DMD DIAMOND

Cooperative consensus vs. Competitive consensus

The first blockchain to implement a cooperative consensus with a delegated PoS-powered validator election

White paper

Abstract: Founded in 2013, DMD Diamond is constantly evolving and upgrading to new market conditions. This document describes the latest DMD Diamond blockchain upgrade — DMD v4 — that combines the best of both Bitcoin, Ethereum, and beyond. Including real decentralization, on-chain governance, fast transaction times, low fees, low carbon footprint, security, interoperability, and smart contracts deployment, DMD v4 has become the first blockchain to implement a sustainable and endless reward mechanic with a low max finite supply of just 4.38 million coins.

This Document is not a Prospectus

This document does not constitute nor imply a prospectus of any sort. No wording contained herein should be construed as a solicitation for investment. Accordingly, this whitepaper does not pertain in any way to an offering of securities in any jurisdiction worldwide whatsoever. Rather, this whitepaper constitutes a technical description of the functionality of the DMD Diamond Blockchain.

Table of Contents

Table of Contents

1. Executive Summary

2. Background
    2.1 Industry challenges
    2.2 The DMD Diamond History
    2.3 The HoneyBadger BFT Consensus Algorithm

3. DMD Diamond Solution
    3.1 Mission
    3.2 Features and Benefits
    3.2 Interoperability and Migration for DApps
    3.3 Smart Contract Support
    3.4 Secure Consensus
    3.5 Network Participants
        3.5.1 Coin Holders & Wallets
        3.5.2 Validators
    3.6 Governance
        3.6.1 Proposal cycles
        3.6.2 DAO Voting Change Decision by Validator

4. Technology
    4.1. The Components of DMD Diamond v4 Blockchain
    4.2 Node Selection through POSDAO
    4.3 Consensus Mechanism
        4.3.1 Lightweight Consensus Mechanism
        4.3.2 Honey Badger BFT Protocol
            4.3.2.1 The HBBFT Main Features
            4.3.2.2. HBBFT Features to Guard Against Attacks
            4.3.2.4 Instant Block Finality
            4.3.2.5. Block validation
    4.4. Nodes and Network Participants

5. DMD Coin Economy
    5.1. DMD Coin Features
    5.2. Issuance of Tokens
    5.3. Network initiation
    5.4. Migration from DMDv3 to DMDv4
    5.5. Solving the Lost Coins Problem (Previously Treasure Digging)
    5.6. Use of Funds

6. Roadmap

7. Team

1. Executive Summary

"Combining the best of Bitcoin, Ethereum, and beyond
to ensure the long-term viability of the DMD Diamond blockchain."

Being one of the oldest projects on the cryptocurrency market, DMD Diamond has undergone several significant changes in its architecture as a response to the constantly changing and evolving technology and market conditions. This document describes the latest upgrade of the DMD Diamond v4 blockchain, designed to solve the greatest industry challenges through combining the best of Ethereum, Bitcoin, and other worlds.

DMD Diamond v4 is an independent blockchain with full-stack integration of application, networking, governance, and consensus layers for building, deploying, and running general-purpose and interoperable decentralized applications in a fast and low-cost manner. By utilizing a mix of Honey Badger Byzantine Fault Tolerance consensus algorithm (HBBFT) and the delegated Proof-of-Stake based validator election (POSDAO) protocols, DMD Diamond v4 has become the first blockchain to implement cooperative consensus with a low carbon footprint, fast transaction times (approx. 400 tx/s (transactions per second))[1] and low fees.

The DMD coin — one of the oldest cryptocurrencies on the market — maintains its original fixed-issuance coin emission model and remains five times more scarce than Bitcoin with a finite supply of just 4.38 million coins. DMD is one of a very small number of coins, including Bitcoin, Litecoin, and Peercoin, that have survived from the inception (2013) to now and that are still actively supported and traded.

DMDv4 is also the first blockchain that implements sustainable endless coin rewards for consensus nodes and dPOS stakers while maintaining a coin maximum by utilizing a new mechanism that reinserts unclaimed and abandoned coins into circulation after a number of years. This mechanism is designed for the long-term limitless growth of the networks and prevents a possible imbalance within scarce-supply coin ecosystems. (More Details in section 5 and 5.5)

Moving with the progress of the industry, the DMD Diamond team has implemented changes that allow interoperability between DMD and other blockchains, using an addressing structure and smart contract engine that allows interoperability and cross-chain movement of values and messages. The "coin wars" are over and it is an industry-wide imperative to create stability and interoperability among the coin and token holders across the cryptocurrency industry. For that reason, DMD is creating strong interoperability capabilities with other Ethereum-based projects (Open Ethereum, POA Networks, xDAI, Artis.eco, lab10.coop, etc.).

The DMDv4 coin development represents the first step towards a DAO (Decentralized Autonomous Organization)[2] as the change is based on a vote taken among the DMDv3 holders, creating a democratic process. DMDv4 is a newly developed chain that will replace DMDv3 and that includes the capacity to add on-chain governance mechanisms that will be deployed in versions 4.1 and beyond.

[1] We expect that even more is possible which is to be checked during the alpha tests so the White Paper will be updated after new performance tests.
[2] https://www.investopedia.com/tech/what-dao/

2. Background

2.1 Industry challenges

The cryptocurrency industry has delivered on its promises of the store of value and privacy of digital assets. However, the technology has also faced a number of issues that all modern blockchains have to address. The following are the challenges that are most critical to address in the industry today.

- Proof-of-Work is not adequate for fast and low-cost transactions.
- Current transaction times take minutes and in the worst case, hours. For real-time purchases, this is simply inadequate for a viable system.
- Security issues are major concerns in the industry. In 2019 there were 94 cryptocurrency hacks, according to Cointelegraph[3].
- New developments have been made in BFT (Byzantine Fault Tolerance)[4] and other security solutions.
- Blockchains that want to provide themselves and the hosted projects with highly customizable on-chain logics need to support smart contracts.
- Big coin holders are often not involved as guardians of the network and are not incentivized to act as such.
- On-chain governance is aligning the values of participants in the networks.
- Many blockchain systems miss a true sustainable coin economic setup ready for centuries. A truly sustainable ecosystem needs to be built around a limited resource developed in a way that the resource can be “recycled” or is “renewable” (e.g. grows new at the same speed as it’s used up).
- Competitive consensus blockchains have limitations on minimum block times and instant finality of transactions.
- Interoperability is becoming important as the industry matures and consolidates around a shared mission to create financial inclusion worldwide.

The DMD Diamond team has always been committed to maintaining the best technology and ensuring that the coin holders are protected and that the DMD chain gains momentum and utility in the industry. As such, the current implementation addresses these opportunities and challenges.

[3] https://cointelegraph.com/news/report-blockchain-related-hacks-have-declined-in-2020
[4] https://en.wikipedia.org/wiki/Byzantine_fault

2.2 The DMD Diamond History

The DMD Diamond coin was created in mid-2013 during an explosion of new coin creation, based on forks of Bitcoin. DMD launched as a limited-supply Proof-of-Work (PoW) and Proof-of-Stake (PoS) coin, which already represented an advantage over the competition, but at the time the code for staking wasn't mature. Despite the initial enthusiasm for the coin, the original creator of DMD disappeared several months after the creation of the coin, which theoretically could have ended badly with the community being disgruntled by the sudden departure of the developer leaving unresolved software issues behind.

Instead, a small community convened, discussing the future and the potential on the Bitcointalk forum. The name of the coin appealed to people, as well as the implicit scarcity and the fairness of the limited coin issue. As a result, a small team of developers and enthusiasts got together to maintain and evolve the code and adjust the vision for the coin, and in April 2014, with the release of DMDv2, the coin's staking algorithm was made stable and worthwhile for network participants.

The survival of the coin and the willingness of a community of enthusiasts to continue to support this project made DMD stand out from other coins. Such disappearances and pump-and-dump schemes were common — the difference was that the community rallied around the coin and continued to uphold the value of the coin. At that time, smart contracts were not yet available — however, there was an ideological underpinning to the release of currency that was supported by regular people seeking financial independence and security from the authorities and debt-backed government money systems.

Sprouting from the community was a group of leaders and developers who were determined to create a sustainable blockchain, stewarded by people who are willing to continue to take responsibility for the project over the long haul, without compromise. The team of stewards of DMD Diamond was determined to create a store of value that they themselves felt comfortable holding. The name Diamond represents scarcity, unshakable strength, and value.

With hard work and a dedicated community, DMD Diamond remained in the top 100 coins on Coinmarketcap throughout boom and bust cycles until only recently. Naturally, the technology was superior to Bitcoin because of the later development and the vision has continued to attract a group of faithful holders who recognize the scarcity of the coin and the integrity of the team as essential for the long-term health of the project.

The strength of DMD Diamond is not only its vision and principles but the devotion to constant evolution. Technology evolves quickly, but most blockchains are designed in ways that are doomed to be stuck with their initial technological decisions, constraining them in ways that prevent adaptation. DMD is sometimes called the Phoenix of Crypto, because the ability to upgrade (reincarnate like the legendary Phoenix) is part of the project vision, as illustrated with the current technological advances of DMDv4.

DMDv1 combined the best from Bitcoin, Litecoin, Novacoin, Luckycoin, and Florincoin, a mix of industry-first blockchain solutions with Proof-of-Work/Proof-of-Stake algorithms for network security. DMDv2, which was based on Mintcoin, repaired the PoS algorithm, and redefined the coin rollout from static rewards with a short emission period of eight years to a

schema with decades-long, constantly decreasing inflation. At the time, eight years seemed like a long time in the industry as a whole, but we recognized that such a trajectory was short-sighted. Therefore, DMDv3 continued following the network reward reduction curve in an improved, smoother, more natural way. DMDv4 is being built with additional sustainability mechanisms and lost coin retrieval for even longer-term trajectories.

With the outbreak of organized ASIC attacks on PoW networks, DMD abandoned the previously used Scrypt algorithm, which was also used in Litecoin. At that time the first specialized hardware was developed that made GPU mining senseless, and DMD switched to Groestl, which was ASIC resistant at that time. This was a revolutionary feat: the world's first successful algorithm change that preserved existing legacy blockchain. It allowed the coin holders to retain their balances and history of past transactions, without the need to take any additional steps. It also allowed ordinary people to keep mining and participating in a fair and wide distribution of coins.

When Masternode technology emerged as a potential platform for bringing Diamond closer to its goals by improving both functionality and utility value of the coin, DMDv3 moved to a third-generation PoS protocol, to mitigate some of the security shortcomings of previous PoS algorithms. The requirement to participate proactively in network security resulted in Diamond blockchain's becoming healthier and more robust.

However, the promise of Masternodes did not pan out as we hoped for: it maintained the same limited set of services including coin mixing, reduced minimum confirmations, and voting over proposals, whereas DMD was aimed at evolving into a blockchain for hosting multiple services and projects. Thus, since 2016, the team has been researching alternatives to decrease transaction times and maximize throughput while reducing the environmental damage potential of the blockchain. Now with version DMDv4, we are realizing the vision of a cooperative consensus (HBBFT Honeybadger) blockchain combined with a dPOS node election decentralization mechanic (POSDAO). This allows us to reach rapid throughput thanks to the advances in asynchronous consensus protocols and the inclusion of smart contract capabilities combined with a high degree of compatibility with the Ethereum ecosystem which creates fertile ground for business creation.

Table 1: The Evolution of DMD Diamond

DMD Diamond v1	● Blockchain codebase – (*Bitcoin) ● Hybrid PoW/PoS – (*Peercoin) ● Scrypt mining algorithm – (*Litecoin) ● Random superblocks – (*Luckycoin) ● Transaction messages – (*Florincoin)
DMD Diamond v2	● Fixed PoS issues – (*Mintcoin). ● Changed mining algorithm to Groestl (*Groestlcoin). ● Removed superblocks for security concerns. ● Changed coin economic setup from an 8-year to a 40+ year timeframe.
DMD Diamond v3	● Changed from PoW/PoS to PoS/Masternode technology – (*DASH,*PIVX). ● Removed transaction messages.
DMD Diamond v4	● Changed blockchain codebase from Bitcoin to Ethereum (*Open Ethereum). ● Added HoneyBadger BFT consensus (an industry first mainnet implementation in Ethereum codebase family (*POA Network,*original HBBFT research paper https://eprint.iacr.org/2016/199.pdf)). ● Added POSDAO validator election contracts. (*xDAI, *LUKSO) ● Expanded coin economic system into a sustainable infinite timeframe one that reinserts abandoned/unclaimed coins and fees (an industry first). ● Removed masternodes.

* As true believers of open source we credit the projects our implementations are based on with more or less adaptation and adjustment by our own team towards the needs of the DMD Diamond project.

DMD Diamond has always been known for its reputable team and constant development, as well as the scarcity of the coin and the fierce loyalty of the coin holders. The move to on-chain governance will finally set in motion the formal mechanisms that ensure that the community truly owns the network and that DMD Diamond can continue to be reliable and future proof.

This upgrade provides the value that was promised at the very beginning of the crypto craze — a trusted coin that has long term viability and isn't just a trading scheme that will need to be replaced in the future. By building in its own governance and the capabilities for upgrading itself, DMD stands out as a crypto project that takes a forward-thinking approach to robustness and trust and follows the old-school logic of no ICO and no pre-mine, just a purely open, decentralized, fully-featured blockchain.

2.3 The HoneyBadger BFT Consensus Algorithm

To meet the market demands of speed and security, the DMD team has analyzed different consensus algorithms available today including one of the most promising developments, the Honey Badger Byzantine Fault Tolerant consensus algorithm.

The Honey Badger Byzantine Fault Tolerant (HBBFT) consensus algorithm[5] was developed in 2016 by Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song specifically to address the issues of slow transaction times and the difficulties of having synchronous communication on a large global network. After extensive research, the DMD Diamond team has determined that using HBBFT will dramatically increase the efficiency and improve the security of the DMD blockchain.

Advantages of moving to the HBBFT include:

- Improved security for Byzantine Fault Tolerance.
- Immediate transaction approval, with no need to wait for synchronous approval.
- A dramatic increase in transactions per second, at least 400 TPS.
- Increasing popularity with implementations in the Helium blockchain[6] and xDAI (upcoming)[7] Artis.eco (upcoming).
- Increased robustness of the blockchain.
- Elimination of the ability to fork the protocol and elimination of the problem of orphan blocks in the chain.
- Identification and elimination of malicious nodes.
- Ability to implement dynamic block times.

A more detailed discussion, including references to additional reading, is described in *the Honey Badger BFT Protocol section*.

[5] https://eprint.iacr.org/2016/199.pdf
[6] https://developer.helium.com/blockchain/consensus-protocol
[7] https://www.xdaichain.com/for-validators/consensus/honeybadger-bft-consensus

3. DMD Diamond Solution

3.1 Mission

The fourth iteration of DMD Diamond is a cornerstone of a store-of-value monetary system that is not government-issued or controlled. Our mission is to enable people to achieve financial freedom and independence, by creating a platform that provides a safe, affordable, and rewarding smart contract powered blockchain economy.

Our vision is to contribute to the blockchain ecology through the development of Open Source protocols, utilities, and services, forwarding the interoperability of blockchains, thus increasing the viability of the entire cryptoverse.

3.2 Features and Benefits

To address the industry challenges, the DMD Diamond team presents version 4 of its blockchain. DMDv4 is the first cooperative consensus blockchain with a delegated PoS-powered validator election which allows for high speed and performance, absolute censorship resistance and fork resistance, instant finality of transactions, and other advantages that cannot be delivered by a competitive consensus.

Table 2: Cooperative consensus vs. competitive consensus

DMDv4 *(underlined text is what DMD v4 uses)*	**Cooperative consensus**	**Competitive consensus**		
	HBBFT	**PoW**	**PoS**	**dPoS**
Energy wasted	Minimal	Country-size	Village-size	Minimal
Fork resistance	No forks possible	Medium resistance, reorgs needed		
Finality of transactions	Each block is final	After many blocks		
Censorship resistance	Absolute via threshold encryption	Good once in a block, but can require multiple tries as the block producer can censor the block content		
Random number generation	Random and protected via threshold encryption	Exploitable: the block producer can decide not to generate a block if he doesn't like the random part		
Decentralization	*Low with a static set of validators	Medium because of big mining pools	Very good	*Medium, some nodes are temporary elevated via votings/stake/random elements to create blocks
Dynamic block times	Yes, allows the next block creation to start after 1 sec.	Not possible because competitive consensus needs static block times (at least 15 sec, whereas most systems need way higher: 1 – 10 minutes).		
Performance	High with small set of active nodes and dynamic block times	Low. As competing / forking blocks are possible, higher block times needed to avoid constant forks.		

** To increase the decentralization of HBBFT we did choose to expand it with a dPoS based node election mechanics powered by POSDAO.*

The DMD v4 blockchain adds the smart contract functionality and sets out to align with the industry as it is: the coin wars are over and blockchain interoperability is important for the entire industry. Therefore, DMDv4 is compatible with Ethereum EVM smart contracts, making it simple to port smart contracts written for Ethereum towards DMD Diamond v4.

Diamond is also designed so that it can be a participant in future blockchain-based ecosystems that utilize bridges and other cross-chain value transaction methods. The aim is to provide every participant with maximal freedom to host projects on the platforms that best apply to their needs. The DMD blockchain answers many of those needs, and other blockchains are part of answering specific needs for other developers and participants.

To sum it up, The list of DMD Diamond v4 features includes the following important capabilities:

- Limited issue of tokens, with a low cap of 4.38 million tokens, with full issuance of all tokens at genesis block, with no ability to mine any additional tokens or dilute the existing amount of coins in any way.
- Smart contract capabilities with Turing-complete programming language.
- Instant finality of all transactions using the Honey Badger BFT protocol.
- Fast throughput: predictions and testing demonstrate a minimum of 400 TPS.
- Rotating validation nodes, and maximum validation node staking allows for a randomized distribution of power among validators for 12 hours (Epoch), no concentration of power, and fair rotating.
- Censorship-resistant, utilizing threshold encryption. Single nodes cannot act maliciously against particular transactions because they cannot see the contents of the transaction until it is validated.
- DMD staking happens with a limited set of validator nodes, and a maximum amount staked on top of these nodes because of DMD's scarce supply.
- Interoperability and full compatibility with other blockchains: Code written for Ethereum EVM will run on the DMD v4 blockchain enabling easy migration between chains.
- Fork-proof, with 2/3 majority required, and no opportunity for a dispute of the chain.
- No orphan blocks resulted from simultaneously created competing blocks are possible on the chain, because of its cooperative protocol with fractional transactions contributed by active validators threshold encrypted to the block.
- On-chain governance support with upgrade 4.1.
- Random number generation capabilities built-in.
- No wasted network capacity. If there are no transactions, no empty blocks are created as with other blockchains. DMD may include a very small heartbeat block if for periods of time of more than 10 minutes there are no transactions.
- Recovery of lost coins through a fair aging mechanism that identifies abandoned coins in POSDAO after a number of years.
- Sustainable long-term coin and ecosystem maintenance and issuance.

3.2 Interoperability and Migration for DApps

DMD Diamond has taken the approach that cooperation and interoperability across chains is a must for the sustainable and long-term development of the crypto industry.

For that reason, the DMDv4 is being created as a system that is fully compatible with Ethereum, using Open Ethereum addressing systems and foundations, and running EVM apps according to the protocol standards. The result is that dApps can be easily migrated across chains.

Open Ethereum Client (formerly Parity) is included as part of the package for DMDv4. This is the most well-known and fastest Ethereum client and is robust and well-proven in the industry.

Interoperability Bridges provide connectors to other chains, allowing the transfer of value across coins and other blockchains. DMDv4 allows easy integration by using third-party Layer 2 interoperability solutions that support DeFi apps and other apps that integrate smart contract functionality with multiple different crypto assets. Connectors allow access to games, NFT, DeFi, and other types of dApps across chains.

Other solutions can interact with or run on DMD in the future. For example via TokenBridge[8] Arbitrary Message Bridge (AMB) — a bridge designed for universal cross-chain data transfer — that could potentially allow integration with other chains in the future. The idea behind these bridges is to allow smart contracts from one blockchain to understand and interpret smart contracts from other chains so that they can work together on different types of dApps or communicate across dApps.

Such solutions allow for migration of fee intense parts or whole DeFi protocols, or decentralized exchanges, or similar projects to run partly or as a whole on DMD Diamond blockchain and still able to move assets back to other chains, for example, Ethereum.

3.3 Smart Contract Support

DMDv4 will include smart contract support based on EVM so that existing smart contracts developed on other chains can run on DMD. DMDv4 supports Solidity and the other languages that are supported by the Ethereum blockchain.

Because of the much faster transaction times, lower fees, the ability to run the same code on multiple chains, and easy smart contract migration back and forth, DMD represents an appealing alternative to Ethereum. DMD Diamond is a long-running blockchain with a highly distributed community of holders, meaning that it is a very secure and stable network, so application developers can feel comfortable with using DMD as a fast-throughput alternative to Ethereum.

3.4 Secure Consensus

DMDv4 is a decentralized multipurpose blockchain with a highly secure and distributed consensus algorithm and a distributed system for rewarding the nodes that secure the

[8] https://docs.tokenbridge.net/

system. Diamond has an old community with many coin holders and uses delegated Proof-of-Stake so that every coin holder can be part of the validation mechanism and cast their weight to the validators that are acting in good faith on the system.

The DMD network allows any full node with 10,000 DMD to become a validator candidate, and for any coin holder with at least 100 DMD to stake their coins on validator candidate nodes. In this way, coin holders can signal the nodes they trust most to be reliable/stable and increase by adding coin weight on them the chance to get selected to be part of the active validator set more often. The maximum DMD per node is 50,000 DMD, either held by the node or staked by DMD coin holders. Up to 438 nodes are possible, based on the amount of DMD in circulation.

Validation rotates among the validation candidates, with 25 being picked randomly every 12 hours, called Epoch. During the Epoch, the validator nodes use the Honey Badger Byzantine Fault Tolerance consensus protocol to validate transactions, and Epoch rewards are distributed equally among nodes. The distribution algorithm is weighted such that every node will get chosen to be in the Validator Set in proportion to the amount of staking on the node. To find more information about validation, read the *Node Selection through POSDAO* section.

This system is designed such that:

- Validator Candidate Full nodes secure the system: 438 maximum, 50 – 75 expected.
- A highly distributed system where a random subset selection of 25 active validators is made every 12 hours via POSDAO dPOS mechanic, so all validators candidates have a chance to get a turn twice a day. Note that if there are fewer than 25 candidates, the system can function with fewer validators too.
- Coin holders can stake their coins on the nodes, showing support for the best candidates, which weights the choice and ensures that validator nodes that are more reliable are chosen more frequently.
- Epoch rewards get split equally at the end of the Epoch between all active validators. Each validator then split his share proportionally between the coin owners who staked upon this validator. Misbehaving validators get no rewards at all, their coins get locked and they cannot become a part of the active set during a few Epochs.
- HBBFT consensus algorithm allows fast/instant final transactions, high transaction throughput, and increased security of the system via threshold encryption.

The details of the network are described in the *Network Participants* and the *Nodes and Network participants sections*.

3.5 Network Participants

3.5.1 Coin Holders & Wallets

Any coin holder on the DMD network can stake their tokens on validators to earn Epoch rewards and to vote when governance decisions become available in versions DMDv4.1 and

onward. The staking will be available from a web-based dApp accessible for anyone with a wallet that supports a custom Ethereum style network and WalletConnect[9], such as Minerva[10], Metamask[11], or MyEtherWallet[12]. Anyone with DMDv3 must upgrade to a new wallet and claim DMDv4 as described in *the Migration from DMDv3 to DMDv4 section*, and then they can easily participate in the securing and governance of the network.

3.5.2 Validators

DMD Diamond v4 utilizes validators for the transactions, as per the HBBFT protocol. Each elected (active) validator receives an equal share of Epoch rewards for cooperative contributing to block creation and validating the transactions and compute smart contract executions on the DMD blockchain in a defined timeframe (one Epoch), each active validator shares the rewards among themselves and their delegates. The validation process has been described in detail in the *Secure Consensus* section.

Block rewards for active validators and delegates on them are split proportionally according to the number of coins staked for that validator. However, the minimum to the validator will be 30% of the block reward. If the validator's share of the staked coins is less than 30%, the validator gets 30% and the rest 70% is distributed among the coin holders proportionally according to their stakes.

Validator candidates require:

- Full node installation of the DMDv4 chain on a Linux server with the DMD version of Open Ethereum which include the DMDv4 extensions including HBBFT/POSDAO and the proper configuration
- Internet with Static IP address and a reliable 24/7 uptime.
- Minimum collateral of 10,000 DMD (from validator candidate owner), maximum 50,000 DMD can be staked on one validator candidate (combined from the owner and others who stake on top of his node).
- Link to address of the node that delivers the work.
- The validator candidate registration and collateral locking through the POSDAO dApp.

Note that the node address is not the same as the address where the coins are coming from. Validator candidates re-stake the coins they earn as rewards. Validator candidates and dPOS stakers on top of them can adjust (deposit or withdraw) staked coins anytime (inside the allowed range) and the change (transaction of coins) happens at the next Epoch (12 hours).

POSDAO whitepaper refers to validators and all dPOS staker on top of him as a mining pool. DMD Diamond prefers the terminology validator candidate because no mining is conducted in the DMD network and the word mining is misleading.

[9] https://walletconnect.org
[10] https://lab10.coop/projects/minerva-digital-wallets/
[11] https://metamask.io
[12] https://www.myetherwallet.com

Find more details on how POSDAO works and how validators are selected in the Node Selection through POSDAO section.

3.6 Governance

The DAO Governance module is a weighted voting module that allows validators to vote for system changes, upgrades, and other proposals and optionally approve requested funding from the DMD DAO governance funding pot.

Important: *DAO Governance and POSDAO are different things. DAO Governance is a manual smart contract powering the decision-making tool to vote over proposals, POSDAO is an automated smart contract to support a fair and decentral election of active validators. POSDAO is an essential part of Mainnet launch 4.0; DAO governance is part of the first planned big upgrade 4.1.*

Only validator candidates registered on the permissionless network can vote in the DAO, but coin holders can stake their DMD token with any validator candidate they choose and change their affiliation at any time, with the change taking place when the Epoch changes. To stake, coin holders use a web interface or the interface of a compatible wallet that can connect to a customized Ethereum-like network and interact with dApps via WalletConnect. All voting and staking take place without the need for the full node. The validator votes on behalf of all coins that are delegated to the validator. This way, distributed governance is enabled through delegated Proof-of-Stake.

All proposals and voting are public and transparent. This is important so that participants can delegate their stake to the validators that are voting aligned with their interests.

3.6.1 Proposal cycles

The proposals submitted to the DAO will be discussed ongoingly and any community member can participate in the discussion. There will be a fee associated with submitting a proposal for a vote to avoid malicious attempts to disrupt the process with spam requests. Proposals of any type can be accepted: code changes, requests for funding, or any type of written proposals to the community. On a regular monthly basis, the validator candidates will take a vote on the open proposals and funds will be allocated from the DAO pool accordingly. The monthly cycle will allow 2 weeks of deliberation and feedback and 2 weeks for voting.

3.6.2 DAO Voting Change Decision by Validator

Validators are able to change their decision. Delegates should monitor their validator voting behavior and to switch to a validator that doesn't change his opinion at the last minute. We encourage validators to make decisions early and stick with them, in order to attract further delegates who search for predictable voting results. Validators are encouraged to vote early in order to display their opinion by voting for an option in a proposal. Delegates are encouraged to stake their funds on active validators that vote according to their preference.

It is possible to change a vote during the 14-day voting period and the change will be transparent — so validators are encouraged to explain why they change the vote to provide that those who staked should have a chance to either agree or move their stake to another

validator. Delegates whose validators are inconsistent in their voting behavior are likely to switch to another validator.

4. Technology

4.1. The Components of DMD Diamond v4 Blockchain

The DMDv4 is based on an Open Ethereum node client software with EVM abilities customized by the DMD team. The team has added the ability to support the implementation of the Honey Badger Byzantine Fault Tolerant consensus protocol combined with the implementation of a POSDAO, a dPOS-like mechanic to choose the active validator nodes that create a higher level of decentralization than fixed consensus node protocols. The repository for DMD can be found on GitHub[13].

Diamond DMDv4 uses a suite of technologies that integrate the latest proven technologies, allowing for fast transaction times, full smart contract support, and on-chain governance. In this version of DMD, coin holders can take part in the governance and staking mechanisms without running a full node as described in the *Network Participants section*.

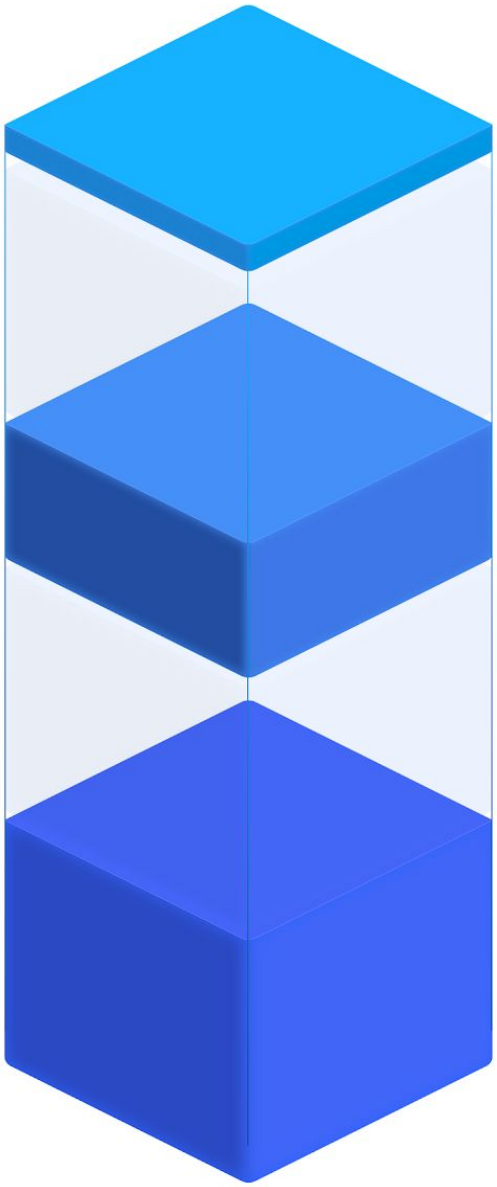
The components of the DMD blockchain include:

- Ethereum Virtual Machine (EVM) based on Open Ethereum is responsible for executing the smart contracts. See the Bytecode article for more information about the EVM[14].
- A smart contract language code used by programmers is used to create smart contracts. DMDv4 is a Turing-complete solution that allows the development of any kind of dApp that can be supported on the blockchain. The DMDv4 supports Solidity and the other languages that are supported by the Ethereum blockchain.
- Node selection, in this case, is based on POSDAO for the selection of nodes for validation in HBBFT. The core code is a set of smart contracts that determines the default functionality of the DMDv4 blockchain. The POSDAO is what makes the blockchain work true decentral by random rotation of power, staking upon different validators and distributing rewards between the active participants, both stakers and validators.
- When the DAO Governance structure is implemented, POSDAO supports it via providing the voters' weight (total staked coins on a validator candidate) which allows the coin holders to vote for (and potentially have automated implementation of) changes such as block gas limit and minimum gas fees and similar changes in the network.
- The consensus mechanism, in this case, the Honey Badger Byzantine Fault Tolerant (HBBFT) protocol, determines the transaction validation rules. HBBFT is used in combination with a POSDAO election of nodes for distributed and secure transaction validation.

[13] https://github.com/DMDcoin

[14]https://www.bitrates.com/guides/ethereum/what-is-the-unstoppable-world-computer#:~:text=The%20Ethereum%20Virtual%20Machine%20(EVM,then%20compiled%20to%20EVM%20bytecode

- Open Ethereum full nodes serve as nodes responsible for creating transactions, writing data to the chain, executing contracts, and communicating with other nodes on the network.
- Compatibility with Browser or APP clients which manage user keys to interact with the blockchain and may provide additional blockchain-based services including swapping, NFT mechanics, self-sovereign identity, etc. These clients with WalletConnect ability allow the interaction with the POSDAO smart contract and its graphical user interface dApp.



Node software layer

(running on each full node)

- Based on Open Ethereum
- Adapted by DMD Diamond to utilize the HBBFT library
- Allows for DMD specific interactions with the contract layer

EVM contract layer

(DMD on-chain contracts)

- HBBFT POSDAO contracts adapted by DMD for the platform needs and specifications
- Claiming contracts
- DAO governance contracts (planned for DMD release 4.1)

dApp layer

(decentral software that interacts with blockchain and contracts)

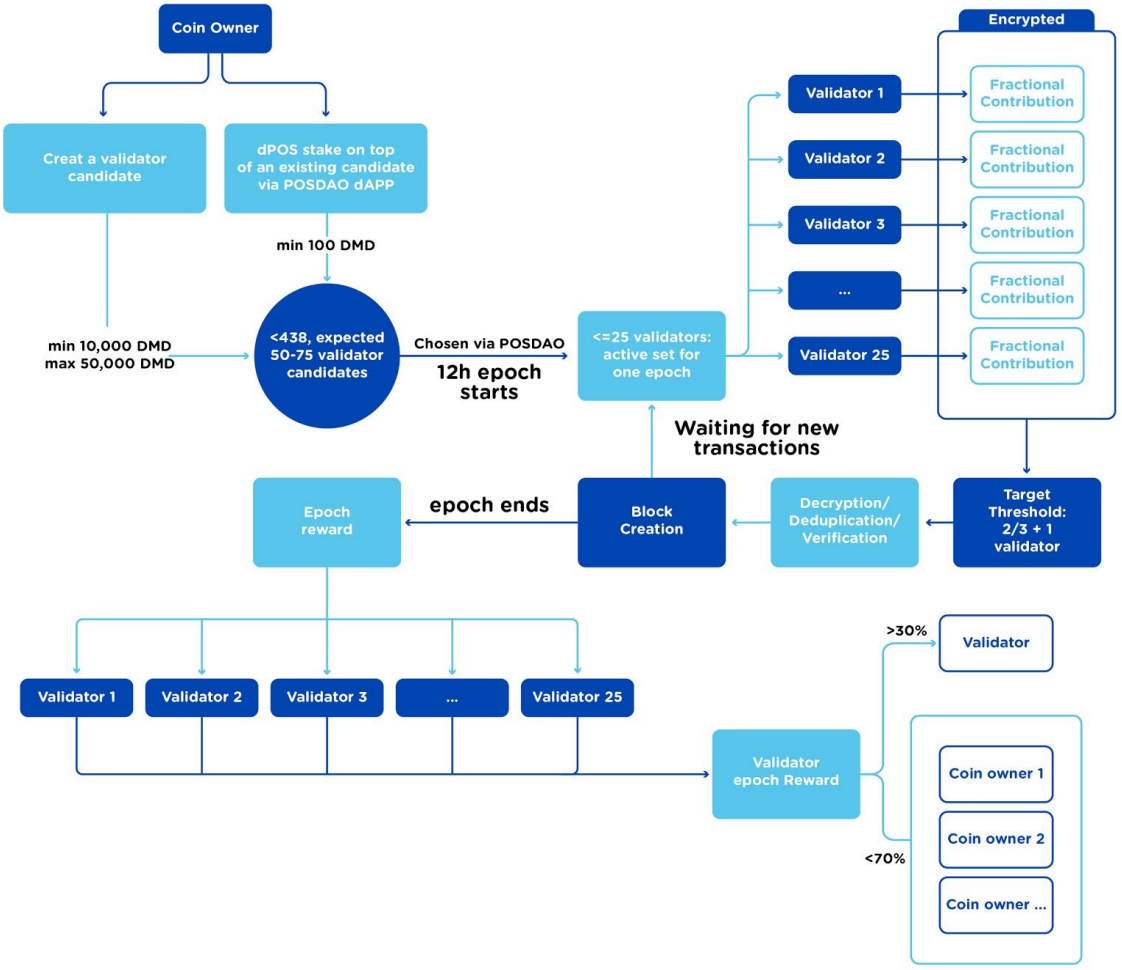
- Claiming dApp
- POSDAO staking dApp
- Key management and blockchain interaction dApps (also known as wallets)

4.2 Node Selection through POSDAO

The Proof-of-Stake Decentralized Autonomous Organization (POSDAO) algorithm is designed to create a decentralized consensus for public blockchains, based on a voting mechanism to elect the active nodes (validators) that participate in block creation. POSDAO provides a leaderless structure that incentivizes validators to act in the best interests of the network.

The following picture shows the leaderless block authoring architecture, with POSDAO selecting the validators, and then the validators approving the transactions and receiving the Epoch rewards.

Pic.1: Staking, Validation, and Rewards in DMD Diamond v4



DMD uses HBBFT as a cooperative consensus algorithm to overcome the issues of slow transaction time and limitations of competitive consensus protocols, but HBBFT requires a low maximum of 25 validator nodes (in the DMD implementation) to take advantage of these improvements. However, the permanent distribution of power in a network of 25 static nodes is not adequate. To solve this, DMD uses a POSDAO implementation in order to select the nodes that will act as active validators every Epoch that runs 12 hours. By electing a new subset from the candidate nodes every Epoch, POSDAO allows for the distribution over any number of validator candidates, both maintaining the speed of the network and creating a

fairly distributed mechanism of securing the system and earning rewards. Note that chances of being selected are increased for nodes that are most trusted, represented by the number of coins staked on top of them.

In DMD, a cap of 438 validator candidates possible because of the scarcity of the DMD coins. These caps contribute to the fairness and the speed of the network. Based on the current network activity, Diamond DMD expects approximately 50 – 75 active validator candidates competing for the active Epoch set.

A maximum staking ceiling of 50,000 DMD ensures that there is no possibility to buy one's way in or collude to become more powerful than other validators on the network. The maximum staking amount also makes sure that even candidates with a minimum stake of 10,000 DMD have a chance to get into the active set and POSDAO dPOS stakers can increase that chance by supporting smaller candidates via staking on them.

POSDAO is a highly secure mechanism with protections against breaches, outlined in detail in the POSDAO whitepaper[15]. Participants stake coins to protect the network via electing reliable and stable nodes to take part in the active HBBFT consensus Epoch. Staking tokens allows the participants to earn rewards and take part in on-chain governance.

4.3 Consensus Mechanism

4.3.1 Lightweight Consensus Mechanism

The move from Proof-of-Work to a lightweight consensus mechanism is an essential improvement in blockchains and is being undertaken in the Ethereum network as well as in newer blockchains. Proof-of-Work is reliable but it has proven inappropriate for the long-term health of blockchains for three reasons:

- high carbon footprint;
- potentially limited throughput;
- and high transaction costs.

For all these reasons, DMDv4 adopts a PoS protocol. To learn more about the energy efficiency of PoS versus PoW blockchains, read the Artis blog article that shows the numbers that are relevant for DMDv4 as well[16].

PoW protocols require specialized hardware requirements for running a hardware node, particularly because of the competition to make an income from mining. Without specific mining equipment expertise and very cheap electricity, it's impossible to become profitable. Staying profitable in the PoW mining world means rapid hardware upgrades, increasing waste, and environmental damage. Blockchains developed today no longer consider PoW to be a viable solution. Proof-of-Work blockchains are notorious for their wasteful and unsustainable energy consumption. For further reading see *Bitcoin's Growing Energy Problem*[17] and *Decarbonizing Bitcoin*[18].

[15] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3368483
[16] https://lab10.coop/blog/artis-energy-efficiency/
[17] https://www.cell.com/joule/pdf/S2542-4351%2818%2930177-6.pdf
[18] https://www.sciencedirect.com/science/article/pii/S2214629618301750

Another disadvantage of PoW protocols, such as Nakamoto consensus, is that they do not produce block finality. In other words, blocks may be mined at the same time by several miners, resulting in a temporary dual-chain state. This can result in long waits before a transaction is verified, high and static block times, and transactions can be removed altogether if they only exist on the short chain. As a result, these blockchains are notorious for the high incidence of forking due to this competitive consensus algorithm. DMDv4 prevents forking by completely eliminating this problem by utilizing a cooperative consensus which allows dynamic extreme low block times if there is a demand on the network and long times without blocks if there is no demand.

Instant transaction finality is a particularly critical feature for high-value financial systems, such as exchanges and other DeFi applications. For developers of any type of finance application, this feature makes DMDv4 superior to other blockchains.

In Proof-of-Stake, anyone in the network can participate in the network security and governance, and PoS is being used in more recent blockchains, but PoS is still a competitive algorithm and it doesn't guarantee the performance that the Diamond DMD team was seeking. Therefore, DMDv4 uses the Honey Badger BFT protocol which achieves consensus without competition, sharing rewards among validators, again making this a more distributed and democratized network. The combination of HBBFT with the validator selection mentioned above is the key to achieving high performance and highly distributed governance without any trade-offs or compromises.

4.3.2 Honey Badger BFT Protocol

DMDv4 includes the adoption of the best-proven consensus algorithms to date, the Honey Badger Byzantine Fault Tolerant (HBBFT) protocol.

DMD Diamond v4 is implementing the HBBFT protocol for faster throughput, higher security, dynamic block times, robustness, and elimination of orphan blocks and forking potential. HBBFT allows nodes in a distributed environment to use an asynchronous methodology to reach consensus on transactions.

As stated in the Honey Badger BFT whitepaper[19]: *"In fact, Bitcoin provides terrible performance by distributed systems standards: a transaction takes on average 10 minutes to be committed, and the system as a whole achieves throughput on the order of 10 transactions per second. … the demand for robustness is often closely related to the demand for decentralization— since decentralization would typically require the participation of a large number of diverse participants in a wide-area network."*

With Honey Badger BFT, block finality is immediate, and transactions can be confirmed within seconds. No mining is necessary to run HBBFT, and the protocol requires a small pool of validators. DMDv4 uses a subset of 25 active validators that are selected from the pool of all valid validator candidates every 12 hours (Epoch).

The ⅔ +1 validator threshold encryption (this means a stable over two-thirds majority of the active validator set is needed (to wait on the last contributing (slowest) node is not required) allows for very fast validation and low transaction fees. Rotating the validators as described

[19] https://eprint.iacr.org/2016/199.pdf

in the *Node Selection through POSDAO* section ensures that there is no centralization and that many full nodes in the network have the opportunity to serve as validators.

To get the complete details on HBBFT, read the original Honey Badger Byzantine Fault Tolerance whitepaper as well as the following articles:

- HBBFT Introduction[20];
- How HBBFT Works[21];
- Threshold Cryptography & HBBFT[22].

4.3.2.1 The HBBFT Main Features

- **Asynchronous**, which is appropriate for a wide-scale global network.
- **Leaderless**, meaning that no one node has to declare a transaction. Instead, the validating nodes each propose a fraction of the transactions, and all nodes author the transactions simultaneously and share the block rewards.
- **Instant finality**, based on the asynchronous nature and the assumption that validator nodes have reliable and secure direct connections.
- **Censorship-resistant** based on the consensus of all validators.
- **Random number generation built-in**. Because some of the functionality of the consensus mechanism for the validation requires random number generation, the HBBFT includes an easy way to generate random numbers, making the chain particularly useful for applications that require random numbers.
- **No empty blocks are produced**. HBBFT approves blocks as quickly or slowly as needed for the blockchain. In the DMDv4 implementation, we will include a heartbeat if there is a long period (10 minutes) with no block production on the chain, but it will be a very small transaction so as not to impact the size of the blockchain.

4.3.2.2. HBBFT Features to Guard Against Attacks

Even when there is heavy traffic, messages can be delivered asynchronously, so information is not lost. Even if a malicious actor is trying to overload the network, or a particular dApp is experiencing a spike for some reason, the network will continue to function, delivering messages as it can.

Validators must reach an agreement on transactions while they are encrypted so that no validator can censor particular messages. The contents of the transaction are decrypted only

---

[20] https://www.xdaichain.com/for-validators/consensus/honeybadger-bft-consensus/building-honey-badger-bft-part-1

[21] https://medium.com/poa-network/poa-network-how-honey-badger-bft-consensus-works-4b16c0f1ff94

[22] https://www.xdaichain.com/for-validators/consensus/honeybadger-bft-consensus/honey-badger-bft-and-threshold-cryptography-part-3

after consensus is confirmed, preventing malicious nodes from selectively approving messages, because the validators can't know what is in a transaction before they approve it.

Malicious nodes can be identified and are reported through a fault log. Networks can then decide the best methods to remove them.

4.3.2.4 Instant Block Finality

The HBBFT protocol provides instant block finality. A block is only produced after the transactions have been finalized by the validating nodes in the network. If a block is signed by the validators, it is finalized, even if it is the latest block. This prevents transitory forking and creates an immutable, immediate ledger of transactions.

4.3.2.5. Block validation

HBBFT relies on the following assumptions:

- A secure connection between every agent performing a transaction.
- Trusted nodes as reference points, so that agents can always refer to trusted validators and full nodes as reference points[23] [24].
- Agreement of 2/3 of the nodes for consensus, rather than 51%.
- Unbounded buffers for nodes.
- Approval of transactions does not have to follow a strict synchronous timing, as long as the consensus threshold is reached.
- Triggers for the consensus finding process are set with the blockchain implementation.

Implementation of HBBFT requires a small number of validator nodes with persistent and reliable secure connections between them. DMDv4 uses 25 validator nodes in an active set, which rotate every 12 hours (Epoch). More details about validators can be found in the *Node Selection through POSDAO* section.

Triggers that are set in DMDv4 for block validation are:

- **Block agreement process**: HBBFT consensus is based on a list of transactions proposed by the acting validators. The validators collaboratively sign the block using threshold signatures.
- **RNG (Random Number) Generation**: HBBFT includes a mechanism for choosing the validators using a secure random selection mechanism. This ensures that validators are selected from the validator candidate pool in a fair and secure manner. A nice side effect such RNG numbers can be used by other blockchain applications that need true randomness without the need to have an own RNG engine.

[23] https://eprint.iacr.org/2016/199.pdf
[24] https://github.com/poanetwork/hbbft

- **Block validation**: Blocks sealed with a threshold signature need to be accepted, so the current validator set needs to match the threshold signature with the validator set master key.
- **Block creation**: New blocks are created as soon as the transactions for the previous block are initiated, even if the full block was not approved yet by all validators. This asynchronous immediate block creation mechanism translates into faster transaction times.
- **Governance contract interaction**: OpenEthereum uses POSDAO to change the validator set between Epochs, and reports malicious validator behavior if detected.
- **Validator set changes/key generation**: For the transition of the validator set, threshold keys are generated on-chain for the new validators through a smart contract.
- **Networking**: HBBFT requires direct contact between all validators in the active validator set.
- **Network startup**: Items must be added to the chain specification so they are included in the genesis block. This includes compiled governance contracts and the public master key. In addition, corresponding key shares must be distributed to initial network validators (this may be accomplished outside of the network) prior to network start.

The one-second minimum block time is in fact a one second waiting time after a block is finished before starting the creation of another block to minimize the delay between the broadcast of a transaction and inclusion in the chain. When there is a heavy network load, it's possible that the block could take longer than 1 second, so there is no guarantee of immediate processing of the block. In other words, the minimum threshold for starting a block is 1 second. The maximum is 10 minutes because the chain creates a heartbeat block if there are no transactions for 10 minutes.

4.4. Nodes and Network Participants

Diamond DMDv4 participants can potentially be one of three types:

- **Ethereum client wallet (participant)**. Any wallet that supports custom Ethereum networks and Walletconnect allows DMDv4 token holders to participate in staking and voting by choosing a validator candidate.
- **Full Node**. A full node includes an EVM, the POSDAO codebase, and the full Diamond DMDv4 blockchain.
- **Validator Candidate Node**. A Full Node can become a Validator Candidate by installing the validator candidate software and staking a minimum of 10,000 DMD. Other coin holders can stake their coins on a validator candidate, up to a maximum of 50,000 DMD. The upper limit prevents the concentration of power. Validator candidates are chosen in every Epoch to be validators, in proportion to the amount of staking they have on the node.

Nodes must run on the Linux operating system (or a System that allows execution of Linux software (e.g. Windows subsystem for Linux). Read more on the validator requirements in the *Validators section*.

It is possible to hold DMDv4 coins without staking or participating actively in the network.

5. DMD Coin Economy

5.1. DMD Coin Features

The functions of the DMDv4 coin include:

- On-chain governance.
- Network security.
- Payments.
- Network fees and deployment of smart contracts.
- DMD represents a limited and constant-size resource that has reward earning abilities.
- Earning rewards for active coin usage as a validator or dPOS staker aimed at protecting the blockchain.

In addition, DMD is highly distributed, being held by a large number of smaller investors rather than concentrated in the hands of a few. Following is the distribution of DMD tokens from Block explorer as of December 2020, showing the highly distributed nature of the token holdings, with less than half of the tokens being held by the top 100 people in the network[25].

Table 3: DMD coins distribution among holders

Top N addresses	Holdings	Percentage
Top 10	480,302 DMD	13.57%
Top 100	1,703,542 DMD	48.13%
Top 1000	3,445,514 DMD	97.35%
All 11160	3,539,236 DMD	100%

[25] https://chainz.cryptoid.info/dmd/#!rich

5.2. Issuance of Tokens

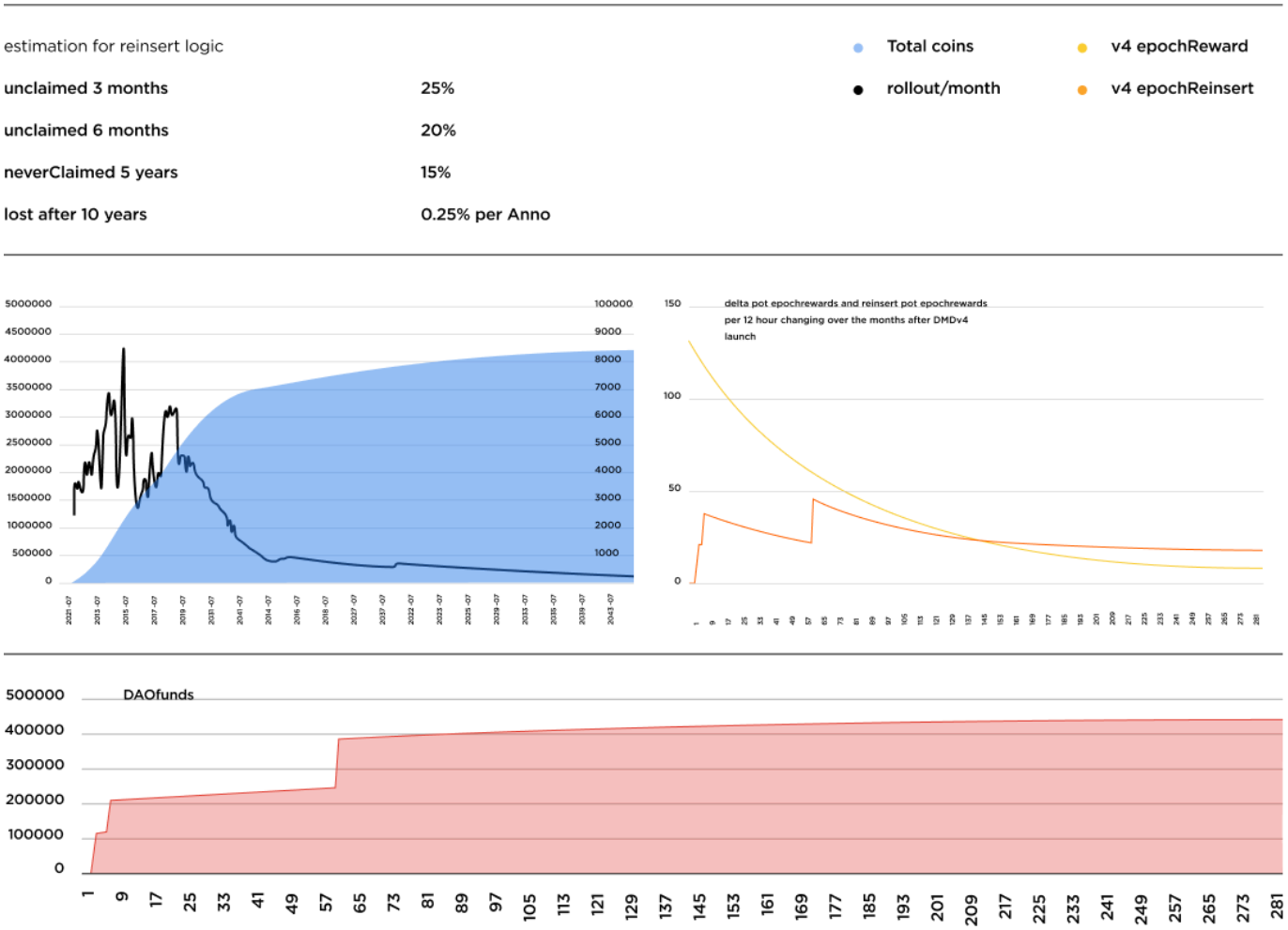
Token issuance for the DMD coins has followed the original plan and continues on the trajectory outlined in the original DMD Diamond White Paper[26]. DMD does not issue coins based on an algorithm. Rather, all coins are created with the initiation of the blockchain and they are allocated to the DMD coin holders on a one-to-one basis. The total emission of DMD coins is 4,380,000.

Table 3: Block rewards and inflation

DMDv1 & DMDv2	July 13, 2013 – August 2017	In its early days, DMD had a Hybrid POW/POS mechanic to roll out coins and reward nodes securing the chain. Around 50% of max coins were distributed in that first 4 years.
DMDv3 Phase1	September 2017 – February 2018	Block rewards for blocks 0 – 115200 constant at 2.35 DMD.
DMDv3 Phase2	March 2018 – August 2020	Block rewards for blocks 134400–691200 followed a decreasing curve from 2.29 DMD per block to the current rate of 0.55 DMD with the correlating decrease in the inflation rate.
DMDv3 Phase3	September 2020	From Block 710400 till block 2284800 the reduction in network rewards will slow down from 0.5 DMD to 0.157 DMD per block, while annual monetary inflation will fall from 3.5% to 0.96% within that period. Release of DMDv4 will freeze Phase 3. Undistributed coins will be moved to the DMDv4 delta pot.
DMDv4	DMDv4 release 2021	The DMDv4 reward logic will recreate a similar curve for roll out undistributed coins and add on top a unique coin reinsert logic that allows for endless rewards even with a small finite supply.

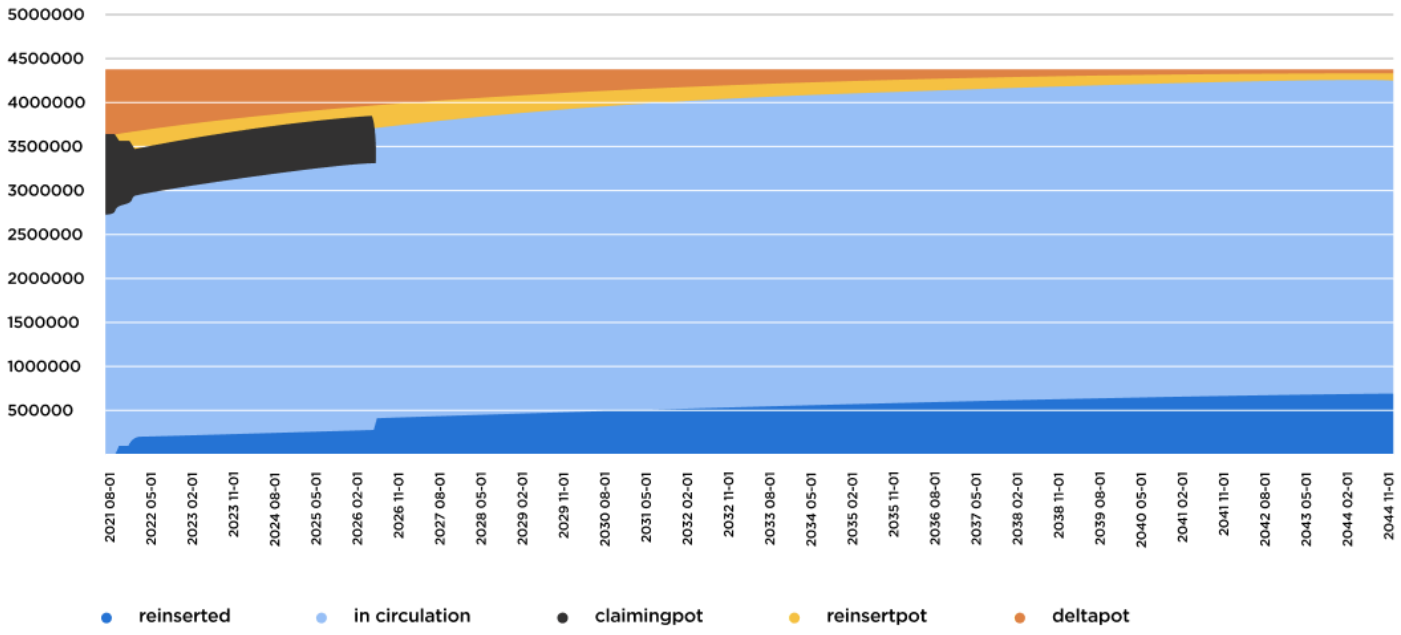
[26] https://bit.diamonds/DMD_WP.pdf

Pic. 2: DMD Coins Rollout & Supply



DMD Diamond's emission model was remodeled with the advent of the second iteration of the core software in 2014. It implied ever-decreasing inflation from a steep 50% APR progressively to around 1% in the years to come. The premise was based on block numbers as signposts for when to introduce changes to the monetary supply. This made it clear and intuitive when and how much the adjustment would have taken place.

Pic. 3: DMD Diamond v4 Coin Reward Perpetuum Mobile via Reinserting Not Claimed and Abandoned Coins



The coin rollout is the cornerstone of DMD's monetary system, however, changes to the way this new blockchain works and accounts change with DMDv4.

As a leaderless consensus, there are no blocks in a classical UTXO sense; transactions are approved as fast as they come which makes it impossible to follow a model where block numbers happen at a predefined time. The only predefined transaction is that if there is no network traffic for 10 minutes, the blockchain emits a heartbeat transaction.

To stay true to the previously arranged coin emission there will be a new way of calculating daily inflation and it ties to the way rewards are distributed among delegators and validators from Epoch rewards that are funded by delta pot and reinsert pot and governed by a sophisticated smart contract construct. More details can be found in *Solving the Lost Coin Problem* section.

DMDv4 release coincides with DMD going through Stage 3 of the emission model as outlined in DMDv3 White Paper where issuance of network rewards slow down from 0.5 DMD to 0.157 DMD per block, while annual monetary inflation will fall from 3.5% to 0.96% within the period of approximately 8 years.

5.3. Network initiation

At the release of DMDv4, all smart contracts are initiated in the genesis block, together with information about bootstrapping validators. In order to start the network, a predefined number of nodes must be selected to provide service for the duration of the initial staking Epoch. That process requires a high degree of coordination, therefore the core team serves as the technical enablers of this blockchain and will host a trusted set of DMD Diamond Foundation nodes to launch the network.

There is no monetary advantage for initiating validators as their pools are empty while the reward itself is lowered.

Registration to join the new network can take place during the initial Epoch with full registration taking an effect at the next staking Epochs.

5.4. Migration from DMDv3 to DMDv4

All holders of DMDv3 can claim an equal amount of DMD for version 4. Claiming DMDv4 does not change anything on the DMDv3 chain, so it's not technically a swap of the coins but that the proof of ownership of DMDv3 entitles the address holder to claim the DMDv4 coins.

Following are the instructions for swapping the coins and the conditions of the coin swap.

- Set up a wallet that can accept DMDv4. Any Ethereum-compatible wallet can accept DMDv4. Minerva Wallet includes DMDv4 as one of its supported coins by default.
- Use the DMDv3 to sign a validation that you are the owner of the DMDv3 coins. Enter the address of your new wallet for claiming DMDv4 coins. The DMDv4 is sent in a 1-to-1 ratio to the new wallet.

When DMDv4 is released, the DMD Diamond team will be releasing full documentation including video documentation of how to claim the coins. Note that this is not technically a swap, because the DMDv3 chain still holds the coins, but once your address has claimed the DMDv4, it cannot be repeated with the same address again.

When you transition to DMDv4, you will also be able to stake DMD on validator nodes for the purpose of earning coins for validation, as well as for voting on proposals in the DAO that will govern the DMD chain. After the transition, the Diamond DMD team will no longer provide any support for the DMDv3 blockchain. DMDv3 is open source, so it is feasible for anyone who wishes to maintain the legacy code to do so.

To eliminate inactive users and lost coins, there will be a claiming period under which your DMDv4 coins need to be claimed in order not to return to the pool of coins.

- Claiming DMDv4 balance within 3 months of release entitles coin holders to the full amount of coins, with 1 DMDv4 coin for every 1 DMDv3 coin owned by the coin holder. The release of DMDv4 is at least 3 months after the release of this White Paper. The rollout will include a trusted phase at the start to ensure that the first validators on the network are known.
- Between 3-6 months of release, DMDv3 coin holders can claim 75% of the coins. The other 25% are returned to the coin pool as described in *Solving the Lost Coins Problem section*.
- Between the 6th month and 5 years, DMDv3 coin holders can claim 50% of the coins they originally held.
- After 5 years, all leftover coins are redirected to the governance and reinsert pot and the claiming period ends.

5.5. Solving the Lost Coins Problem (Previously Treasure Digging)

All coins are created at the genesis block and put in different pools for distribution over time through the blockchain rules of DMD. DMDv4 has four pots:

- **Claiming pot:** The Claiming pot starts as the total amount of coins that should be held by coin holders and are already allocated to the coin holders in DMDv3. At the initiation of the chain, coins are sent directly to their owners as soon as they run the claiming dApp tool to prove ownership of the old DMDv3 address and link it to their new DMDv4 address. The remaining claiming pot is a 1-to-1 representation of all coins that are waiting to be claimed by the DMDv3 coin holders.

- **Delta pot**: The delta is the coins that would have been generated between the current issuance at DMDv3 snapshot and the maximum total coins of 4.38 million DMD. These are the reserve coins that are released over time in DMDv4 as part of Epoch rewards.

- **Reinsert pot:** The Reinsert pot is funded with half of the coins that are abandoned by being staked on an inactive validator node. Coins are recovered to the reinsert pot under two circumstances: when people do not claim their DMDv4 coins and when validators are inactive for 10 years. Validator nodes are closed if they are not active for 10 years, so if someone stakes their coins on a validator node that has not been active for 9 years, their stake will be reclaimed 1 year later — but it should be obvious that someone should not stake coins on an inactive validator.

- **Governance pot:** The Governance pot will be managed by a DAO. The pool is funded by half of the lost coins that are not placed in the reinsert pot, and the coin holders can create and vote on proposals for distribution of the coins. Voting on the use of the Governance pot is weighted according to people's coin holdings so that the network will vote in the best interest of maintaining the value of the coins.

The block rewards that are allocated from the Delta and Reinsert pools are related to the amount of funds in those pools. As the size of the pool reduces, the amount of DMD per transaction will also reduce. Depending on the value of the coins at the time, this may or may not represent a real change in the reward value for the validators.

Coins are recovered according to the following schedule:

- If a DMDv3 holder does not claim their coins within 3 months of the DMDv4 mainnet release, 25% of the coins are recovered and split between the Reinsert and DAO pools. As of the publication of this White Paper, DMDv3 holders can claim their coins, so in fact, they have 6 months from the date of release of the White Paper to claim DMDv4.

- If the DMDv3 holder does not claim their coins within 6 months of the release of DMDv4, another 25% of the coins are recovered.

- If the DMDv3 holder does not claim their coins in 5 years, all coins are recovered and they lose their rights to claim DMDv4. This could happen intentionally if they decide to stay with DMDv3 or if they are simply inactive.

- If a validator candidate is inactive for 10 years, the staked tokens for the validator nodes are recovered into the pools. Also, any delegated staked tokens for that inactive validator are returned to the pool.

These mechanisms are sustainable over the long term to remove the problem of missing coins, and also to continuously fund the DAO and the Reinsert pool.

5.6. Use of Funds

During the coin rollout, 10% of coins are used to fund the development. In addition, the DAO is funded by 50% of the unclaimed coins in the transition from v3 to v4. The DAO funds will be used to promote the DMD project, as voted on by the community members. Funds can be used for chain upgrade developments, marketing, or any other activity that the coin holders choose to fund based on proposals to the Governance DAO.

6. Roadmap

Table 5: The roadmap of DMD v4 release and future development

Stage	Date	Description
White Paper		DMD Diamond releases its v4 White Paper.
Open testnet	>= 1 month later	Open testnet starts with candidate release of DMD v4.
Claiming tool tests	Around the same time	The claiming tool is being tested.
DMD v4 mainnet	>= 3 months later	DMD v4 mainnet is live.
DMD v4.1		DMDv4.1 core content will be on-chain governance systems (DMDDAO) that interact with POSDAO for voting weights.
Future goals are set and voted on by the stakeholders and DAO participants.		
Possible future goals		● Message Bridge (AMB) development: A bridge designed for universal cross-chain data transfer. ● DEX or protocol for automated liquidity provision with a positive impact on the DMD coin economic model, with fees to reinsert pot and bonus rewards for active stakeholders. ● Any other suggestions initiated by the community of stakeholders and validators.

7. Team

Aleksander Mesor, Chief Executive Officer

Leading the Diamond DMD Foundation for more than 7 years, Aleksander brings unmatched dedication and passion to the project, as well as experience in operations, leadership, and communications.

Helmut Siedl, Chief Visionary Officer

Leading the vision and research on the mechanics and technology of the coin, Helmut brings impeccable attention to detail and deep research skills for assessing and adopting the best technology for the DMD project. Helmut has been deeply involved in the blockchain space for more than 7 years and is a co-founder of the lab10 and a founder of Blockserv Blockchain Services, leading technology initiatives that create a freer society.

Thomas Haller, CTO

Bringing deep experience in software development and blockchain, Thomas provides technical guidance for the implementation of the DMD technology.

Dr. David Forstenlechner, contributor

David brings more than 15 years of software development experience to the project as a contributor.

Dietmar Hofer, contributor

An expert in complex software development projects, Dietmar brings his expertise to create the most advanced blockchain technology features to the project.

Whitepaper Contributors:

- Grace Rachmany
- Aleksander Mesor
- Helmut Siedl
- Stacy Muur
- Thomas Haller

Community Review Participants:

- DrDMD (slack)
- Knotwork (slack)
- Digital_Demon (telegram)
- WaddlingDuck (telegram)
- gg (slack)

- stillontop (slack)
- dsoronda (slack)
- panzerfly (slack)
- Supermegatom (telegram)
- Trimegistus (bitcointalk)
- EXPose (discord)
- dforsten (slack)
- didi (slack)
- MitchellMint (discord)