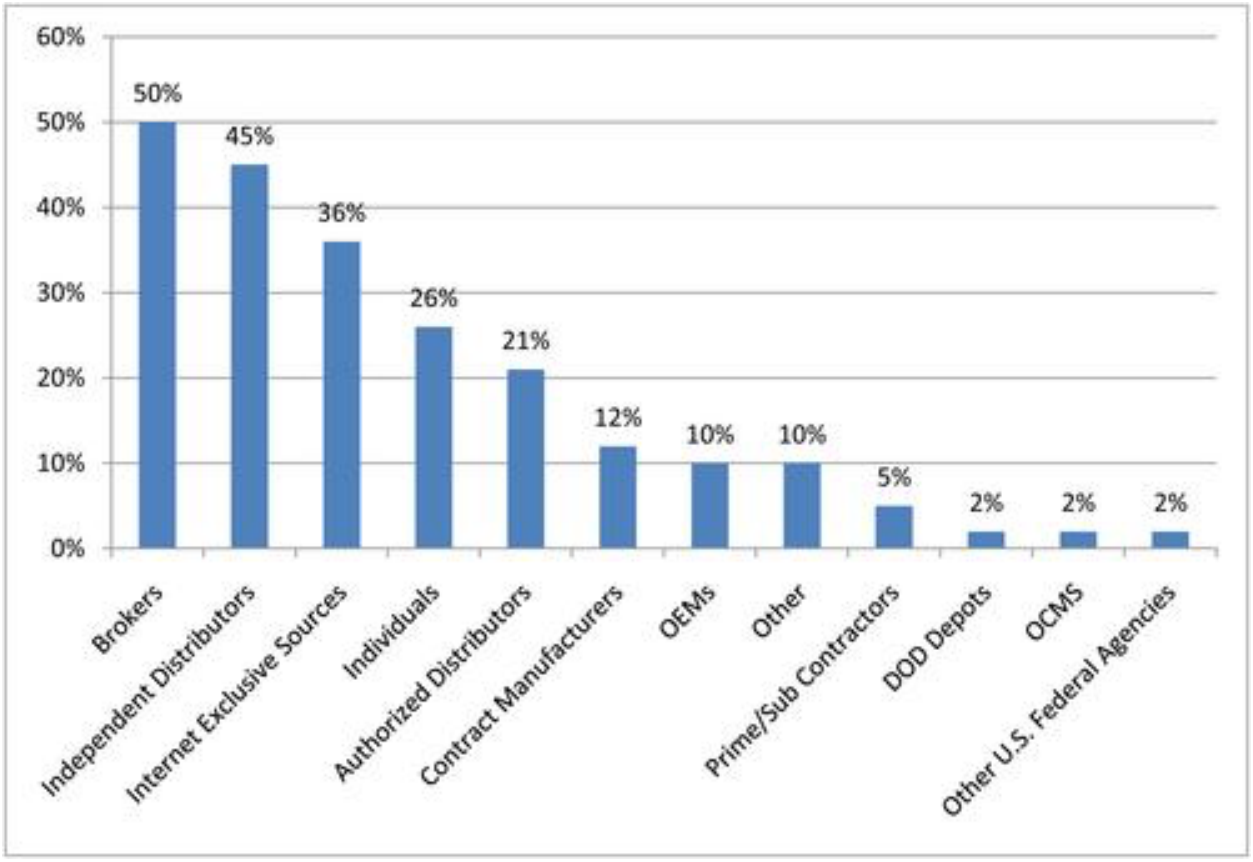
MyBit services have potential for trillions of dollars worth of assets to flow through the platform annually. As of 2015 only 7.3% of commerce was conducted online ($1.672 trillion) out of the the $22.822 trillion total. By 2019 online is expected to grow to 12.4% ($3.551 trillion) out of total retail sales of $28.550 trillion.

These numbers show a few things very clearly. 1) There is a large need for securing offline transactions (proving authenticity and rightful ownership) and tracing lineage. 2) The retail industry is constantly growing. 3) An increasing amount of people are gaining internet access globally so they will be able to utilize our platform.

Therefore, our market potential is poised to continuously grow driven by the factors of an annual increase in total commerce globally and access to internet steadily increasing year over year.

7.2. Value Lost through Fraud

Fraud costs companies an estimated $3.7 trillion each year. That figure does not include the amount of money companies actively spend on fraud prevention measures. The majority of fraud is detected purely by luck – only 3% of fraud is found by auditors according to K2 Intelligence. Everyone loses in the case of fraud. Companies suffer from reduced profits, consumers face an increase in the cost of goods to offset incurred losses, and governments are allocated smaller budgets due to less taxable events.



As the figure above shows, brokers and distributors are the largest contributors to fraud.

7.2.1. Counterfeit

According to the World Trademark Review the counterfeit industry costs companies in excess of $600 billion annually.

- If high-priced items (that are largely affected by counterfeits) were registered at the point of production it would enable consumers to easily verify authenticity by tracing the lineage far beyond the current owner/seller. This would remove friction in the sales process and eliminate the need for costly third-party authentication services.

7.2.2. Supply Chain

Of the $3.7 trillion in estimated annual fraud, the supply chain industry accounts for over $700b of it. Fraud in the supply chain can be particularly hard to spot

due to the complexity of the systems and extreme lack of transparency. The largest contributors of fraud in this industry are project managers and invoice approvers who account for 26% of supply chain Fraud according to a CFO.com survey of 2,600 professionals

- Anti-fraud through transparency – By utilizing Blockchain technology to hash digitalized assets, companies will be enabled to take a real-time view paired with asset tracking to uncover new leakages. They will also be able to identify leakages and react faster. This leads to a more productive ecosystem which generates increased profits.

7.2.3. Healthcare

3 percent ($60b) of annual spending is lost to fraud.

- Automation + consumer control in the managing of records – Easily hash any digital record to provide a timestamped proof of ownership as well as management controls for cryptographically securing and permissioning access to documents. This is a major step towards real-time updates across multiple service providers which strengthens the integrity of available data.

7.2.4. Insurance

An estimated $80 billion a year is lost to fraud across all lines of insurance (*Coalition Against Insurance Fraud estimate*). Fraud accounts for 5-10 percent of claims costs for U.S. and Canadian insurers. Our core focus will initially be property-casualty insurance which accounts for $32b annually (*Insurance Information Institute, March 2015).* Currently, insurers' main fraud-prevention measures involve upgrading analytics to detect fraud before claims are paid. While this is a good preventative measure it slows down the claims process.

- By replacing a large portion of logic and manual processes with automation and computer code that is guaranteed to execute as written, it has the potential to greatly reduce overhead costs to insurers by reducing friction and error rates.

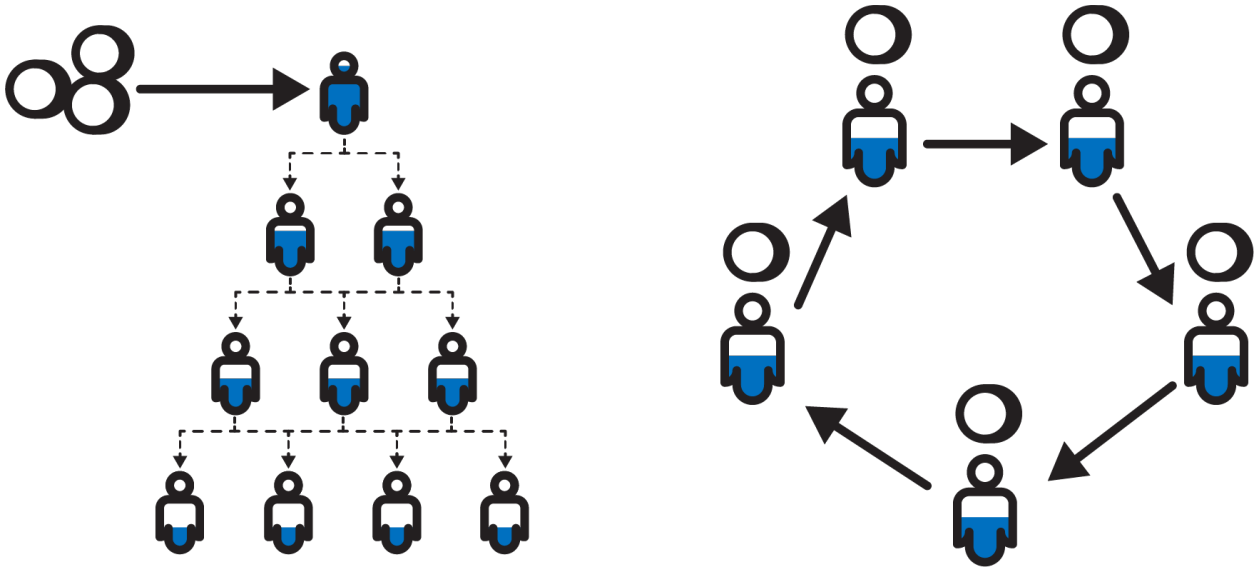
8. Monetization

The core functionality of the application, including the registration, transacting, and querying of assets, will remain free to users and we will monetize by offering a service to secure assets with a smart contract powered Trust that incurs a very small monthly fee.

Another monetization route is to is to charge enterprises an integration and monthly subscription fee to implement mass-registration portals unique to their respective supply chains/business models.

8.1. Profit Sharing

This business model provides a unique compensation model for both active and passive participation. It enables participants to be paid proportionately for the work they have completed. Money flows circularly in the ecosystem rather than flowing to the top as seen in traditional models.



8.1.1. Active Profit Sharing

Developers can profit by developing smart contract powered trusts and customized registration portals for enterprises. An individual or enterprise can submit an RFP for a customized development which developers can bid on.

80% of service project revenues will be paid to the developer(s) who completed it, 20% will be distributed among tokenholders.

Marketing, Sales, and Business Development specialists can receive increased profit sharing proportions for signing up a large retail company.

80 – 100% of monthly subscription revenues will be distributed proportionately to token holders.
0-20% of monthly subscription revenues will be distributed to the specialist who closed the deal. This percentage is determined by the Blockchain Consensus Mechanism in which a majority of the nodes must approve the terms.

8.1.2. Passive Profit Sharing

Tokenholders also have the ability to not directly participate in the development and maintenance of the Decentralized Asset Management platform, but still be rewarded for helping make it a possibility by receiving proportional disbursements of monthly subscription and service revenues and token price appreciation.

8.2. Token Pricing Model

There will be a fixed number of tokens issued. All bids and monthly subscriptions must be paid in the form of tokens. Therefore, it is basic supply and demand theory that proves as demand for the platform increases (more users and companies joining), the value of the token will in theory increase.

9. Team

Our Kick-Ass team brings a fantastic mix of Software Engineers, Blockchain Technocrats, Design Experts, Consumer Product Marketing & Branding Specialists, and Enterprise Application Sales Strategists.

Alex Dulub – Solidity Developer

Alex brings 10+ years experience in designing high-performance and functional enterprise applications. Several years ago he began to focus on Blockchain and Decentralized technologies of which he has created various, custom cryptocurrency and smart contract solutions for a wide range of business applications.

Pedro Barros – Full Stack Developer

Pedro has 6+ years experience as an engineer and has built applications ranging from simple mobile apps to robust enterprise software. His specialties include Angular2, Ionic, Ruby on Rails, Nodejs, and cloud application deployment, to name a few.

Ian Worrall – Decentralized Solutions Architect / Entrepreneurial Background in Finance and SaaS

Ian has been involved full-time in the Blockchain industry since early 2013 when he began a small mining operation that grew rapidly. Since then he has managed a company that builds custom software for small businesses up to large corporations. His true passion is decentralized applications and the potential they have to disrupt traditional business models.

Jacob DeBenedetto – UI/UX Designer

Jacob brings 5+ years of software development and graphic design to the team. He has experience designing and implementing incredible user interfaces across a variety of application verticals.

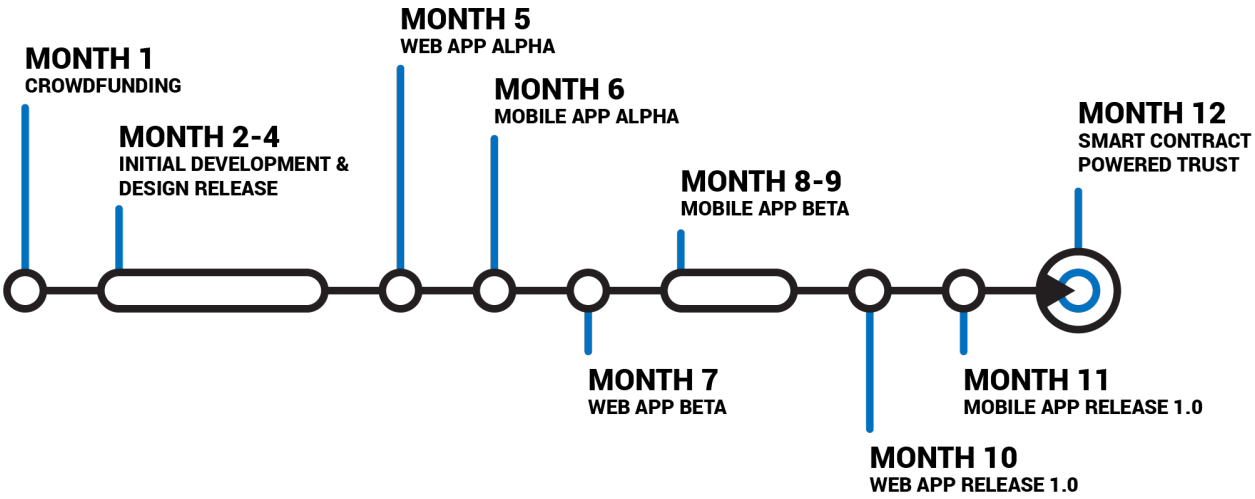
Thomas Pollan – Enterprise Business Applications / Sales & Strategy Background

Mr. Pollan has over 30 years of business consulting and business start-up experience. Mr. Pollan's roles have included Senior Director, Client Principal with Hewlett Packard Enterprise, Senior Partner with Accenture, and founder and President of Pollan Enterprises, a multi-million dollar holding company for new start-up businesses.

Garrett MacDonald – Community Manager / Marketing & Branding Background

Garrett is a passionate innovator who has been involved in the Bitcoin/Blockchain industry since 2011. He has founded a million-dollar bitcoin mining company, lived by himself in a log cabin in the Rockies for a winter, and has traveled 20,000 miles around Europe on his motorcycle.

10. Milestones Timeline



11. Community Driven Development

Transparency and interactions with our community are our core principals. We want to keep the community updated with every major milestone achievement, issue, resolution, and updates. Bi-monthly releases will be sent out to all network participants on a private channel and regular AMA sessions will be hosted on Reddit or Slack.

We want to give everyone a chance to be involved by contributing code, sales, marketing, Beta testing, etc. to help drive this to success.

“In this new world there are no more winners & losers, everyone succeeds or fails together so let’s join forces & kick some butt!” – Ian

For a full list of our social channels please see below:
Facebook: https://www.facebook.com/MyBitDApp/
Twitter: https://twitter.com/MyBit_DApp
LinkedIn:
Slack:

Reddit:
Medium:
YouTube:

Voting: We will use consider.it for community consensus management during the development process so our approach is transparent and the community can actively engage in driving the development decisions of our platform. Each token will account for 1 vote.

12. Conclusion

This paper has introduced Mybit, a decentralized asset management platform, which provides a more efficient and secure method to administer ownership. It has the potential to disrupt traditional systems, offering immense value to both individuals and companies. It removes the friction in the registration, transfer, and overall management processes of assets. MyBit functionality is designed to be a building block for future asset management systems utilizing a decentralized architecture.

13. References

"Centralized Vs. Decentralized Organizational Structure." *Centralized Vs. Decentralized Organizational Structure | Chron.com*. N.p., n.d. Web. 12 Jan. 2017.

http://keydifferences.com/wp-content/uploads/2015/05/Centralization-Vs-Decentralization3.jpg

Norton, Steven. "CIO Explainer: What Is Blockchain?" *The Wall Street Journal*. Dow Jones & Company, 02 Feb. 2016. Web. 12 Jan. 2017.

DavidJohnstonCEO. "DavidJohnstonCEO/DecentralizedApplications." *GitHub*. N.p., 02 Feb. 2015. Web. 12 Jan. 2017.

"Decentralized Application Layer." *Decentralized Applications - Codius Docs*. N.p., n.d. Web. 12 Jan. 2017.

http://image.slidesharecdn.com/blockchainfromabankingperspective-160419115524/95/blockchain-from-a-banking-perspective-18-638.jpg?cb=1461068068

Mougayar, William. "Understanding the Blockchain." *O'Reilly Media*. N.p., 15 Jan. 2015. Web. 12 Jan. 2017.

Chan, Ronald. "Consensus Mechanisms Used in Blockchain." *Linkedin*. N.p., 2 May 2016. Web.

"Ethereum Project." *Ethereum Project*. N.p., n.d. Web. 12 Jan. 2017.

"Proof of Knowledge vs. Proof of Membership." *SpringerReference* (n.d.): n. pag. Web.

"Blockchain Technology." (2016): n. pag. Web.

Pabari, Mayur. *Decentralized Specs*. N.p.: Mayur Pabari, 9 Jan. 2016. PDF.

Matt Lindner Associate Editor. "Global E-commerce Sales Set to Grow 25% in 2015." *Global E-marketer Set to Grow 25% in 2015*. N.p., n.d. Web. 12 Jan. 2017.

Quiggle, Dennis Jay Jim. "By the Numbers." *Fraud Statistics*. N.p., n.d. Web. 12 Jan. 2017.