0xMonero

(Whitepaper Revision 1.2)

0xMonero: Privacy is Freedom

Overview

0xMonero is a multi-contract, multi-chain, privacy focused project built on Ethereum. $0xMR is compatible with all Ethereum Dapps, DEXs, and wallets. The project was fairly launched with no pre-mine on April 18th 2020. The founders of 0xMonero are anonymous and project development is overseen by the developer community “Semilla Labs”. The founders of 0xMonero created the project as a life raft for Monero miners and investors (0xMR is not wrapped Monero) and as a means for providing privacy options for Web3 users. The project and community (founded by 0xBitcoin and Monero miners) are open to like minded people who share our values- to promote freedom and privacy for all.

0xMonero utilizes the ERC20 EIP918 contract standard (0xMR) for mining and fair distribution. The EIP918 standard was created by a developer known as “Infernal Toast”, and is categorized as open source and free-use. The total and circulating supply of 0xMR is limited to 1.865250 million tokens (0xMR mining has ended).

Regulatory Compliance

The founders foresaw a financial regulatory environment where privacy coins are banned in every country and delisted from exchanges due to the fact that their sole utility lies in acting as a private alternative to CBDCs.

0xMonero will not be banned because it's built on Ethereum and has utility above and beyond the use of payments.

Banks and financial institutions are adopting blockchain technology and are using Ethereum. They are required by law to keep their customer’s identity and financial transactions private and will utilize zk-SNARKs to do so. This loophole protects 0xMonero from regulatory scrutiny. Furthermore, 0xMR was fairly launched, acts as a utility token, raised no funds from the public, and all tokens were mined into existence. 0xMR is regulatory compliant and cannot be ruled as a security by the SEC. The project can not be shut-down because it exists as an immutable smart contract on Ethereum that is managed by the community; there is no foundation or company to target. 0xMR can never be delisted as it is traded on decentralized exchanges.

Real World Utility

Many thought leaders in the cryptocurrency space believe that “up to 99% of cryptos will die”. Our team members have been involved in the industry since 2012 and have seen the rise and fall of numerous projects. This experience led us to the unique approach we have taken with 0xMonero. We believe that having good tech or raising a lot of money from the public aren’t enough to build a successful project, you need a sound business use case that generates revenue. That’s why we have focused to date on providing utility, platform integrations, and building partnerships.

0xMR has been integrated into numerous decentralized exchanges, wallets, and token bridges. 0xMR users can play hundreds of casino games in several partner casinos and 0xMR can be yield farmed on multiple chains. The 0xMR token can be used to pay for privacy services (like 0xTIP) created by 0xMonero developers.

Privacy

When interacting with any blockchain it is imperative that one use a VPN or TOR. If you fail to take these measures your ISP and your government can see that you are interacting with cryptocurrencies. Failure to take these measures could open you up to financial and legal liability depending on your jurisdiction.

Some features employed by 0xMonero to obfuscate transactions are:

- **0xTIP**- Use 0xTIP by 0xMonero to mix and bridge privately between Ethereum and BNB chain. 0xTIP also allows off-chain transfers and additional features such as off-chain private swaps and multiplayer mobile games are being added. Mixing is done using bulletproofs, stealth addresses, ring-signatures, and relayers upon withdrawal from the service.
- **Browser Wallets**- Use LUMI browser wallet in conjunction with Brave Browser TOR or the Incognito browser extension with Brave Browser and a VPN.
- **Game**- Use our partner casinos (LNOcasino.club, NEAR.casino, and Betcrypt365.com) to mix your tokens and receive funds in a new wallet.
- **Bulletproofs**- Users can currently wrap 0xMR with Bulletproofs (p0xMR) using the incognito blockchain service. Their wallets also provide stealth address functionality. Incognito supports shielding of 0xMR on Ethereum, Fantom, Aurora, BNB chain, and Polygon.
- **L2/Off-Chain**- You can transact privately with 0 gas fees using L2 solutions like the pillar wallet.
- **ChainHop**- A strategy employed which involves users moving their 0xMR between blockchains. Users can interact with Gnosis Chain, Syscoin, NEAR, Polygon, Fantom, Binance Smart Chain, and more using bridges. These bridges allow you to obtain 0xMR with different contract addresses. Additionally, several bridges employ relayers that break the link between sending and receiving wallets.
- **Trade**- You can trade 0xMR privately on pDEX and PrivacySwap.

Monero’s Flaws

0xMonero’s founders were Monero miners and investors who decided to create 0xMonero after discovering several flaws within Monero, namely:

1. Wallets are buggy and not user friendly.

2. Fake branded wallets that steal funds.

3. Users have to install wallets on Linux using the command line because Windows marks them as malware.

4. A complicated command line interface is required to access all privacy features.

5. A full node requires days to sync and requires well over 100 GB of storage.

6. Wallets cannot successfully sync to the blockchain.

7. Official desktop wallet has been infected with malware.

8. Mobile wallets and light clients may connect to malicious nodes and transactions may not be validated.

9. The majority of nodes are malicious and leak user's IP addresses.

10. The blockchain suffered several hacks, including a bug that allowed infinite coin minting.

11. The founder was arrested, which means he likely shared technical/user/personnel data to reduce his prison time.

12. The founder cannot access his wallet in prison, so funding for development and marketing has ceased.

13. Transactions are tracked by governments (Darpa) and Ciphertrace (patented).

14. Official website has been infected with malware.

15. The majority of hashrate is contributed by cryptojacker malware and bots.

16. The majority of hashrate is in one pool that can double spend and bring the entire blockchain down at any time.

17. The blockchain cannot be audited to see if there were additional coins minted or double spends.

18. Original devs have left to other projects, one dev contributes the majority of code and instead of working on fixing the node and wallet issues, is focused on atomic swaps.

19. Inflationary with an infinite supply- this and the inflation bug are why the price doesn't do well.

20. Banned in most first world countries.

21. Delisted from all major exchanges.

22. Mining software has viruses inside.

23. Most dark markets do not use Monero, they use Bitcoin.

24. No smart contract functionality or other utility other than being a method of payment.

25. Slow transactions.

26. Blocks cannot scale to be used as a real currency because of block size and node requirements.

27. Since privacy is enabled by default, all coins are essentially blacklisted.

28. Using the chain makes you a target for law enforcement as the majority of blockchain criminal activity involves Monero.

29. Larger cap cryptos are launching privacy functionality (Bitcoin/Litecoin) thereby eliminating the need for Monero completely.

30. There are hundreds of other Bytecoin forks with better features.

Fluffy Pony himself stated in an interview that he wants “all on/off ramps for Monero to have AML/KYC and that all transactions should contain geolocation data so that they can be taxed”. See for yourself:

https://www.coindesk.com/videos/recent-videos/moneros-spagni-cryptographers-are-always-going-to-be-one-step-ahead-of-regulators

The reality is that Monero is an overpriced fork of Bytecoin that can be tracked. There are a hundred similar cryptonote coins with similar privacy features and better functionality.

Research Monero exploits:

https://monero-badcaca.net/

https://www.monerooutreach.org/breaking-monero/

https://news.bitcoin.com/ciphertrace-patents-monero-transactions/

https://sethsimmons.me/posts/moneros-ongoing-network-attack/

Upgrade your Monero

0xMonero solves most of the issues present in Monero and can be considered a technological upgrade:

1. Easy to use wallets.

2. Easy mining on a Windows PC (ended).

3. Scalable 20k+TPS on L2 and faster with ETH2.0 sharding.

4. Secured by Ethereum’s Proof of Stake consensus- 0xMR cannot be 51% attached.

5. Fairly mineable (no Asics or FPGAs) (mining ended).

6. Limited token supply with fair distribution (no pre-mine).

7. Built in coin mixing.

8. Compatible with all Ethereum Dapps, DEXs, and exchanges.

9. Part of the 250k strong Ethereum developer community.

10. Smart contract functionality.

11. Bridges to the most popular EVM blockchains.

12. Decentralized- cannot be banned, blacklisted or delisted.

13. Legally compliant- no ICO/IDO, no team tokens.

14. Anonymous team- The project cannot be stopped.

15. Can be used in our partner casinos and in DeFi.

The choice is simple, the future of privacy is on Ethereum, and it's 0xMonero.

UTXO vs Account based Ledgers

The argument that account based cryptos are not as private as UTXO based cryptos like Monero is inherently false and comes from a misunderstanding of how account based ledgers work. You can retain anonymity with an account based ledger as long as you avoid tying your account to ENS or by associating your wallet to an exchange with KYC. All account based wallets are anonymous and include coin mixing by default.

"With regard to fungibility, the account model offers better privacy. There is complete transparency of UTXO movements (read assets) in the UTXO model when no privacy-preserving techniques are applied. However, the account model comes with a built-in "coin mixer" of sorts. When an account is funded with several transactions, the result is a single balance. When a payment from this account is made, an observer cannot determine which of the incoming coins is being spent. Consider the example of the account model above where Alice sends 8 ZEN to Bob, and his balance is updated to 9 ZEN. When Bob subsequently spends 1 ZEN, nobody can determine if the single ZEN stems from Alice or a different source".

https://academy.horizen.io/technology/expert/utxo-vs-account-model/

0xMonero is built on Ethereum, is account based, cannot be blacklisted, and is inherently anonymous. The way you maintain privacy on an account based ledgers is completely different from UTXO based ledgers like Bitcoin and Monero. When transferring funds on an account based ledger, you can easily employ one of the aforementioned techniques to hide your wallet. There is no need to use things like RingCT or other privacy protocols to hide transaction data because there is no transaction data to hide as EVM tokens do not contain transaction data. Instead, as previously stated, when using account based ledgers you must act to hide your wallet; whereas with UTXO based cryptos you must act to hide your wallet and each individual coin transfer, as both are tracked.

UTXO based cryptos carry transaction data in the coin and show everywhere they have been since they were minted. You could be holding blacklisted coins right now and not even know it. An exchange could flag your deposit and freeze your funds. You could even become part of a criminal investigation if you hold blacklisted UTXO based coins. Even if your UTXO based crypto is considered private now, it will likely be cracked in the future and your transactions will be visible to authorities.

How to Mine 0xMR (mining has ended)

In order to prevent the centralization of mining by Chinese ASICs (which has killed other mineable token projects), the team elected to only enable solo-mining. The team is planning to create a pool that incentivises miners with low-spec devices to ensure democratized distribution. These instructions are not fully exhaustive and are only a starting point for mining. The miner should adjust config files as well as the gas minimum/maximum/limit to achieve the best results.

Configure Windows:

- Download and install- microsoft.com/net/download/thank-you/dotnet-runtime-2.2.2-windows-x64-installer

- Download and extract the Solidity SHA3 miner- github.com/lwYeo/SoliditySHA3Miner/releases

- Set a Windows Defender exclusion for the miner folder

- Go to Infura.io, register, copy your webapi link

  Edit the solo batch file:

- Change what you want to mine with by saying true or false (cpu/gpu)
- Insert your infura webapi
- Insert the contract number-

  0x035dF12E0F3ac6671126525f1015E47D79dFEDDF
- Set your gas minimum, maximum, and limit
- Enter your private key for the wallet you will mine to (you need ETH in the wallet to mine as there is a gas fee)
- Save then execute the solo miner batch file

2023 Roadmap

- Additional casino integrations
- Bridges to additional Web3 chains- Hedera, Candle, Internet Computer
- Additional exchange listings- Saturn Network, AMMs, CEXs
- More DeFi integrations
- Integration with additional privacy platforms: Railgun, Aztec, Zkopru, ZeroPool, Hermes, Conceal Protocol…
- Launch our own private L2

Important links

0xMonero.com

Twitter.com/0xMonero

t.me/Monero0xMR

t.me/TIP_0xMR_bot

t.co/5YdrYTsHZv

cryptovoxels.com/spaces/e62be768-626a-4de5-a367-978af2239924

cryptovoxels.com/play?coords=SW@290W,666S

coingecko.com/en/coins/0xmonero

etherscan.io/token/0x035dF12E0F3ac6671126525f1015E47D79dFEDDF