Methuselah v2 Whitepaper

The world’s fastest blockchain-powered botanical tracking system

Table of Contents

Introduction

Imagine being able to scan a code on a recent purchase and know where the plant grew, in what conditions, and who handled it until you bought it. This kind of open information is the future of supply chains and it's already here today. There are already current blockchain offerings but none that specifically target botanicals that can be used by farmers, vertical or otherwise, merchants, distributors, testing facilities, and so much more.

We present to you the world's fastest blockchain-powered botanical track and trace platform with a full suite of free software that ensures better consumer safety and regulation adherence. We have used the latest technology, the best practices, cryptography, and a whole of experience to provide a unique modular platform.

Our goal is to present to you a no-nonsense alternative to the typical state-mandated archaic software platform. We aim to provide an open platform where information is freely available with privacy where expected. Regulation is easy and open for government entities and the general public.

Continue reading to gain an understanding of what we intend to provide and how it is superior to the current offerings both distributed and centralized.

Integration with current regulation systems like Metrc is provided. Methuselah will become a certified enterprise partner in order to automate integration with provided software solutions with an eventual goal of obtaining future state contracts becoming an industry leader.

The home base for the founding team is currently the USA but the platform is intended for an international audience.

Overview

After researching the budding cannabis industry and working in cryptocurrency space, it has been realized that there is a noticeable miss for a quality merge between the two. Some previously released big-name coins have been nothing more than forks that offer no real innovation to either industry. State-mandated systems are nothing more than giant CRUD applications that require tiresome manual data entry and lock you into using their platform at extra costs.

As you continue to read you will be convinced that Methuselah offers a sound realistic implementation in the tracking of botanical assets, cannabis or otherwise. Beyond being user-friendly it is also one of the fastest blockchain systems currently in existence that offers a hybrid delegated proof of stake and proof of ownership consensus protocol.

Security is a priority of Methuselah and this is shown in the design of the system that limits corruption to only a single account, minimizing the overall impact on the network to none. Each account is responsible for its own sidechain that uses proof of ownership while a centralized blockchain is validated using a delegated proof of stake.

The simple but effective transactional layer of Methuselah allows for easy expansion to different verticals: instant secure messaging, decentralized database systems, scientific/research data sharing, biometric identification systems, private blockchains, smart contracts, etc.

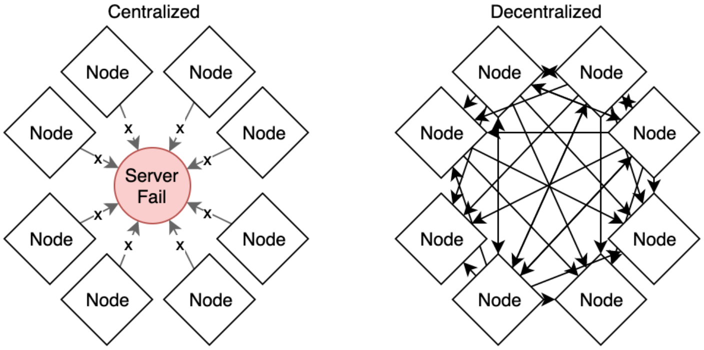
Identified Problems

Manual data entry is prone to human error and can cause time delays if the information is not immediately entered in current regulatory enforced systems. Manual entry systems provide the opportunity for malicious intent making sound cybersecurity best practices even harder. Current systems are not optimal providers of accountability within the system and provide analytics for business optimization being nothing more than modern data entry terminals that mimic those of the 80s and 90s.

Health hazards or product contaminations in current tracking systems are without real-time cost-effective notification systems. Product recalls currently can cost upward of tens of millions of dollars not including the loss in sales and damaged reputation.

The current systems typically use RFID technologies that require users to purchase tags from them and do not take advantage of readily available mobile devices that can scan QR and other barcodes without the costs of unique equipment.

Centralized systems are a single point of failure, require maintenance, come with a cost, and do not offer the redundancy of a decentralized network. Servers must be maintained by a professional and often rely on 3rd party sources for hosting and connectivity, exponentially increasing the risk.



While providing no incentives to its users, the economic and environmental impacts of these legacy systems and methodologies are not forward-thinking but are in a constant state of depreciation.   Costs are passed to its users who have no choice but to go with the less than ideal circumstance or face prosecution.

Straight to the point, current systems do not make life easier for users and there is no legitimate reasoning behind sticking with legacy monolithic systems that continue to fail over and over again.

Problem Analysis

Methuselah focuses on the users of the system by providing a professional, researched, and tested user experience that decreases the occurrence of errors by limiting manual entry to only what is required beyond what can be realistically automated.

The decentralized ledger that is commonly referred to as the blockchain, provides optimal accountability with an open format making analytics extremely easy. At any time from anywhere in the world, the life cycle of the product can be tracked and researched for accuracy. Regulatory bodies don't have to enforce reporting as it comes readily available for viewing and is encouraged by Methuselah.

The connected nature of Methuselah allows for the best safety reporting in the entire world. Customers can be notified in real-time decreasing the potential harm and possibly saving lives. Methuselah offers targeted notifications to only affected entities in the supply chain as well as public safety notices.

Save money by using the equipment already available without the recurring costs of RFID tags. Methuselah can integrate several different identification systems even supplementing currently used systems. Due to the open-standard and open-source nature of this project, integrations are amongst the easiest possible. Methuselah leverages, but is not limited to, mobile technology to lower costs of operation for its users and decreases onboarding times to get up and running.

Methuselah does not require a hosted or maintained server architecture in addition to the individual users' hardware configurations. There are no recurring costs for maintenance and thus no requirement to charge users to use a mandated system.

The hardware requirements for Methuselah are minimal, a Raspberry Pi is more than enough to operate the platform, most organizations already own more than enough to start using it. Safety is not furnished by the hardware or software running the API but provided by industry-proven cryptography that is backed by vetted mathematics. There is the potential for side-channel attacks as with any system but Methuselah protects against them as much as feasibly possible.

Methuselah has a positive environmental impact as it requires less electricity, less hardware, and minimal staff in order to operate. Operation costs for Methuselah are pinned to transaction fees saving hundreds or even thousands a month for an average small to medium business.

Methuselah improves users' lives by increasing time and money that provides the freedom to focus on other aspects of life or business.

The Past Considered

Inspiration comes from current international standards like GS1 and ISO standards. They have served us well and will continue to do so in the future as they paved a path to providing regulation and a standardization of processes that makes supply chains and asset management better. Although these organizations and systems have improved things, they also limit the availability of information to the general public and have a fiscally high point of entry. In order for a system to be widely adopted, it must be accessible for everyone as well as being easily understandable going forward.

The current most widely used blockchains today use proof of work or proof of stake; while serving its purpose, it has a large negative impact on the environment and also a high point of entry to use. Proof of work algorithms require expensive hardware and high energy costs in order to be competitive, while proof of stake algorithms require large investments being prone to manipulation due to flaws in the most commonly used staking protocols. There have been 51% attacks, stake grinding, resource exhaustion, and many other inconsistencies in current implementations over the years.

Things have been changing for the better, but the need for full archiving of ledger data seems to be consistent with security and is still a misconception even though it is common practice. There is no need to fully track everything, only what is required to ensure security is met, this is visible in the movement of using snapshots in place of full chain data for several blockchains.

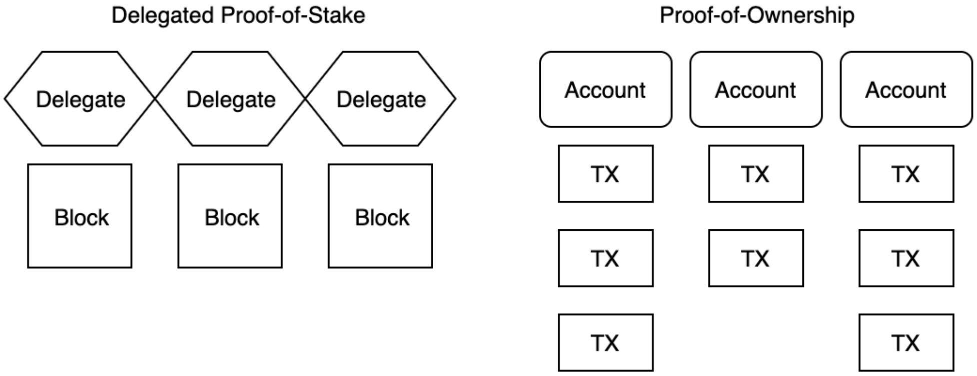
In the past selecting a software solution and its hardware was an all-in commitment that has been outgrown by the incoming gig economy and subscription models. Today entities, users or corporations, should be able to easily integrate solutions that they need without committing to the costly full suite of systems of the past.

Current blockchain systems mostly provide full disclosure of all data and have resulted in the rise of private blockchains for corporations and the like. There needs to be the possibility for public and private data going forward for a broader acceptance of the technology.

Several of the most popular blockchain systems deployed today have a long initialization period that can take weeks to become an active participant on the network. In order to cut down on these times users must have an intermediate understanding of a broad range of technologies in order to actively decrease this period without the loss of security. This is not a common acceptable metric of usability, and prevents further adoption by the general public. Initialization and setup should take only minutes in order to keep with current usability trends and prevent negative psychological framing. Previously this aided in the security of the system but is no longer a requirement.

Analyze Differences

Instead of using the more common consensus algorithms or even a single one, Methuselah uses a hybrid approach that decreases initialization time, lowers hardware requirements, and saves on the required space needed to run a node. Even full archiving nodes such as delegates still only require minimal time to download.



Proof of work requires miners to calculate hashes in order to obtain a hash that meets a threshold to be considered valid. This threshold is changed in order to control the output of blocks and consequently coins into the supply. The ecosystem of Methuselah does not require a controlled emission as all tokens are generated initially allowing for speed to become the primary focus next to security. Blocks can be generated as fast as they can be validated without the worry about inflating the price. There is no need for special expensive hardware as validation is doubled by ownership verification and bonds staked by elected delegates. Obvious inspiration comes from Bitcoin.

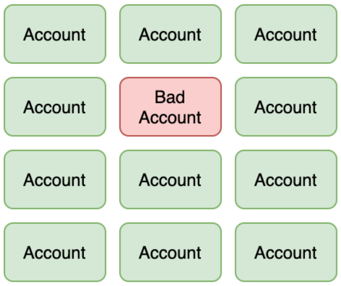
Proof of stake, most commonly, requires wallets or nodes to be connected to the network at all times increasing the demand for electricity lowering ROI. Many staking protocols are prone to manipulation by taking advantage of time and holdings. Methuselah only requires that delegates be online and active freeing users from running servers or worrying about losing their internet connection. Manipulation is avoided by the use of bonds that delegate posts for each block they create that becomes forfeit if the block is voted invalid by other delegates; which removes the need for complex calculations and relying upon the accuracy of previously validated data. Calculations in Methuselah are simple and very specific to avoid tolerance levels being used to gain an advantage. Inspiration was mainly taken from Peercoin, PIVX, and more recently Tezos.

Methuselah does have an investment layer similar to masternodes in many aspects, except unlike masternodes delegates actually serve a real purpose beyond being money grabs or a form of ICO. Delegates must be vetted by the Methuselah Foundation and meet performance requirements in order to keep their active status and be elected to win rewards. Delegate performance is constantly monitored by the foundation to ensure proper operation of the network.

Instead of a specific governance protocol, a democratic approach is preferred: accounts vote for a delegate that will have a positive impact on the platform. Delegate elections are based on the popular vote of accounts at a specific time in each term. Voting can be done at any time allowing for the quick movement away from unfavorable or underperforming delegates. Experience has shown that current proposal based systems lack participation and the risk required to entice good behavior.

Most blockchain systems like Monero and Bitcoin aim at trying to keep some form of, if not absolute anonymity for its users while Methuselah takes a hybrid approach of public exposure and privacy. Corporations or types of partners to the platform must have their information public, just like any other store or service provider, while regular users can enjoy the privacy of staying anonymous without losing the ability to receive safety-related notifications about their purchased products. This does not prevent partners of the platform from utilizing a private chain and keeping their data completely anonymous.

Most common blockchain structures resemble that of a linked list or other linearly structured data systems. Methuselah uses a block lattice-type structure that allows for accounts to be their own sidechains that are secured with proof of ownership. As mentioned, this limits the potential impact of a compromised account to only that account, but also optimizes storage space to maintain at minimum, the head of the account or last transaction; taking space from possible terabytes of data to megabytes. If one is familiar with the technology, it is possible to run Methuselah v2 on an ESP32 microcontroller. The lattice-type structure is comprised of send transactions initiated from an account with those transactions being validated by delegates in blocks. Inspiration was taken from Nano in regards to the block-lattice structure and focus on speed.



Compromised accounts are isolated.

For clarification, there are two concepts of a “blockchain” in Methuselah, the central validation blockchain using a delegated proof of stake and the individual account sidechains that are backed by proof of ownership. Delegates provide another layer of validation by verifying the accuracy of transactions created by accounts and voting upon the grouping by other delegates. Accounts prove ownership of the chain and the new data associated with it using cryptographic signatures. Slight inspiration from Hyperledger and other permission-ed blockchains.

The decision to avoid the UTXO model in favor of sequencing was chosen for Methuselah in order to keep the node requirements lean while still providing the ability to perform batch transactions. Only the account can increase its sequence on its sidechain. This design decision was inspired by Stellar.

Analyze Solution

In this section, we will go into greater detail about the decisions made and why we believe that they are correct and suitable in the new architecture of Methuselah.

Go was the selected programming language of choice for the rewrite from scratch because of its support, simplicity, very easy cross-compilation, and built-in concurrency capabilities. Go was created by some of the same individuals that brought us C, UTF8, and Unix, basically very smart people. Go is not as low level as C or C++, the most commonly found languages in the space, so there are less inherent risks of exploitation.

Badger is a key-value file storage system that provides high-end performance on more common SSD drives. It is written in Go and does not require any external dependencies or interfacing. There are forks of go-eth (Ethereum) that use badger due to its performance. LevelDB implementations, at the time of writing, require interfacing overhead between Go and its native language.

Noise protocol is written in Go by Perlin Network and provides end to end encryption and Kademlia hash table routing. The interface is simple and allows for granular control of message formats while simplifying NAT traversal out of the box. LibP2P by IPFS is another popular choice for distributed networks written in Go but suffers from a specific use case not closely aligned with Methuselah's.

ED25519 is an elliptic curve public-key signature algorithm used for accounts due in fact that it provides fast key generation, signing, and signature verification. It provides strength similar to a 3000 bit RSA and has a 2^128 target while avoiding side-channel leakage attacks. Public keys are small containing only 32 bytes without compression. This allows Methuselah to maintain its lightweight data requirements.

Delegated proof of stake adds a second layer of validation and investment that is self-regulated where all elected delegates in a term must validate every block. Delegates must also come to a majority agreement of 75% on every block in order for the block to be considered valid.

Before a delegate's turn in block creation, they must submit a bond transaction to the network that will be held until it expires or used in a valid forfeiture. The bond transaction will be included by the next delegate if forfeit or removed from the pool. Delegates that do not produce a block within 5 seconds or their block is not voted valid lose their turn and bond.

Delegated proof of stake allows for offline staking and reward potential for its constituents with kickbacks and network improvements. Accounts can elect a delegate that provides rewards creating the potential for staking pools.

Account sidechain proof of ownership empowers the modular design of Methuselah while allowing for easy additions of functionality based on an account. Ownership is proven by the account signing transactions that can be validated with the signature, sequence, and its publicly known public key.

Resource usage is light and relies heavily on the underlying cryptography which means if an account is compromised, which will happen as someone always get socially engineered, the damage is limited to only that account, the perpetrator cannot prove ownership of any other account.

Required operation size for a connected node grows linearly with the number of active accounts. Account lookup, along with all sections of Methuselah's code is asymptotically optimized for performance.

The popular vote was selected as an easy no-nonsense way of calculating totals at any given time on the blockchain. Delegates are easily selected from most votes to least with only the top 21 being selected for the next term. Delegates must provide KYC information before being accepted and the cost of maintaining minimum balances alleviates any form of Sybil attack against the voting process.

Total supply exists at the very beginning and is held in genesis accounts that are hardcoded into the consensus protocol and controlled by the foundation. Fraud is easily shown by the internal reporting requirements of the foundation that will make all transactions public knowledge.

Summary

Methuselah is part of the next generation of blockchain technologies with practical application, professional engineers, experienced architects, and world-class performance.

Methuselah is not looking to take anyone's BTC or blow smoke, but to provide a realistic option to safety utilizing blockchain on emerging and current botanical markets and supply chains. It is a legitimate software offering with real potential and eventual incorporation.

If a cost-effective professionally developed supply chain and merchant solution sounds like a good idea then we encourage you to look at Methuselah as a viable option for migration or start.

Terminology

Account - It is a cryptographic key pair that holds a balance and signs transactions. Transactions have a minimum balance to be considered active on the network.

Address - The public key address for an account that can receive transactions on the platform.

Block - A group of transactions that will be validated and voted upon by other delegates in the current term of its creation.

Block Vote - Delegates vote on blocks during a round in a term to validate the accuracy of the delegate creating the block.

Bond - An amount of stake in the creation of a block that will be forfeited by a delegate if an invalid block is provided by a designated position in the current term.

Delegate - A vetted account that is allowed to receive votes to be selected for a position in a term to create blocks for a reward. Delegates must pay a fee and provide KYC information.

Delegate Node - A full node ran by a delegate that must meet hardware and performance requirements during operation or it will lose its position and delegate status for the operator.

Election - The tallying of votes for delegates placed in order of most to least to select delegates for the next term.

Fee - An amount paid to the foundation for redistribution back into the platform and it's supporting systems.

Forfeit - The loss of the bond posted by a delegate during block creation. The bond is paid to the delegate in the next position in the current term.

Foundation - The governing body of the platform that manages fees and the base protocols of the network.

Genesis Account - The initial accounts governed by the foundation that is hardcoded into the protocol.

Module - A piece of software that runs on the platform and adds a set of features to the network.

Name - The label for an account on the network.

Network - The sum of all nodes connected under the consensus protocol.

Node - An account connected to the network abiding by consensus protocols to communicate with other nodes. A node can operate in different modes that will provide different features depending on its settings.

Peer - Peer is often used specifically in the networking layer of the peer to peer protocol but is synonymous with a Node.

Position - An ordered placing in a term held by an elected delegate selected by a majority vote.

Rename - The act of relabeling an account on the platform for a fee.

Term - A term, a set the number of blocks in length, in which votes are tallied and delegates are selected by a majority to do the creation and validation of blocks.

Transaction - The base component of the platform that is transmitted from peer to peer that contains network and module data.

Transaction Fee - The amount paid by an account to a delegate for selection in a block.

Vote - The act of an account voting for delegate in hopes that the delegate is a majority and selected for the next term. Votes are permanent until changed by paying a fee.