Monero Diamond (XMD)

monerodiamond.club

Abstract. Monero Diamond is a community-led project designed to create a limited supply hard-fork of the Monero cryptocurrency to a new scalable blockchain algorithm. The idea is to create a decentralized environment in which professional developers chosen by the community, enhance, simplify, and develop Monero Diamond to scale for mass use. The original Monero vision was to create a private digital currency; however, a conservative, centralized core control of few and slow development process prevents new users and technologies from being incorporated.

A more rapid development process based on bounty programs that will allow new people around the world to participate, will potentially make Monero Diamond the first private digital currency used by millions of people with open endless development possibilities. In addition, Monero Diamond will adhere to core Austrian school of economics principles by capping the total Monero Diamond coins that can be created, parting with Monero's infinite coin supply structure.

1. Introduction

Monero was created for a specific reason: to be an alternative digital currency to Bitcoin that is private and anonymous. Unlike Bitcoin, Monero is an untraceable cryptocurrency based on the Cryptonote protocol. Transactions, amounts transferred, and wallet addresses of both senders and receivers in the Monero network are all obfuscated. Therefore, transactions cannot be linked to a particular user.

Unfortunately, Monero has suffered from several drawbacks. For example, Monero's infinite coin supply, the centralization of decision making that prevents the implementation of new features, the scaling issue of a bloated blockchain, the high transaction fees, and the growing hash rate that is mainly based on mass usage of botents and unsuspected browser based miners that prevents genuine miners to compete.

Some critical flaws that cannot be fixed rapidly due to Monero's voluntary donation based development process has deterred Monero’s widespread adoption. Due to these circumstances, it is better to create a hard-fork split that will indefinitely fix these problems. Fixing these problems will require a dedicated team of full-time developers, which is how Monero Diamond was born

2. Max Coin Supply

The Monero source code was forked from Bytecoin, an implementation of the Cryptonote protocol. The Cryptonote white paper suggests that a predefined maximum coin supply such in the case of Bitcoin, is simply an intuition, and that a natural upper bound of coins to be created should be the largest number that can be represented, and essentially infinite:

“not on intuition such as N coins ought to be enough for anybody.”

Unfortunately, Monero implemented this suggestion, guaranteeing an infinite amount of XMR coins created. This is one of Monroe's fundamental flaws that cannot be fixed. In the same way central banks around the world print money out of thin air, Monero’s infinite coin supply is a tax in the form of inflation for all XMR holders.

Bitcoin’s 21 million maximum coin supply was introduced specifically to avoid having a body that controls the money supply, completely restricting future inflation and devaluation of Bitcoin coins.

Based on this merit alone, Monero would never be able to compete with Bitcoin as the world’s best digital currency, since the idea of infinite coin supply is the incorrect intuition.

Monero Diamond adheres to core Austrian school of economics principles and caps the total amount of XMD coins that can be created to 300 million. The initial coin amount in circulation at the time of the hard-fork would be one times the amount of XMR coins (~16,8 Million). XMR holders prior to the hard-fork will receive one-times the amount of XMD coins.

3. Scale & Features Development

Although a conservative approach for feature development in Monero could be seen as a strength, for example of privacy concerns, such an approach also prevents it from integrating crucial features that could differentiate it from other cryptocurrencies in terms of mass use. Monero Diamond takes the approach of fast development and feature integration.

Monero does not scale. As of the time of this writing, Monero's median transaction size excluding coinbase transactions is 51.2 times larger than Bitcoin's median transaction size (13.21 kb vs 258 bytes). If Monero was to handle the cumulative transactions amounts of Bitcoin, its blockchain size would be higher than 7.7 Terabytes (in comparison to Bitcoin's 155 Gigabyte blockchain). In turn, the fear from an imminent bloated juggernaut blockchain comes with higher median transaction fees than Bitcoin.

Monero Diamond plans to tackle the scaling issues, which is the main source of problems in Monero, and in all cryptocurrency coins for that matter, and integrate the MimbleWimble protocol so that the blockchain size will be bound to the number of users using Monero Diamond (not the number of transactions being made in the network). This will significantly reduce both transaction costs and blockchain size, permanently solving the scaling problem.

Monero Diamond will also take a more pragmatic approach when it comes to end-user applications and usage for example, introducing a light Monero Diamond wallet by default so that users will not be asked to download the whole blockchain if they do not want to. Users with high privacy concerns will still have the standard privacy wallet by default.

These development features cannot be achieved in a timely manner by solely fundraising from the community. Monero Diamond will issue bounty programs for top-tier developers and researchers to rapidly develop all aspects of the Monero Diamond network.

4. Monero Diamond & Monero Comparison:

	Monero Diamond	Monero
Max coin supply	300 million XMD	Infinite XMR
Coins in circulation at hard-fork block	~16.8 million XMD	~16.8 million XMR
Emission per block	Smooth emission decline with a 6 XMD minimum until max supply reach.	Smooth emission decline with a 0.6 XMR minimum for infinity.
Starting block	1729888 (while a snapshot of all previous blocks was taken from Monero's blockchain)	0 (Genesis)
Block interval	120 seconds	120 seconds
Difficulty adjustment	Every block	Every block
Difficulty algorithm	Improved LWMA	Simple average (N=720)
PoW algorithm	Cryptonight V7	Cryptonight V7

5. Hard-Fork Split

Monero, like many other cryptocurrencies, is based on a decentralized consensus mechanism. Monero nodes run software that is restricted to certain consensus rules so that nodes not complying with these rules would not be included in the Monero network. Other nodes in the Monero network check if a certain block, when it is mined, complies with these consensus rules. It is either accepted by other nodes in the blockchain if it does, or rejected in case it does not.

A hard-fork occurs as a result of Monero Diamond's deviation from the current Monero consensus rules. Monero nodes and Monero Diamond nodes will still comply with the same rules, validating everything that took place on the blockchain before block 1729888 . But from block 1729888 , Monero Diamond's new rules come into effect, which will cause nodes of Monero to reject blocks that were formed with Monero Diamond rules and Monero Diamond nodes to reject Monero based blocks . Thus, the network will split.

The Monero blockchain will continue to add new blocks to its blockchain; however, from block 1729888 , Monero Diamond will begin creating a new branch of blockchain that diverges from Monero. Monero Diamond and Monero will share the same history of transactions and balances up until that point. This new branch will represent a new cryptocurrency: Monero Diamond.

The new consensus rules imposed by Monero Diamond will come into effect at block 1729888 . From this point forward, miners on the Monero Diamond network will begin to add blocks to the new branch: Monero Diamond's blockchain.

Monero (XMR) holders prior to block 1729888 will automatically receive the equivalent of ten times the amount of their Monero holdings in Monero Diamond (XMD).

6. Monero Diamond (XMD) Airdrop

Rules of Monero Diamond Airdrop:

- Limited to 39999 participants.
- To recieve 100 XMD (Monero Diamond) you need to complete required tasks! Please keep following all accounts of which the task you have joined till the end of airdrop.
- The XMR tokens will be distributed on 31th December 2018.
- Each valid referral will be worth 50 XMD tokens. To count as valid referral, the referred person needs to complete at least the required tasks.
- Get more info: @MoneroHardforkBot

Also to acquire Monero Diamond, you simply need to hold Monero prior to the fork, ensuring you will receive automatically the equivalent of XMD the amount you hold in XMR. A wallet with the same address, private keys, and mnemonic phrase you had in Monero will be created for you and your XMD holdings.

If you own XMR on an exchange or any other third-party service and do not have exclusive access to your private keys, then it is up to these providers to support Monero Diamond after the fork. In this case, you should check if the third party that holds your XMR supports Monero Diamond and will issue your XMD holdings to your account. We strongly advise to transfer your XMR either to a service that will support the split, or to your private wallet prior to the fork, as you will not be able to receive your XMD holdings after that point.

7. Hard-Fork Release Timeline

7.1 Monero Blockchain Fork

When Monero reaches block number 1729888 , a snapshot of the Monero blockchain will be taken. The Monero Diamond network will launch a few days later with the first Monero Diamond block added on top. Monero will keep adding blocks to its blockchain; but when Monero Diamond is launched a few days later, it will begin adding blocks to the snapshot that was taken.

The delay in the fork is needed so that Monero Diamond’s seed nodes, worldwide full nodes, and the RPC wallet, CLI wallet and GUI wallet will all be tested and compiled. When everything is ready after testing, the peer-to-peer network will begin. Monero Diamond full nodes will only accept the network signature of Monero Diamond.

Block 1729888 will be the first Monero Diamond block mined solely on the Monero Diamond network. At this point, the Monero Diamond cryptocurrency will be created while Monero continues adding blocks to its blockchain.

7.2 Monero Diamond Blockchain, Wallet RPC, CLI & GUI release

All coins, transactions, fees, and balances will be represented in Monero Diamond as one times the amount of their Monero counterpart. Essentially, every value on the Monero blockchain will be copy. For example, block 1 in the Monero blockchain contains a coinbase transaction with an output of 17.592169267200 XMR. Thus, coinbase transaction in block 1 of the Monero Diamond blockchain will go to the same original miner who mined the original block in Monero. He will receive 17.592169267200 XMD for that transaction.

In the same manner, if you had a balance in your Monero wallet of, say, 3.1415926535897 XMR prior to the fork, then you will receive 3.1415926535897 XMD. This was done to differentiate the two cryptocurrencies while making the two cryptocurrency wallets – Monero Diamond's and Monero's – to reject one another's blockchain.

If you own XMR at the time of the fork and have access to you private keys, you will be able to spend your XMD at the ratio of 1:1 at any point in the future. If a third-party service is holding XMR on your behalf, then they will receive the XMD. Exchanges or any other third-party services are not obligated to credit you with your XMD in the ratio of 1:1. Therefore, you must make sure beforehand that they will do so, or move your XMR to a private wallet before the fork.

8. Development Finance

The first block that will be mined on the Monero Diamond blockchain will have a customized coinbase transaction amount that will allow the development team to mine it in a controlled manner, using it for future development of Monero Diamond. The Monero Diamond development team will manage 5.859375% of the total supply of Monero Diamond coins, using it to enhance the development of all future works.

This will enable Monero Diamond to rapidly develop many urgent tasks in the form of developer bounties, adding many paid full-time developers to the team.

- 66.6% of the funds mined by the development team will be proportionally distributed to all team members and contributors.
- 33.3% of the funds mined by the development team will be transferred to a multisignature wallet, with the private view key being released to the public.
- All future expenses such as storage costs and developer bounties will be detailed and transparent.

Most of the bounties will go to developers and third-party services, like storage and security services. The core mission of Monero Diamond is to rapidly add features and fix the current Monero drawbacks. Although market forces will eventually price XMD, we have brought many expert developers onboard, and are welcoming many more to join the team prior to the launch.

Future development:

- Web wallet & Light wallet
- PoW modification
- MimbleWimble integration

Infrastructure:

- Servers:

Website server

Block explorer server

Online wallet server

Pool server 10+

initial full nodes 5+

Checkpoint servers 5+

DNS seeds

- DNS fees
- System administration and DevOps
- Security testing

Conclusion

Monero Diamond is a global open-source project promising to deliver a true private cryptocurrency adhering to core Austrian school economics. It is aimed for mass adoption and scale. Monero Diamond was not developed to compete with Monero, but rather with Bitcoin. Monero Diamond facilitates the desire to have a truly private and decentralized cryptocurrency that is also quick and easy for everyday use.