



DigiByte

Community Infopaper

V1.0 April 2020

Introduction & History

DigiByte is a truly decentralized UTXO blockchain that was fairly launched on January 10, 2014. DigiByte is also truly permissionless, since there is no central controlling authority. Accordingly, this Community Infopaper is written without requiring authorization from any single individual.

The DigiByte blockchain is an immutable ledger, a chain of blocks all with verifiable digital signatures since its creation in 2014 and backed by billions of dollars of cryptographic computation. Its blockchain is also fully open-source, released under the MIT license, and completely verifiable by any individual or entity. DigiByte embraces the Bitcoin core ethos of “Do not trust, verify”, in that no entity should ever need be “trusted” in order to send/receive DigiByte (DGB) or to store/retrieve data from the DigiByte blockchain.

DigiByte originally utilized the Litecoin code-base, with a completely independent blockchain and a unique Genesis Block. It has undergone several non-contentious soft-forks and hard-forks, none of which culminated in a chain-split, but rather a complete consensus resulting in seamless upgrades of the entire DigiByte network.

DigiByte never held an ICO, but was fairly launched in an open and transparently planned manner. DigiByte does not take a percentage of block-rewards for a founders fee. The minimal 0.5% pre-mine was given away in its entirety to community members in the first month of its existence in order to incentivize early client downloads, ensure the survival of the blockchain, and to develop the original Android/iOS applications.



DigiByte focuses on speed, security, and scalability. It prides itself with being “faster, more secure, forward thinking”. With significantly faster block timings than any other UTXO blockchain to date (15 seconds), DigiByte has encountered and overcome a number of issues that many other blockchains such as Bitcoin will not face until the advent of the next century. It is due to this forward thinking nature that DigiByte adopted the SegWit protocol through a soft-fork consensus in 2017, being the first major blockchain to do so, well before Litecoin or Bitcoin adopted the upgrade.

DigiByte believes in on-chain scalability as a core tenet of its blockchain, with “second layer” protocols never expected to be the primary “solution” for increased throughput or transaction capacity. This on-chain scaling coupled with OP_codes and SegWit allows for a large number of usage scenarios, such as distributed applications (DApps), document notarization/validation, token issuance, and asset digitization.

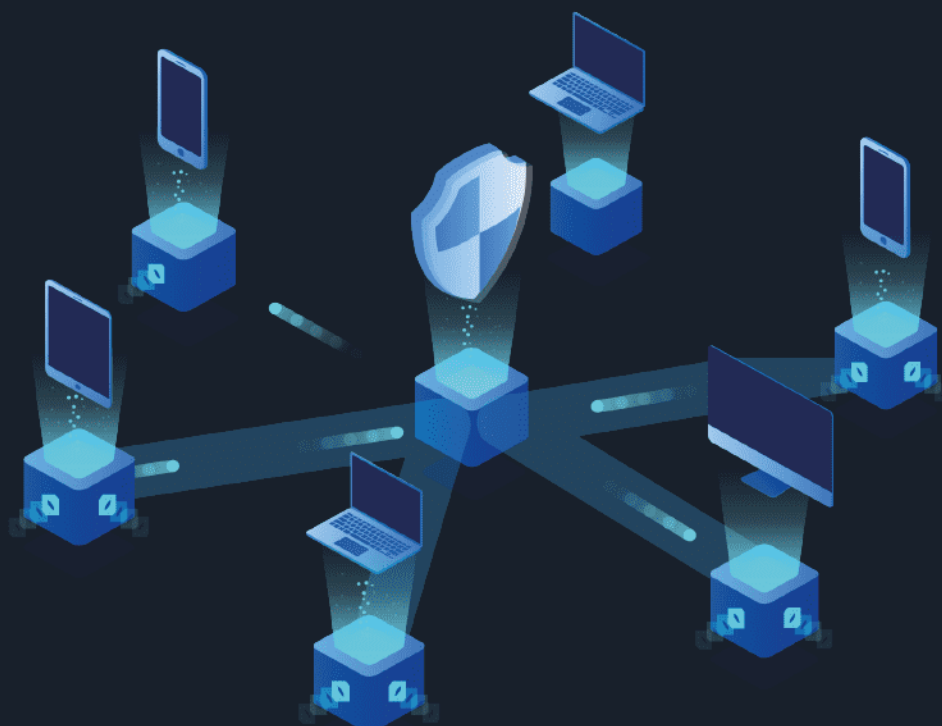
DigiByte has a maximum supply of 21 billion DigiByte, to be fully mined by the year 2035. While other blockchains only utilize a single mining algorithm to mine new blocks and introduce new assets into circulation, DigiByte has employed five unique and independent algorithms in a “MultiAlgo” solution since block 145,000 in September 2014. DigiByte holds the dominant hash-power in 3 of its 5 algorithms globally, by an order of magnitude more than any other competing blockchain. This provides greater security to the network while helping prevent any “rented hash power” from attacking the blockchain.

DigiByte continues to pioneer in the areas of security based on the “forward thinking” of its foundation by creating the Odocrypt algorithm. Odocrypt is a mining algorithm which rewrites and morphs itself every 10 days in order to prevent ASIC dominance, focusing on utilizing FPGA mining. Future algorithms will also likely be replaced as necessary on an on-going basis to ensure maximum security of the DigiByte network, while simultaneously expanding upon the decentralization/distribution of the DigiByte blockchain.

DigiByte has been leading innovation with the industry-renowned DigiShield, a real-time difficulty adjustment mechanism which ensures the stability of block generation timing, despite exponential increases/decreases in mining hash power. DigiShield is utilized in a respectable number of other major cryptocurrency/blockchain projects, such as Dogecoin, ZCash and dozens more. DigiShield was originally created for a single mining algorithm, and shortly after DigiByte changed to MultiAlgo, it was ported and upgraded to become MultiShield. This allows for regular block timings across multiple mining algorithms, as well as an even block mining distribution between algorithms, while also preventing mining dominance in the event of a sudden inflow/outflow of substantial mining hash power.

DigiByte Key Specifications

Launch Date	January 10th, 2014
Genesis Block Hash	"USA Today: 10/Jan/2014, Target: Data stolen from up to 110M customers"
Blockchain Type	Public, Decentralized, UTXO, Proof of Work, Multi-Algorithm
Ticker Symbol	DGB
Maximum supply	21,000,000,000
Block Reward Reduction	1% reduction monthly
Block emission schedule	Fully mined by 2035
Mining Algorithms	SHA256, Scrypt, Odocrypt, Skein & Qubit
Algorithm Block Share	20% per-algo, contested each block
Difficulty Retarget	Every block, 5 separate difficulties (Per-algo)
Block Timing	15 seconds per-block (75 per-algo approx)
Segregated Witness Support	Yes (First major blockchain to activate)



Key Aspects of DigiByte

Decentralization

DigiByte is the most decentralized Proof-of-Work-mined blockchain in the world. Decentralization means there is no central controlling entity that is able to dictate direction, terms, use of the network, changes, charges and fees, locking of funds, or undoing transactions. Although the world predominantly understands centralized control, the mind-shift to decentralization is an incredibly important progression in today's global society. Where many other cryptocurrencies concede significant compromises in one or more aspects of decentralization (if not all), DigiByte remains unwavering in its dedication to decentralization as a key aspect of being a globally distributed blockchain solution.

DigiByte maintains this decentralization through a combination of methods, namely:

- 1) Multiple algorithms;
- 2) GPU/FPGA mining;
- 3) On-chain scaling;
- 4) Educating the importance of running a full-node;
- 5) Embracing code contributions that uphold the ethos of DigiByte.

This decentralized nature is of vital importance not only for the survival of the DigiByte blockchain, but also to prevent any tampering from malicious actors, governments or corporations. Due to the lack of any “head” or controlling party, there is no entity to manipulate, blackmail, or “lean on”. In a world growing ever divided, there is solace in the consensus of the DigiByte network, that it can be relied upon as accurate and truthful without reservation.



Pure Consensus

This consensus is the core foundation of the DigiByte blockchain. Since its inception in January 2014, DigiByte has had its consensus mechanism reliant on the belief in on-chain scaling, speed, security, and forward-thinking progression of the DigiByte blockchain.

This consensus is obtained through a vastly distributed network of nodes running the Core DigiByte wallet, which holds a complete and continuously updated copy of the DigiByte blockchain, as well as block creation via the “Proof-of-Work” (POW) mining method. Other blockchains have shown that Staking, Distributed Proof-of-Stake, and other such poor attempts at alternative consensus methods are far too susceptible to centralization, manipulation, and tampering by various malicious individuals or organizations. Similarly, trusting a 3rd-party for consensus defeats the purpose of being a distributed and decentralized blockchain in the first place, with users genuinely being better off with a centralized database.

Proof-of-Work is the only proven and reliable method of obtaining a distributed and decentralized consensus (A solution to the Byzantine Generals Problem), which is why DigiByte proudly remains true to POW. Proponents of alternatives usually cite delays in block creation and propagation; however, thanks to DigiSpeed, the DigiByte blockchain overcomes this. Which is why the most battle-hardened POW consensus method is still being utilized today for DigiByte. There has never been any rational argument against the ability of POW to arrive at a sound consensus.

Permissionless Network

DigiByte is a completely permissionless blockchain. Since there is no centrally controlling entity to dictate the network, there is no need to seek “permission” from anyone. As such, permission is implied no matter what “use case” you would like to implement or accomplish with DigiByte. Examples include advertising the acceptance of DigiByte as a payment method, listing DigiByte on an exchange, using DigiByte with your platform/service, or when spending/sending/receiving DigiByte. In addition, anyone is free to speak on behalf of DigiByte, to promote DigiByte, or to even author a community Infopaper such as this.

DigiByte's permissionless nature is both a by-product of decentralization, as well as an intentional aspect that the community deeply values and celebrates. This is what also prevents influence, changes, or take-overs by malicious parties, because the permissionless nature requires consensus from the majority of the network. It is a key characteristic of DigiByte which has held up against any would-be attempts from malicious actors for the past six years and counting.

On-Chain Scaling

DigiByte is a network that believes on-chain scaling should be the primary method for future growth in transaction volume and frequency. A true transaction only happens when it occurs on-chain and has been incorporated into the blockchain. Compare this to second-layer methods where transacting can occur without ever being presented to the network, thus defeating one of the primary reasons blockchain as a technology was created, immutability.

The very essence of the DigiByte blockchain is predicated upon the fact that all blocks since the very first Genesis Block are able to be replayed and cryptographically validated, with all transactions being visible. There are no anonymous/shielded transactions employed, as DigiByte believes a key defense for anonymity is the significant growth of on-chain transactions and the pseudo-anonymous nature of the UTXO's architecture. In keeping with that philosophy, the DigiByte blockchain will scale in future through block-size increases, with proposals for the size to double every 2 years.

Broad support & network participation

DigiByte aspires to be broadly supported across a variety of platforms, to encourage participation from as many entities as possible. Part of pushing the boundaries regarding block timings / sizes means that not all will be able to participate with a full Core Node (for example, drivespace / data transfer / memory requirements), however broad support is available across Windows, Linux & OSX.

DigiByte development has also intentionally added backwards compatibility for older versions of Android that are prominent in developing & impoverished nations. This allows for greater participation, despite aging hardware devices. Broad network participation is also why the Android / iOS applications have been translated to 50+ native languages.

Protocol Upgrades

DigiByte at Launch

DigiByte was the brainchild of Jared Tate, who wanted to create a blockchain that addressed many of the perceived shortcomings of Bitcoin. DigiByte originally started out as a Script-only mined blockchain, with 60 second block times and a two hour difficulty retargeting frequency. Compared to every other Proof-of-Work UTXO blockchain that existed during its 2014 launch, this was considered incredibly revolutionary, and still is to this day. Although the block-timing has changed with network upgrades, the maximum supply of DigiByte will always remain fixed at 21 billion and the last DigiByte to be mined is scheduled to occur prior to the year 2035. DigiByte was created to be “forward-thinking”, with two primary objectives: cybersecurity and on-chain scalability. This is why the news article headline “USA Today: 10/Jan/2014, Target: Data stolen from up to 110M customers” was hashed into the Genesis Block. These guiding principles have remained in effect over the past five years, and will continue to guide the future of DigiByte.

DigiShield

During the launch of DigiByte back in 2014, most blockchains utilized either SHA256 or Script algorithms. Mining pools that would automatically profit-switch known as “Multipools” would regularly switch back and forth between cryptocurrencies that they mined, depending on the mining difficulty and the block-rewards. Miners utilizing these Multipools would have their hashing power changed between a variety of blockchains - such as from DigiByte to Dogecoin to Litecoin.

These fluctuations would cause blockchains to sometimes experience exponential increases in mining hash-power of up to 10 times the normal level, which would rapidly speed up block production until the next difficulty retarget. Once the difficulty retarget for the blockchain had occurred, making mining more difficult and less profitable, the hash-power would then be taken to another more profitable blockchain. This led to many blockchains seeing a rush of block production, followed by a complete stalling when the hash-power fell off. Some blockchains could go for days without a block being found as a result of the major difficulty adjustment. This unsustainable volatility led to the development of DigiShield. DigiShield was created as a mechanism for real-time adjustment of block-difficulty, which allows for the effective handling of sudden influxes of mining hash-power or the equally significant outflux.

This prevented “chain-freeze” and also helped smooth out block creation times. DigiShield was implemented on the DigiByte network as the first protocol upgrade on February 28, 2018 at block height 67,200.

The DigiByte core developers then directly assisted the Dogecoin development team to implement DigiShield, another of many blockchains that had been suffering as a result of erratic Multipool hash-power swings. DigiShield has since been implemented in dozens of other blockchains such as Zcash, Ubiq, and Monacoin.

MultiAlgo

DigiByte upgraded its network yet again on September 1, 2014 at block height 145,000 with the implementation of multiple mining algorithms. While some blockchains had initially launched with multiple mining algorithms, DigiByte was the first blockchain to upgrade from single to multiple algorithms.

The change to five algorithms (SHA256, Scrypt, Qubit, Myr-gr and Skein) was initiated in order to improve the security of the blockchain, while allowing for equitably distributed mining, decentralization, and increased protection from 51% attacks. By having some of the algorithms remaining “GPU friendly”, it allowed for people to mine DigiByte from home, contributing to the security of the DigiByte network from their desktop PC.

It was also at this point where the block timing was adjusted from 60 seconds to 30 seconds, which was approximately 150 seconds in between each mining algorithm finding a block. This further affirmed DigiByte as a leader in the UTXO blockchain space and was also the second seamless and non-contentious network upgrade that DigiByte successfully executed.



Since DigiShield was originally created only for single mining-algorithm blockchains, this necessitated the launch of the MultiShield network upgrade which occurred on December 10, 2014 at block height 400,000. The MultiShield upgrade allowed for the real-time mining difficulty adjustment of DigiByte spread across all 5x algorithms, which further ensured that block timings would remain steady. MultiShield also allows for a sudden influx and exit of hash-power on one or more mining algorithms, all in real-time, further protecting the DigiByte network.

MultiShield also renders DigiByte impervious to the plague of single-algorithm 51% attacks that rented hash power made so common during 2018, along with the timestamp vulnerability attacks that affected other multi-algorithm blockchains.

MultiShield works by increasing the difficulty for an algorithm every time it finds a block, while simultaneously decreasing the difficulty of the other algorithms, which protects against a single-algorithm takeover. Should a manufacturer of an ASIC ever be found to intentionally or inadvertently placing a back-door into their miners that would allow them to redirect the hash rate elsewhere, MultiShield would prevent that malicious hashrate from affecting the production of blocks and a double-spend occurring. Where other single-algorithm blockchains would fall victim to such an attack, or to pool collusion from 2-3 operators, MultiShield would render such an attack futile.

Even if an attacker was able to secure 90% of the hash rate on their primary attack algorithm, and 35% on the remaining 4 algorithms, they would still not have the majority of hash power and be unable to successfully attack the DigiByte network.

Rented attacks are the most common types of attacks on single-algorithm blockchains, however despite there being several SHA256 pools which have over 50% of the hash-power of the entire DigiByte network, that is still insufficient to attack against MultiShield. Should an attacker somehow gain control of all the remaining SHA256 hashpower being used by BTC in the whole world (61,000 PH/s at the time of writing), they would have 2^{10} SHA256 hashpower compared to DigiBytes 40PH/s. Attempting to attack DigiByte with that hash power would double the difficulty every 5x blocks, meaning that after approx 50 blocks (12.5 minutes) the honest miners would have outpaced such a doublespend attempt. By contrast, that same hashpower could be used to attack any other SHA256-only blockchain such as BTC, BCH, BSV repeatedly and continuously. It is for this reason that many exchanges require a mere 40 block confirmation (10 minutes) for most deposits.

Since 2018, DigiByte has constantly remained the dominant global hash-power for Qubit, Myr-Gr, and Skein by an order of magnitude, and now also with the Odocrypt algorithm.

MultiShield was the third seamless and non-contentious network upgrade that DigiByte successfully executed.

DigiSpeed

Right from the start, DigiByte had a very fast block-timing by UTXO standards at 60 seconds; however, the development team sought to further improve this, based upon the research paper “Information Propagation in the Bitcoin Network” from Microsoft Research Labs and the STEM university ETH Zurich, Switzerland. Shortly thereafter, on December 4, 2015 at block height 1,430,000, the DigiSpeed network upgrade took place. This upgrade halved the block timing from 30 to 15 seconds, becoming the fastest Proof-of-Work blockchain in existence.

The DigiSpeed upgrade also implemented a block-size doubling every two years in order to consistently increase the transaction processing capacity twofold until the year 2035. This was done in order for DigiByte to remain true to its ethos of always being forward-thinking, in order to prepare the network for growth and avoid being limited by an insufficient block size. However, the block-size doubling aspect was grandfathered as part of the SegWit upgrade, due to it's 4X weighted capacity increase, with expectations of further refinement and reimplementatation in the future.

DigiSpeed was the fourth seamless and non-contentious network upgrade that DigiByte successfully executed.

Segregated Witness

In order to further optimize its data-storage, resolve transaction malleability issues, and in keeping with the forward-thinking nature of DigiByte, Segregated Witness (SegWit) was activated in April of 2017. DigiByte was the first major blockchain to activate SegWit, weeks ahead of Litecoin and months before Bitcoin.

SegWit makes transactions smaller by segregating part of the data, which in turn increases the effective capacity of each block by around 4X. This is achieved by segregating the signatures from the transaction data. As a beneficial byproduct, SegWit also fixes transaction malleability, and subsequently paves the way for safe Atomic Swaps between DigiByte and numerous other blockchains. The N-Version Bits upgrade was also included alongside the SegWit activation.

This was the fifth seamless and non-contentious network upgrade that DigiByte successfully executed.

ReserveAlgo

DigiByte blocks had never been mined with a non-standard Script version, however the Core blockchain allowed for this at the time. The ReserveAlgo upgrade, while only a minor tweak, was a sound improvement allowing future algorithm replacements to be more seamless.

This upgrade was locked-in by consensus as of Block 8547840, Apr 15, 2019.

Odocrypt

On July 21, 2019, Block 9112320, DigiByte successfully launched its newest mining algorithm OdoCrypt. This polymorphic mining algorithm rewrites itself every 10 days in order to prevent ASIC dominance and promote the use of FPGA mining.

The benefits will be threefold:

- 1) DigiByte will be only blockchain mining this algorithm, immediately making it the dominant hash-power world-wide.
- 2) Further distribution of the blockchain by once again making mining more accessible to typical hobby-based miners.
- 3) Prevent a single ASIC vendor benefitting from a monopoly on hardware manufacturing by utilizing “off the shelf” FPGA hardware.

If DigiByte is the only blockchain with a particular mining algorithm, it means there is no hash-power to rent from 3rd-party services, further emphasizing DigiByte as the dominant chain and securing the network.

Since the hardware for Odocrypt mining is not cost-prohibitive as we have seen with expensive ASICs, this also means that home-users are further encouraged to download the blockchain through the DigiByte Core application. Odocrypt also launched with all the necessary documentation and software for users to both solo and pool-mine on their own. This prioritization of hobby mining further distributes the blockchain and adds to the security of the entire DigiByte network.

Dandelion++

As part of the DigiByte 7.17.2 protocol upgrade, DigiByte brought in Dandelion++ as the default transmission method for transactions. Dandelion is fully backwards-compatible with non-Dandelion supporting nodes, though due to the nature of the Odocrypt upgrade, all Core Wallets now support Dandelion.

Dandelion works by initially distributing the transaction to a single connected node, rather than the traditional mempool dispersion method of broadcasting it to all nodes you have a connection with. That individual node flips a virtual coin (10% chance), and will send the transaction again to another single individual node, and so forth until the transaction is eventually flowered like a Dandelion.

This protects the users privacy by effectively masking the source IP address from any snooping nodes, making it implausible for spectators to observe where a transaction began with any viable degree of certainty. Dandelion does not affect DigiBytes 15 second block timing, however transactions naturally take slightly longer to reach the mempool when using the Dandelion protocol. For this reason, transactions can have Dandelion disabled on a per-transaction basis, if the additional speed is required.

Dandelion has been activated on the Core DigiByte wallet software, as well as Android & iOS apps.

Future Upgrades

Additional Algorithm Changes

DigiByte plans to further replace one of the original mining algorithms with another GPU-specific mining algorithm, again increasing the participation from home-users and casual miners. In addition, this will further strengthen the distribution of the blockchain, encouraging users to mine using the DigiByte Core application.

There is still ongoing discussion around which algorithm should be implemented; however, the focus of this discussion is based upon which of the existing algorithms offers the least in terms of a number of things, such as:

- 1) Accessibility of mining hardware and a broad network participation;
- 2) Documentation on the mining algorithm and supporting mining-pool software;
- 3) Security offered to the network in terms of average hash power over a prior period;
- 4) Future predictions for the hash power;
- 5) Whether hash power can be rented easily;
- 6) Will DigiByte be the primary source of hash-power for the particular algorithm.

The weight given to each consideration listed above is variable and the DigiByte development team welcomes constructive input from the entire community in order to reach a well thought out and agreeable course of action.

The broader DigiByte community has universally indicated throughout 2019 that the implementation of ProgPoW for GPU-focused mining should be prioritized, followed by a further algorithm replacement, ideally with a CPU-focused algorithm.

DigiByte would ideally have a MultiAlgo setup with one algorithm for each of the following targeted hardware:

- 1) ASIC
- 2) FPGA (Odocrypt)
- 3) GPU
- 4) CPU
- 5) And a 5th yet to be decided by the DigiByte community

The precise make-up of these algorithms is still being worked through on an on-going basis.

Staking Algorithm

DigiByte continues to investigate a hybrid Proof-of-Work + Proof-of-Stake model, with the prospect of replacing one of the 5 Proof-of-Work mining algorithms with a Staking model. The benefits of which are primarily twofold:

- 1) Reward token holders simply for owning a portion of DigiByte and running a full-node;
- 2) Further reduce the possibility of double-spend attacks via Proof-of-Work.

The incentive to run a DigiByte Core full-node and keep it online to support the network is naturally admirable; however, primarily due to regulatory uncertainty combined with a lack of concrete evidence that Staking actually fortifies security, the possibility of this type of network upgrade is still under heavy scrutiny both from developers and the entire DigiByte community.

Memory Utilization Optimization

With the high number of blocks already in the DigiByte blockchain, there are limits being reached that affect the ability for a 32-bit processor to address the memory needed to run a full DigiByte node. These limits are unique to DigiByte as it paves the way for issues that will not be applicable to Bitcoin until the next century.

Although 64-bit processors have been commonplace now for well over a decade in the Desktop computer and Server market space, there are other embedded devices such as the Raspberry Pi which have remained predominantly 32-bit with 1GB of RAM. Further optimization of the memory utilization is not only beneficial for improving the longevity of 32-bit hardware and operating systems, but it also allows for systems with less RAM to smoothly operate a full DigiByte Core node.

Many desktop computers still ship with only 4GB or 8GB of RAM, and so users should be able to run the DigiByte Core software on their computer, without significant detriment. Hard drive space is easier to upgrade and more readily available, so mapping certain memory pointers on to the hard-drive will be the likely solution. It also allows for enthusiasts to rent a most cost-effective Virtual Machine, with RAM being a substantial aspect to the overall rental cost.

It is the goal of the DigiByte community to cater to as many hardware configurations as possible, as has been the case with Android app development, in order to ensure that as few people as possible get left out due to their outdated or lower end hardware.

DigiByte Platforms

Mobile Applications

In mid-2018, DigiByte launched its Android and iOS applications to the Google Play Store and the Apple App Store, respectively. These are best-in-class SPV applications that allow users to easily take their DigiByte with them, without requiring the complete download of the entire DigiByte blockchain.

The applications have focused on broad translation support for global adoption with 50+ full native languages completed so far. These applications are fully-fledged, with a unique, stylish, and highly polished interface implemented as the result of a community-run design contest.

Support for legacy versions of Android was also prioritized so the application can be accessed and installed by lower-cost hardware that is prevalent in developing and impoverished nations. This allows for global reach, with users able to operate the application in their native language. DigiByte mobile applications continue to be developed, with additional technologies being added in, such as Digi-ID.

Digi-ID



Digi-ID is a fast and secure authentication method that can be used to replace standard usernames, passwords, two-factor timed one-time passwords, building swipe-cards, and more. Authentication with Digi-ID is designed to overcome many of the pitfalls and vulnerabilities with traditional security methods. This includes things such as SIM-swapping, rendering SMS authentication insecure, or phishing for rolling TOTP codes.

Digi-ID can also be used for non-traditional authentication, such as games, phone/PC applications or building security. Digi-ID also does away with the need for multiple “accounts” as your Digi-ID is simply authorized access to a different aspect of a website, building, product or platform. Rather than requiring a user to utilize a unique login for personal use, and another for company dealings, the users single Digi-ID can be utilized.

Digi-ID is anonymous, with no information being stored or transmitted via the blockchain. There is also no personally identifiable information kept inside of the DigiByte mobile applications, nor any form of data-logging. This allows for easy compliance with GDPR regulations.

Digi-ID has already been implemented into the Coinomi application suite, and there are a number of additional “authenticator” applications available. This implementation into additional wallets further lowers the barriers-to-entry for new users, and a broader audience penetration with existing software.

Using Digi-ID as a basis for their authentication technology, the likes of AntumID have already created a variety of identification protocols built on top of the Digi-ID protocol, some with identity verification, as well as ground-breaking deterministic password-replacement technologies (DigiPassword).

DigiAssets

DigiByte is bringing the ability to launch “Digital Assets” on the blockchain with the DigiAssets platform. These assets can be both fungible or non-fungible tokens, credits, shares, event tickets, coins, trading cards, property deeds or titles, travel tickets, and more.

Issuance of DigiAssets can take place both in a computer web-browser as well as development focus around extended issuance capabilities from the Android & iOS applications.

Mobile issuance coupled with the vast translation focus of DigiByte brings DigiAssets to a truly global audience across a variety of markets, both first-world, developing, and impoverished nations. Users worldwide can create a DigiAsset from their mobile phone, backed by the security and on-chain scalability of the DigiByte blockchain. DigiAssets are verified on the DigiByte blockchain, making them immutable, unforgeable, and making supply and ownership transparent. These DigiAssets can then easily be traded, sent, or received by users around the globe.

DigiAssets have the standard capabilities expected by users, such as the ability to further burn asset supply, and adding additional metadata to assets in the form of key + value pairs. With DigiByte’s on-chain scalability, proven battle-hardened security, and enviable decentralization, DigiAssets is the perfect platform for launching any type of digital asset.

Closing Summary

DigiByte is one of the few forward-thinking blockchains that is not merely limited to being used as just a digital currency (despite the fact that DigiByte truly excels in this area over and above every other Proof of Work blockchain), but rather as a multifunctional and highly purposed blockchain. This was one of the many reasons why the founder, Jared Tate, named the project DigiByte as opposed to including “coin” in the name as many other projects have.

DigiByte as a project and community are not content with the status quo, in any way. They are always pushing forwards, working to improve the project and also the world we live in.

DigiByte is committed to being an industry-leading project that can easily say it is faster, more secure, and more decentralized than any other Proof-of-Work blockchain project. This comes as a result of being MultiAlgo, with MultiShield security, combined with the drive from the users and community to always grow and perform better.

Through more than six years of active development and pushing the boundaries of a UTXO blockchain, DigiByte has not only a proven track-record of rapid and secure transactions, but also an incredibly bright and promising future through its ever-developing use-cases and of course, its dedicated and driven community of volunteers.

