Logo, company name

Description automatically generated

Contents

[1. What is Blockchain? - 1 -](#_Toc115725505)

[2. What is Monero (XMR)? - 1 -](#_Toc115725506)

[3. History of Monero (XMR) - 2 -](#_Toc115725507)

[4. Why do people invest in the coin? - 2 -](#_Toc115725508)

[**4.2. Primary use case** - 2 -](#_Toc115725509)

[**4.3. Privacy features** - 3 -](#_Toc115725510)

[5. Strengths and Weaknesses - 4 -](#_Toc115725511)

[5.1. Strengths: - 4 -](#_Toc115725512)

[5.2. Weakknesses: - 4 -](#_Toc115725513)

[6. Monero’s Market Price - 5 -](#_Toc115725514)

[7. How does it works? - 7 -](#_Toc115725515)

[7.1. Stealth Address - 7 -](#_Toc115725516)

[7.2. Ring Signature - 8 -](#_Toc115725517)

[8. Conclusion - 10 -](#_Toc115725518)

[References: - 11 -](#_Toc115725519)

# 

# What is Blockchain?

The main purpose of blockchain is to allow digital information to be distributed on the public ledger to every node on its network to everyone. Once the data is recorded inside the blockchain it becomes complicated and impossible to alter, edit, or destroy. This technology is created by the infrastructure around trust, not with either central bank, companies, or government, but is the trust between users. To ensure the integrity of the chain inside each block contains data, a hash, and the previous hash that are connected to each other so if one of the previous hashes changes the chain will be cut immediately. A hash is a cryptographic algorithm that calculates the data from any size to a fixed length. Also, it can be compared to a human's fingerprint due to one reason for uniqueness. For instance, if you are buying bitcoin: every validity transaction is stored in the block and will be sealed by hash, if you are making any changes the hash will modify accordingly. So, a hash is one of the strong foundations of cybersecurity that secures the block and all of its contents, the purpose of this cryptographic hashing method is to convert every possible data into a string character. Nowadays, technology is more advanced than it is ever in our case computers could calculate thousands of hashes per second which is easy to staple on the accuracy of new transactions. Each time a general ledger transaction is altered, edited, changed, or deleted the balance for the general ledger is distributed and updated to the blockchain network. Therefore, to ensure the speed and integrity of new blocks the term “Peer-to-peer” is being added to this technology. Moreover, since blockchain is a decentralized network used by cryptocurrencies and lacks governing authority, they employ proof of work or the “Miner” to verify the transaction by comparing each account’s balances from one block to another by scanning through the previous hash algorithm. Additionally, on the decentralized network, even though one node encounters a failure the data that has been made will not fail because it is already replicated on every node of the blockchain.

# What is Monero (XMR)?

Monero is a cryptocurrency based on privacy coin that guarantees privacy protection and anonymity. It comes from ‘Monero’, which means ‘Coin’ in Esperanto. And we can call it XMR. It’s Monero’s ticker, short name using in stocks.

It made by Monero Core Team led by Riccardo Spagni using C++. And it was designed to reduce the defects of Bytecoin and make something better.

Monero is the most famous known personal cryptography. Its typical characteristic is anonymity, more specifically Unlinkability & Untraceability. In a nutshell, there are not able to connect two Monero transaction and know the source or purpose.

# History of Monero (XMR)

In 2014, A BitcoinTalk forum User, ‘thankful\_for\_today’ forked the codebase of Bytecoin under the name ‘BitMonero’. He gathered like-minded people and form a team, but they are unsupported and didn't get the attention even though a lot of changes and updates. And they disappeared at some time. Later, a user group led by Johnny Mnemonic decided that the community needed to take over the project and changed its name to ‘Monero’ five days later. Additionally, Monero Core Team, which consists of core development, development, community, research Lab was created. After that, it has continued to develop to this day. For Example, in 2015, they Increased block time to 2 minutes, changed support services and machanisms, and added more features.

Moreover in 2017, they were further enhanced Monero's anonymity by using Bitcoin Core Development, Gregory Maxwell confidential trading algorithm and RingCT theory.

# Why do people invest in the coin?

There are two main reasons which leads people into investing the coin, it’s primary use and its privacy features.

## 4.2. Primary use case

* Peer to peer transaction

Through the utilization of it’s complicated blockchain ledger. Its privacy has led to Monero’s developing in cryptography. Monero is popular amongst a strong base of users who believe in the fundamental principles of privacy, basically conceptualized with the inception of bitcoin.

* Privacy over scalability

Bitcoin sacrifices complete privacy for scalability. But, Monero has placed a higher emphasis on privacy over scalability, focusing on implementing the privacy features before scaling. As a result, Monero emerged as one of the leading privacy cryptocurrencies.

* It’s use is driven by the users

The government officials find Monero’s advanced privacy features as a problem when it comes to tracking criminals. On the contrary the people who use this cryptocurrency see it as a right to transact with each other privately and can’t be violated by centralized authorities. Monero has been chosen the currency of choice on dark-web sites such as former drug marketplace AlphaBay.

This shows it’s use in illicit dealings; however, Monero is used for many reasons too. The reason it’s used is up to the users, as the Monero community said: it’s use is driven by the users themselves, not designed by the technology.

## 4.3. Privacy features

* untraceable transactions
* Ring confidential transaction scheme
* New level of anonymity

Monero’s transactions are untraceable. The transactions using the Ring Confidential Transactions scheme were put on by the Bitcoin developer Gregory Maxwell, and are one of the primary components that allows transaction obfuscation in Monero. It is also a method for making the transaction being sent unclear. Recently, Monero instituted testing for Bulletproofs, which are optimized Pedersen Commitment (Ring CT), where transaction amounts are obfuscated using a short non-interactive zero-knowledge proof. This is a new level of anonymity for the network as Bulletproofs bring the benefits of implementing zero-knowledge proofs but are much more efficient and do not require a trusted setup. And as what the associate professor of University of Montreal, David Décary-Hétu, said: “There are other coins that can provide some level of privacy, but for some reason, Monero is the one that probably has the best crypto and the best means of hiding transactions”.

# Strengths and Weaknesses

## Strengths:

* Multiple keys

There are two types of keys, View and Spend keys. Each type of key has a public and private key, where View key is for the recipient, to get to see the transaction and do no other. For the Spend key, it’s a key used to send transactions.

* Default privacy and anonymity

Monero uses a public ledger, but even though, all transactions are made unclear, complicated, and obfuscated; therefore, it can’t be traced.

* It is fungible

Unlike bitcoin, the coins don’t show where they came, the coins in Monero are unlabeled. For example, fiat money is fungible since you can trade a $10 for two $5, but you can’t do the same with cars, a blue car can’t be traded for a red car since it’s ‘tainted’. The same goes for Monero and Bitcoin. In Bitcoin you can see if the coin has been used illegally before by checking its blockchain if it’s ‘clean’ or ‘tainted’. For Monero the coins aren’t labeled which makes it easily traded and used.

## Weakknesses:

* More popular blockchains

A threat of a more popular blockchain would adopt the privacy technology features.

* Difficult user experience

The design of it is very complicated which makes it difficult for users to use. The user interface is very unfriendly and that is a big disadvantage of Monero. It’s like a Blackberry, a very popular product, with great technology, but a very bad design and hard usage, too many buttons.

* Fewer wallet options

Due to the privacy technology associated with a transaction its hard to find a wallet for it.

# Monero’s Market Price

* No one can predict prices of cryptocurrencies with total certainty, thus it is crucial to understand that the following XMR price predictions serve merely as a suggestion of possible price development and are not intended to be used as investment advice.
* The forecasters have said after looking at Monero’s price predictions in 2022: there’s still hope that the XMR may continue growth until the end of 2022. With the help of reliable technology and the positive dynamics of crypto market, XMR has a big chance to become the most traded cryptocurrency. Many crypto experts believe that XMR will rise in the long term due to persisting optimism that this currency can attract much more attention. At the end of 2022 XMR can have an average rate of $345. Its range can be $330 to $380. According to TradingBeasts, XMR may grow about 110% in the next three years, $360 in the end of 2022 and $500 by the end of 2023, and with this assumption TradingBeasts are confident that XMR has a good growth potential and there’s no reason for it to crash.

Chart, line chart

Description automatically generated

Here is the future predictions in 2023:

Text

Description automatically generatedText

Description automatically generatedTable

Description automatically generated

Table

Description automatically generated

How

# **How does it work?**

In order to provide privacy and anonymity Monero relies on two important concepts which known as the stealth address and the ring signature. So what are these two? In the following section will be illustrated how each of these privacy features are operates.

## Stealth Address

Stealth address allows the sender to generate an one-time public address by combining public view key and public spend key together on behalf of the intent recipient for every transaction. Whereas, on the recipient side they can still use a single public address to receive all the transaction. On the other side, Monero consumers will generate another one-time private view key and a private spend key combined together to see all the associated transaction within their account, also the private key of Monero user is exactly the same as Bitcoin as it is ultilize a key to authorize the payment.

Diagram

Description automatically generated

Source: <https://www.google.com/search?q=stealth+address+&tbm=isch&ved=2ahUKEwiNp7zx-MP6AhXkTPUHHYJnAGoQ2-cCegQIABAA&oq=stealth+address+&gs_lcp=CgNpbWcQAzIECCMQJ1CEDViEDWD9DWgAcAB4AIABkQGIAZEBkgEDMC4xmAEAoAEBqgELZ3dzLXdpei1pbWfAAQE&sclient=img&ei=5cU6Y82gNuSZ1e8Pgs-B0AY&bih=841&biw=1707&rlz=1C1VDKB_enTH1017KH1018#imgrc=8KULEPrSR-lHjM>

## Ring Signature

Ring signature is a concept from general cryptography that refer to a digital signature of a specific group of individuals who consisted of private keys. Implying, whenever the sender attempts to make an XMR transaction their Monero wallet will automatically generate five different keys from the past transaction on the Monero network and combine it with the sender key. Additionally, these keys did not need any particular permission from the owner when it is taken to form a ring. With this algorithm, it is impossible for the third party or hacker to tell whose key was used to sign, which result in making the transaction anonymous.

Diagram

Description automatically generated

Source: <https://www.google.com/search?q=ring+signature+of+the+monero&tbm=isch&ved=2ahUKEwjGldGBhcT6AhXBCIgKHW9aD-kQ2-cCegQIABAA&oq=ring+sign&gs_lcp=CgNpbWcQARgAMgQIIxAnMgQIIxAnMgUIABCABDIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgARQyBtYtCZgny5oAHAAeACAAYYBiAH5CJIBBDAuMTCYAQCgAQGqAQtnd3Mtd2l6LWltZ8ABAQ&sclient=img&ei=ndI6Y4ZTwZGgBO-0vcgO&bih=809&biw=835&rlz=1C1VDKB_enTH1017KH1018&hl=en#imgrc=EAahitzfhDHoYM>

To increase the security of these privacies Monero declared new confidential feature known as the Ring Confidential Transaction or Ring CT in January 2017. Specifically, what it does is to secure and hide the amount of the transaction that are being made on the network.

To sum up, for Monero to become one of the most outstanding private cryptocurrencies is due to these special privacy feature that it consisted of. The stealth address will hide the intent recipient and the ring signature will hide the original sender by manipulating the real key with decoy keys which generated from past transaction of other users. While ring confidential transaction will hide the number of XMR being sent.

# Conclusion

Undeniably bitcoin has been taking the initial step to more private digital currency over few decades, however, since 2014 Monero has shown a significant noticeable advance to the true fungible electronic currency. Since, it obtained the financial anonymity amongst many privacy coins available on the blockchain network. Monero has secured the top rank with their special cryptography and features such as stealth addresses and ring signatures.

Additionally, the community that runs Monero value privacy as a fundamental principle. It is true that mostly Monero users are inspired more by values than the monetary benefit. With a determined community and regular modifications anticipated for the future, Monero appears to have staked out a role in the crypto markets, and it will keeps growing.

# **References:**

1. <https://www.getmonero.org/get-started/what-is-monero/>
2. <https://www.cryptoeq.io/corereports/monero-abridged>
3. <https://www.analyticsinsight.net/monero-price-prediction-is-it-still-a-good-option-why-tama-looks-hotter/>
4. <https://ambcrypto.com/predictions/monero-price-prediction-2023>
5. <https://www.youtube.com/watch?v=cjbHqvr4ffo>
6. <https://www.youtube.com/watch?v=M6kxtiKKyMQ>
7. <https://www.youtube.com/watch?v=SSo_EIwHSd4>
8. Ring Signature: <https://www.youtube.com/watch?v=zHN_B_H_fCs>
9. Bitcoin Vs Monero's img: <https://www.google.com/url?sa=i&url=https%3A%2F%2Fcoinsutra.com%2Fmonero-cryptocurrency%2F&psig=AOvVaw0W0jbYpisxdkbWGuq8-xY6&ust=1664610275478000&source=images&cd=vfe&ved=0CAwQjRxqFwoTCMDkjNeCvPoCFQAAAAAdAAAAABAO>
10. <https://www.google.com/search?q=monero&tbm=isch&tbs=rimg:CRMmKfP4C8A4YcGIHoYqYpLs8AEAsgIMCgIIABAAOgQIABAA&rlz=1C1VDKB_enTH1017KH1018&hl=en&sa=X&ved=0CB0QuIIBahcKEwjA5IzXgrz6AhUAAAAAHQAAAAAQaA&biw=835&bih=809#imgrc=k-9_3HYHI_24yM>
11. <https://www.getmonero.org/get-started/what-is-monero/>
12. <https://www.cryptoeq.io/corereports/monero-abridged>
13. <https://www.analyticsinsight.net/monero-price-prediction-is-it-still-a-good-option-why-tama-looks-hotter/>
14. <https://ambcrypto.com/predictions/monero-price-prediction-2023>
15. <http://wiki.hash.kr/index.php/%EB%AA%A8%EB%84%A4%EB%A1%9C>