# WOWNote v 6.9

RootInit
init.cx

May 12, 2023

## 1 Introduction

"Monero"[1, 2, 3] has been a successful derivative of the CryptoNote[4] proof-of-concept cryptocurrency and has become the most popular privacy focused p2p digital currency. Both digital privacy advocates and the general cryptocurrency using public have come to appreciate its private and anonymous transactions and ASIC resistant proof-of-work algorithm. Today, the Monero user base is growing at a steady pace[5]; users are attracted to the low transaction fees and enhanced anonymity provided by its "transaction mixing" and "stealth addresses"[6] and merchants value its predicted emission and fast transaction speed[†1] due to the two-minute block time. Monero has effectively proven that electronic cash transactions can be as, or more, private as paper money with a much higher degree of fungibility[†2] and with easily verifiable proof of payment[8].

Unfortunately, Monero suffers from overwhelming practicality and over-seriousness. "Wownero,"[9] a digital currency forked from Monero[3, 10] seeks to solve this problem. Wownero is a memecoin primarily targeted toward transactions such as betting on snail races and tipping meme creators, but also a fully functional digital currency capable of being used in any financial transaction[9]. Because of Wownero's less critical[citation needed] nature the community enjoys less stringent testing and validation requirements resulting in faster release of new features, lower block confirmation requirements, and much more playful presentation and branding[11].

This document is intended to serve as an addendum to the existing Wownero white paper (`wownero.org/whitepaper.pdf`) and attempts to provide a brief synopsis of the core technologies Wownero (and Monero) utilize. A brief history of Wownero and a brief synopsis of core technologies will be provided. The Wownero blockchain, Proof-of-Work algorithm, and privacy enhancing features will be summarized in respective sections.

While I have made a strong effort to provide accurate information, my lack of expertise in cryptography and the level of abstraction required to sufficiently condense the material may result in inaccuracies.

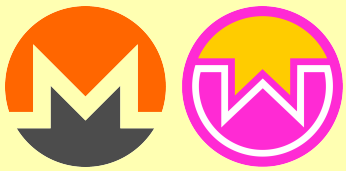

Figure 1: Monero (left) and Wownero (right) Logos

[†1] **Transaction speed** is conditional on the number of confirmations and the network congestion level.

[†2] **Fungibility** is the attribute of being indistinguishable from one another[7]. For instance transparent blockchains result in "tainted" or "dirty" currency as coins are distinctly identifiable.

## 2 Wownero History

Wonero is a Monero software fork created by John Winter Murphy ("jwinterm")[12] in response to, and with the goal of beating, "MoneroV"[13]. Wownero started as a casual discussion between John Murphy and his friend, Carty Sewill, about a hypothetical meme coin with some of the same features as MoneroV but as a fully legitimate and functional non-scam coin[13].

MoneroV, announced February 2018, was another fork of Monero with the main defining feature of having finite supply and no tail emission[14]. In addition to the software, MoneroV also forked the Monero blockchain giving all existing Monero users 10 "XMV" for each "XMR"[†1] they held. Because MoneroV presold coins to investors, claimed a large percentage of coins as a "dev tax," it is widely believed to have been entirely a scam[15, 14].

Wownero was successfully launched on April 1st 2018 achieving their goal of launching ahead of MoneroV[13]. Carty Sewill designed the original logo (Figure 1) and artwork used for the project[13]. Like MoneroV, Wownero featured a limited max supply of approximately 10x the amount of Monero coins, but without any scammy pre-mined coins or ICO[†2] and utilized its own unique Genesis block[†3] making it an entirely separate cryptocurrency from Monero.

Wownero was described by jwinterm in a personal communication as "to Monero what Dogecoin is to Bitcoin" (2023 [13]). True to this claim, Wownero, has predominantly been used by a largely meme based community and, like Dogecoin, Wownero is categorized by many as a "shitcoin" though some may (sarcastically) disagree as shown in `Figure 2`.


Figure 2: A meme facetiously disputing Wownero's status as a "shitcoin."
Image source `suchwow.xyz` credit *"trichom"*

A strong and active community has formed around Wownero and developed a full software ecosystem to make Wownero a more functional and user-friendly coin. Community projects include:

- GUI, TUI, and VR wallets[16].
- Blockchain explorers[17].
- Informational websites[9, 11].
- Promotional memes, artwork, and stickers[18].
- A Discord server, subreddit, and dedicated forum[19].
- A privately hosted Git server for software development collaboration[10].

[†1] **XMR** is the common shorthand used for Monero similar to Wownero's abbreviation of "WOW".
[†2] **ICO** or Initial Coin Offering refers to a presale of a token offered to investors before launch
[†3] A **genesis block** is the initial block in the blockchain.

Monero and Wownero have always had trouble getting listed on most major exchanges as such exchanges generally avoid privacy coins both for fear of future regulatory legislation, and because centralized exchanges (which require ID verification) are not likely to be popular with the privacy coin demographic. Wownero has been primarily traded through "TradeOgre" and has reciently been listed on various exchanges including "MajesticBank," "LocalMonero," and "Agoradesk" [13]. The Wownero community is optimistic regarding near future listings on other exchanges.

# 3 Blockchain

A blockchain is a decentralized and distributed digital ledger that records all transactions[7]. This core technology that makes cryptocurrency possible was originally proposed in 2008 for "Bitcoin" by a person or group under pseudonym "Satoshi Nakamoto"[20]. The blockchain is stored on a network of nodes (computers running the blockchain's daemon[†1] software) with new transactions and blocks being propagated via a peer-to-peer (P2P) protocol[21]. An LMDB (Lightning Memory-Mapped Database) is used for both Monero and Wownero blockchain data storage[3, 10].

## 3.1 Transaction Process

When a transaction is initiated it is broadcast to the network and stored in each node's transaction cache, also known as a "memory pool," if the transaction passes validation checks[21]. These transaction validation checks typically check factors such as confirming the money exists, it has only been sent once, it is being sent by the address which owns it, the transaction received amount equals the input, and the transaction is correctly formatted[2]. "Miner" nodes attempt to create a new "block" from this transaction queue and when successful a new block is added to the blockchain[21] containing a list of hashed[†2] transactions.

Most blockchains enforce a multiple confirmation requirement before received funds can be used in a transaction again ("unlock time")[23]. This prevents double-spend and similar attacks by making the transaction more difficult to reverse as an attacker would need to overwrite multiple blocks on the blockchain. This becomes exponentially more difficult to do as more confirmations are added. Monero requires 10 confirmations[24] before funds are unlocked while Wownero requires only 4 confirmations[10]. For CryptoNight protocol blockchains, like Monero and Wownero, it also serves to prevent people from making multiple transactions at the same block height which may compromise ring signature based transaction obfuscation.

It should be noted that for small transactions it may not be necessary to wait for the full blockchain confirmations and in some cases just the validated initial broadcast may be sufficient to approve a sale.

## 3.2 Blocks

Blocks are created by miner nodes and the "block time" (average time interval between block creation) is controlled by adjusting the proof-of-work algorithm difficulty against

[†1] A **Daemon** is a program which runs as a background service and communicates with other nodes.

[†2] **"Hashing"** refers to the use of a mathematical algorithm to produce a numeric value that is representative of input data[22].

the hashrate[†1] of the network[25, 23]. The *average* block time for Monero is pre-set at 2 minutes[1] as opposed to 5 minutes for Wownero[10].

In addition to a list of hashed transactions, each block will contain header information and a new hashed "coinbase transaction" which rewards the miner for creating the block[26, 21]. The block header data will include a hash of the previous block ensuring that the blockchain must remain a sequential and complete "chain"[2, 23]. This ensures that previous block alteration or removal is impossible without replacement of all subsequent blocks[2].

Because it is possible for more transactions to occur between blocks than would fit within the block size limit,[†2] transactions may remain in the queue until a later block. To prevent transaction spam, Monero has a dynamically calculated minimum fee on all transactions, however, if a sender needs to ensure their transaction is added to the earliest possible block they can raise the fee above the minimum[2]. Because the transaction fee is given to the miner who creates the block, transactions offering a higher fee take priority in the queue. To prevent miners from producing unnecessarily large blocks (such as by padding to max size with zero value transactions) an excessive block size penalty is subtracted from the block reward[4]. This balances with the transaction fee reward to create a stable equilibrium of average block sizes.

### 3.3 Outputs

Units of a cryptocurrency can be split into very small fractional amounts though there is a finite limit called "atomic units." For Monero the atomic unit size is `0.000000000001` XMR or one "piconero"[7].

Because it would be impractical to track the movement of each of these atomic units individually, an "output" and "input" based system is used instead[20]. These outputs combine amounts of currency into single units, similar to how a $10 bill combines the value of 1000 pennies[27]. If no single output is large enough to cover a transaction they can be combined, however there are always at most two outputs per transaction comprising the payment amount and the "change" returned to the sender[20]. The one drawback to this system is that, as outputs are "locked" while a transaction is taking place and pending sufficient confirmations, a user lacking multiple outputs will be unable to send another transaction until the first one is fully confirmed. This is a rare issue however as almost all frequent users will have multiple outputs and the input output system is managed invisibly to the end user by the wallet software[27].

### 3.4 Emission

Both Monero and Wownero had no premine, instamine, or presale of any kind to ensure a fair and even distribution[1, 9]. Monero had irregular emission with block rewards steadily decreasing until they reached a flat 0.6 XMR block reward which will continue in perpetuity[28]. Wownero took a different approach with a total supply of 184,467,440 coins to be mined over 50 years and no tail emission[10]. This may be an issue long term as without an incentive to mine the security of the network could be reduced[2].

[†1] **Hashrate** is a measure of the computational power of a cryptocurrency network.

[†2] **Block size limit** is a pre-set but not hard-coded parameter[4]. Note: Both Monero and Wownero have an adaptive block size limit calculated dynamically[24].

### 3.5 Blockchain Upgrades

Both Monero and Wownero utilize a "hard fork" mechanism to implement scheduled software upgrades into their networks[10, 3]. A hard fork occurs when a majority of nodes no longer accept older versions of the blockchain[29]. In the case of Monero and Wownero this has only occurred due to official changes to implement new features such as new proof-of-work algorithms or implementation of "bulletproofs"[3].

In a hard fork the blockchain becomes split into an old and new version of the blockchain[29]. Because of this it is possible for an official hard fork to be rejected by nodes which do not accept the changes which leads to a split. This has happened with other cryptocurrencies such as "Etherium Classic" which was formed in 2016 due to differences of opinion on whether a smart contract hack should be rolled back[30]. Monero and Wownero have prevented this from occurring (so far) through clear communication, ensuring there is broad favorable consensus regarding an upgrade before an update is released[31]. Because only changes accepted almost unanimously are implemented a "non-contentious hard-fork" occurs in which the old blockchain dies off due to a lack of nodes running the older version.

Some changes, referred to as "soft forks", can occur while remaining backwards compatible with the original blockchain. These changes require only miner nodes to update, and normal nodes remain unaffected[32].

To the end user all upgrades require only a simple software update of the client software[31].

### 3.6 Consensus

Because of the decentralized, peer-to-peer, node based nature of cryptocurrency, maintaining consensus between the distributed nodes of the network is of critical importance. A majority of nodes must agree on the same blockchain, block creation structure, and transaction rules in order to prevent malicious actors from exploiting the network. This is achieved through the use of consensus algorithms, which enable the nodes of the network to agree on a shared version of the blockchain.

To ensure every node uses the same blockchain, the chain with the highest cumulative difficulty[†1] is considered to be the legitimate version[2]. This ensures that, in order to force an alteration to the transaction history, an attacker must create a fork of the blockchain with higher total difficulty than the original. This would in almost all cases require the attacker to control over 50% of the total network mining hashrate to grow faster than the main chain[2].

Both Monero and Wownero utilize a proof-of-work algorithm (described in a later section) to maintain block consensus[1, 9]. Other cryptocurrencies may use proof-of-stake (in which block validators are chosen based on their stake in the network[33]), proof-of-capacity (in which miners prove storage capacity instead of computational power), proof-of-authority (in which validators are chosen based on their reputation or identity), or any other algorithm.

[†1] **Cumulative difficulty** refers to the total difficulty required to mine every block in the chain.

# 4 Proof-of-Work

"Proof-of-work," or PoW, is a type of consensus algorithm used in blockchain networks since Bitcoin[23]. In this concensus algorithm transactions are validated and new blocks are added to the blockchain through a computational puzzle that must be solved by miners[20]. While PoW has some drawbacks, such as high energy consumption, it remains one of the most widely-used and secure consensus algorithms in blockchain technology[33].

## 4.1 Early Proof-of-Work

Not all proof-of-work algorithms are equal, however. The first proof-of-work algorithm used was a double SHA-256[†1] based function used in Bitcoin[20]. This was intended to result in an egalitarian "one-CPU-one-vote" system[20].

Unfortunately, and likely unforeseen to Satoshi Nakamoto, the explosion of Bitcoin's popularity resulted in bitcoin mining ASICs[†2] being developed and advances in GPU compute technology made GPUs much more efficient at mining blocks. Because of this CPU mining was rendered uncompetitive and mostly impractical giving a massive advantage, by orders of magnitude, to owners of ASIC mining rigs and GPU clusters[34].

## 4.2 CryptoNight

The CryptoNote protocol on proposed an algorithm, later dubbed "CryptoNight" which was intended to "close the gap between CPU (majority) and GPU/FPGA/ASIC (minority) miners"[4]. This algorithm worked by utilizing a memory bound function which would be most efficient on CPUs due to the large L3 cache modern CPUs possess[4]. The 2 Mb of memory required by the CryptoNight algorithm was thought to be extremely difficult to develop an ASIC around and GPU processors do not have internal cache but rather rely on significantly slower memory on a separate chip[4].

Ultimately CryptoNight failed in its efforts to provide ASIC resistance and ASICs capable of running the CryptoNight algorithm were developed[35]. Coins utilizing CryptoNight were forced to either accepted ASIC mining or switch to a different PoW algorithm.

Choosing the latter option, the Monero Research Lab upgraded the CryptoNight algorithm to v7, v8, and "CryptoNight-R" though all of these modifications were eventually defeated by improvements in ASIC technology[35]. The CryptoNight-R algorithm introduced a novel change of randomized integer math which was *temporarily* very effective but only used in Monero between March 9, 2019 and November 30th 2019 as a new superior algorithm was internally developed specifically for use with Monero[3].

## 4.3 RandomX

Based on the same core principle of introducing randomness as CryptoNight-R, the Monero Research Lab developed an entirely new Proof-of-Work algorithm called "RandomX" with much stronger ASIC resistance while retaining the same private hashing as CryptoNight[34]. Rather than rely on any single specific attribute of CPUs (such as cache size), RandomX instead is based on execution of random code inside a virtual machine[25]. RandomX has two modes with different memory requirements. A *light* mode requiring only 256 MiB of memory (intended for normal nodes) to use for verification and a *fast* mode

[†1] **SHA-256** is a cryptographic hash function used for data integrity and authenticity verification in various computer security applications.

[†2] An **ASIC** or Application-Specific Integrated Circuit is a computer chip that is designed to perform a specific function with high speed and efficiency due to its specialized nature[22].

requiring 2080 MiB of memory (intended for miner nodes)[25]. Because of the *random* nature of the algorithm, only general purpose processors are capable of efficiently running it rendering ASICs theoretically impossible[34]. Additionally, the high memory requirement for mining makes the mining software easily detectable by antivirus programs, low memory IoT devices unable to mine at all, and prevents web applications from mining covertly. These restrictions should reduce botnet[†1] mining, making it much harder for a malicious actor to obtain a high percentage of hashrate illegitimatly[36].

Monero implemented the RandomX algorithm on November 30th 2019 as part of v12 update[3].

### 4.4 Wownero

Wownero likewise implemented a series of ASIC resistant POW algorithms including a slightly modified version of CryptoNight-R on the October 6th 2018 update codenamed "Cool Cage"[10]. They also briefly used a pseudorandom function "CryptoNight/WOW" from February 19th 2019 until the implementation of, RandomX based, "RandomWOW" which, due to lower testing requirements, they were able to implement ahead of Monero on the June 14th 2019 codename "F For Fappening" hard fork[10].

RandomWoW's differs from RandomX in that it uses a scratchpad (workspace memory)[36] size of only 1 MB compared to RandomX's 2 MB scratchpad size[10]. RandomWOW also has a limit of 16 chained VM executions per hash to further increase program compilation difficulty for GPUs and ASICS[10].

Wownero took an additional step to promote decentralization through preventing public mining pools by requiring "Miner Block Header Signing" which requires miners to sign blocks with their private key[10, 13]. Because private keys cannot be shared without giving away full access to your wallet, this rendered Wownero solo and private pool mining only as of the July 4th 2021, "Junkie Jeff," update[10].

## 5 Privacy Enhancing Features

Wownero is a privacy respecting memecoin[9] and, as such, aims to provide users with strong anonymity and confidentiality. To achieve this, Wownero employs a range of privacy-enhancing features, including stealth addresses, ring signatures, RingCT, Dandelion+, and integration with TOR and I2P networks. The majority of these features were upstream inherited from Monero[10, 3], but the Wownero developers have implemented some tweaks and modifications of their own.

### 5.1 About Monero Addresses

Conventional Bitcoin-like cryptocurrency addresses use a single key pair, similar to those used in *RSA encryption*, but based on elliptic-curve cryptography[†2] [2] rather than integer-factorization cryptography. Bitcoin wallet keys are generated using the "Elliptic Curve Digital Signature Algorithm" (ECDSA)[37]. The key pair consists of a public key ($K$) and a private key ($k$) and, as is standard for asymmetric encryption, the public key is distributed freely (in the form of a derived address) while the private key must be carefully protected.

[†1] A **botnet** is a network of infected computers that are remotely controlled by a single attacker for malicious purposes.

[†2] **Elliptic-curve cryptography** (ECC) uses the algebraic structure of elliptic curves over finite fields to perform cryptographic operations using smaller keys compared to conventional methods with the same level of security.

A standard Monero wallet address requires *two* public-private key pairs. A view key $(K^v, k^v)$ and a spend key $(K^s, k^s)$[38]. This double key pair system is a feature of CryptoNote coins and allows compartmentalization of access. For example, the view key can be shared to allow another party to audit incoming transactions and current balance without giving them the ability to send coins[7]. Monero addresses are generated using the "Edwards25519 Elliptic Curve" signature scheme[39].

I was curious what this curve looked like and plotted the positive and negative solutions to Curve25519 function in `Figure 3`. I do not believe this provides any greater understanding of the underlining mathematics, but now we know that it bears a striking visual similarity to a "stick drawing" of a fish.

$$y^2 = x^3 + 486662 * x^2 + x \implies \begin{cases} y = +\sqrt{x^3 + 486662x^2 + x} \\ y = -\sqrt{x^3 + 486662x^2 + x} \end{cases}$$

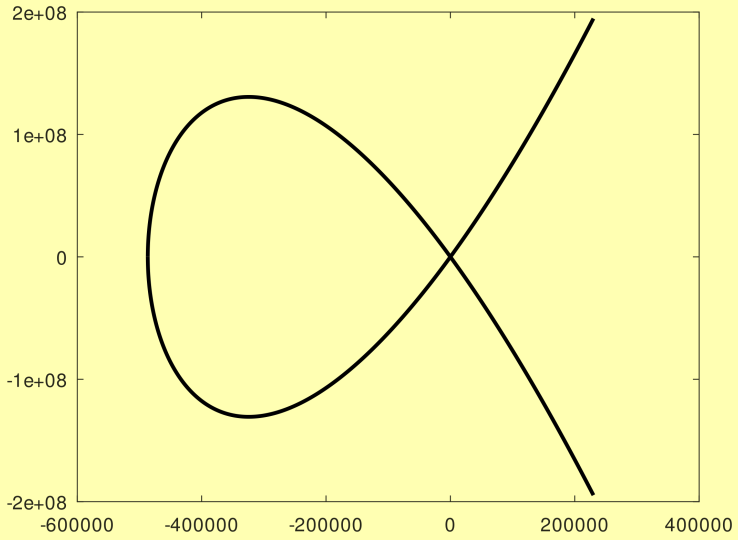


Figure 3: The Edwards25519 Elliptic Curve
Image credit: *RootInit*

In addition to the public spend and view keys, Monero and Wownero addresses also contains a "network byte," which makes the address network type identifiable, and a checksum to make mistyped addresses easily detectable[38]. The complete anatomy of a Monero address is as follows:[38]

1. A 1 byte network byte located at index 0.
2. A 32 byte public spend key located at index 1.
3. A 32 byte public view key located at index 33.
4. The first 4 bytes of a hash of the rest of the key located at index 65.

Most cryptocurrencies use base58 encoding, originally developed for Bitcoin[2], for the final address. Base58 is similar to base64 but omits the characters `I, O, l, 0, +, and /` to avoid ambiguity when read[38]. Monero addresses use a modified version of base58 which performs the encoding in 8 byte blocks and pads the final block with 1s[38]. This produces a fixed size output ensuring all addresses are of the same length.

An example final Monero address after base58 encoding into a 95 character string:
`84DwgAEGE3NBeocw33eoj8ZjomhVYTQEuUKew8yvYJMxgfdDU9Y91BBgtvAX6dJ3PddVJRwe3trRcNku3fMEHc3A7XYmDbC`
A main chain standard Monero address will always have an *4* or *8* as the first character[†1].

An example final 97 character Wownero address:
`WW33MLqvVUJZxDs4WkqgHn4SkTdKFn6hb2VAN8MBvENjfu2iug6p3CSJPDsVpggtEDZd715Xj4zy2jabweCV6WmY2kF6NMuZE`

It appears that the reason for the longer address is due to the use of two bytes to represent the network. Because of this, every standard main chain Wownero address will start with *Wo* or *WW* at the cost of a pre-encoding address size of 70 bytes in length *not* 69.

## 5.2 Stealth Addresses

"Stealth addresses," also known as "one-time addresses,"[2] allow the recipient address written to the blockchain to be a unique single-use address that cannot be linked to the original address [40]. Without stealth addresses it would be possible for an observer monitoring blockchain transactions to link transactions through heuristic pattern analysis of received transactions. For instance, linking a purchase of Monero via credit card to all other received payments would be trivial and completely de-anonymize the user.

The procedure for generating a stealth address was first described in the CryptoNote white paper[4] and has become one of the core Monero and Wownero privacy enhancing technologies[7].

### 5.2.1 Stealth Address Cryptography

An example usage of a stealth address in a transaction between a sender, "Shinji", and a recipient, "Rei", will be explained[2, 4].
**[Sender] Shinji's Steps**

1. Shinji initiates a Wownero transaction sending an amount, $a$, addressed to an address Rei provided.
2. The wallet software separates the address into Rei's public view and send keys $(K_R^v, K_R^s)$
3. A random number $r$ is selected $(r \in_R \mathbb{Z}_l)$[†2†3].
4. A one time address $K^o$ is calculated as

$$K^o = \mathcal{H}_s(rK_R^v, a)G + K_R^s$$

   [†4†5]
5. The transaction is sent to the network with the one-time address $K^o$ as the recipient along with the value of $rG$.

**[Receiver] Rei's Steps**

1. Rei's wallet checks every transaction using her private view key. $k_R^v$ and
   (a) Multiplies her private view key $k_R^v$ by $rG$ $(rK_R^v = k_R^v rG)$

[†1] It is entirely coincidental that the example Monero address starts with 84
[†2] The $R$ indicates random selection from the set
[†3] $l$ indicates exclusion of the Curve25519 infinity points from the set
[†4] $G$ refers to the Ed25519 "generator point" on the curve which is the first point after infinity.
[†5] $\mathcal{H}_s$ refers to a one-way cryptographic hash function.

(b) Derives the original public send key $K_R'^s$ with

$$K_R'^s = K^o - \mathcal{H}_s(rK_R^v, a)G$$

(c) Transactions in which the derived send key match Rei's public send key ($K_R'^s = K_R^s$) are addressed to Rei.

2. Having identified the transaction, the public and private spend keys for the output can be calculated.

$$\begin{aligned} K^o &= \mathcal{H}_s(rK_R^v, a)G + K_R^s \\ &= (\mathcal{H}_s(rK_R^v, a) + k_R^s)G \\ k^o &= \mathcal{H}_s(rK_R^v, a) + k_R^s \end{aligned}$$

Rei can now spend the received amount as desired using the spend key pair $(K^o, k^o)$ and the amount is added to his balance by the wallet software.

Stealth addresses can be used optionally with non CryptoNote based coins, including Bitcoin, if both parties wallets support the feature[40]. Monero and Wownero *require* their use and their respective wallets perform this automatically and transparently[7].

### 5.2.2 View Tags

As of the Monero v15 update on August 13, 2022[3] and Wownero's very recent April 1st update codenamed "Kunty Karen"[10], a new noteworthy piece of data was added to blocks. "View Tags" are 1-byte "tags" added to each transaction using a shared secret generated by the sender using the address provided to them by the recipient[41]. Because all Monero transactions hide the recipient, wallet synchronization requires each transaction to be cryptographically decoded as described above to determine if the transaction is addressed to you.

The addition of view tags reduces sync times by $> 40\%$ by reducing the number of transactions which have to be fully checked (as shown in 5.2.1 Receiver step 1) down to only 1/265th the total transactions[41].

## 5.3 Subaddresses

While Stealth Addresses protect you from 3rd parties linking transactions together, the *sender* must necessarily know the address to which they are sending funds. "Subaddresses" allow a recipient to create a new publicly disclosable address for a transaction or category of transactions[42] allowing them to hide their primary address from even the person sending them funds[7].

The same functionality could be achieved by using multiple wallets, and for maximum unlinkability this remains the best option. Subaddresses exist to provide a convenience advantage over creating multiple wallets as they require a user to manage only a single seed phrase and keys[42].

For an example of why this is necessary, suppose Rei utilizes the same address both to receive payments from an e-commerce business website and for personal use. Rei wins a bet and receives a personal payment from Shinji. By random chance Shinji is a customer of Rei's e-commerce site and recognizes the address revealing Rei as the operator of the site.

### 5.3.1 Subaddress Cryptography

To prevent this Rei creates a subaddress to receive the funds. Both Monero and Wownero wallets make this very easy and the address is created as follows[2]:

1. Rei's public view and send keys are represented by $(K_R^v, K_R^s)$. The new $i^{\text{th}\dagger 1}$ subaddress keys will be represented by $(K_R^{v,i}, K_R^{s,i})$
2. Rei's subaddress is generated from his main address

$$K^{s,i} = K^s : \mathcal{H}_s(k^v, i)G$$
$$K^{v,i} = k^v K^{s,i}$$

So,

$$K^{v,i} = K^v(k^s + \mathcal{H}_s(k^v, i))G$$
$$K^{s,i} = (k^s + \mathcal{H}_s(k^v, i))G$$

[2]

The generated subaddress $(K_R^{v,1}, K_R^{s,1})$ can then be used in transactions just like a primary address. As with a primary address, a stealth address will be generated from it, substituting $(K_R^{v,1}, K_R^{s,1})$ for $(K_R^v, K_R^s)$ as

$$K^o = \mathcal{H}_s(rK_R^{v,1}, a)G + K_R^{s,1}$$

Rei's wallet will identify the received transaction, derive the transaction public send key (which will be the subaddress key $K_R^{s,1}$), and extract the one time keys for the transaction same as described in the 5.2.1 transaction.

### 5.3.2 Other Functionality

Subaddresses are useful beyond privacy protection. For instance by providing a different subaddress for every expected payment it becomes easy to identify the purpose of a received payment[42]. For instance providing a different address to each of multiple tenants leasing a building would allow you to know who has paid their rent. Subaddresses can also be used for more general categories rather than individual senders. For instance by categorizing into "accounts" for mining, work, personal, etc. or to wallet for separate business enterprises while retaining individual auditability[42].

## 5.4 Ring Signatures

As stealth addresses and subaddresses ensure the anonymity of the recipient, "ring signatures" conceal the identity of the sender[7]. Ring signatures, are a well established cryptographic Schnorr-like[43] signing scheme[44]. They are special in that they allow any member of a group of users to cryptographically sign a message while protecting the identity of the individual signer[44]. They were developed by a group including Rivest and Shamir (well known for the **RS**A encryption scheme) and were first introduced at ASIACRYPT in 2001[44]. Ring signatures are a core part of any CryptoNote coins unlinkability guarantee, including Monero and Wownero[4, 7, 10].

Ring signatures in Monero utilize a "ring" set of public keys, one of which must belong to the signer and the rest of which are used only as decoys. The primary feature of ring

[†1] $i$ represents the index of the subaddress. E.G. {1,2,3...}

signatures over conventional "group signatures" is that it should be infeasible to determine which ring member was the actual signer[2]. Under the CryptoNote protocol a random subset of other users public keys are used along with the transaction sender's key to form a ring[35].

For Wownero, the ring size is set to 22, which offers a *theoretically* higher level of mixing compared to Monero which requires a ring size of 16[†1][7]. This helps balance out Wownero's lower volume of transactions, users, and slower block time. While 16 or even 22 possible other addresses may not seem like a lot, this transaction mixing occurs for every transaction and over time the list of who may have transacted with any particular address will include almost everyone on the network[45].

### 5.4.1 Ring Signature Cryptography

The procedure for signing and verifying a message $m$ with a "Spontaneous Anonymous Group" (SAG) ring signature $\mathcal{R} = \{K_1, K_2, \ldots, K_n\}$ is as follows
**Transaction Signing**

1. A random number $a$ is selected ($a \in_R \mathbb{Z}_l$).
2. Multiple decoy responses $r$ of size $n$ = ring size $-$ 1 are selected from a pool of addresses ($r_i \in \mathbb{Z}_l$ for $i \in \{1, 2, \ldots, n\}$)[†2].
3. A challenge $c_{\pi+i}$ is calculated for the actual signer $i$ [†3][†4]

$$c_{\pi+1} = \mathcal{H}_n(\mathcal{R}, m, [aG])$$

4. Challenge values are calculated for each decoy response $i \in \{1, 2, \ldots, n\}$

$$c_{i+1} = \mathcal{H}_n(\mathcal{R}, m, [r_i G + c_i K_i])$$

5. The real response value $r_\pi$ is defined such that $a = r_\pi + c_\pi k_\pi \pmod{l}$
6. The signature $\sigma(m)$ is a tuple of the previously found values $\sigma(m) = (c_1, r_1, \ldots, r_n)$

The final complete ring signature consists of the signature $\sigma(m)$ and the full ring $\mathcal{R}$. [2]
**Transaction Verification** The signature $\sigma(m)$ can be proven by network nodes to correspond to a valid private key in ring $\mathcal{R}$

1. We iterate over the set of ring entries $i \in \{1, 2, \ldots, n\}$ replacing $n + 1 \to 1$ as

$$c'_{i+1} = \mathcal{H}_n(\mathcal{R}, m, [r_i G + c_i K_i])$$

2. Any transaction in which the last term calculated is equivalent to $c_1$ is proven valid ($c_1 = c'_1$). [2]

### 5.4.2 Ring Signature Implementations

Several variations of the described SAG ring signature have used for both Monero and Wownero in addition to the previously described SAG signature[2]. At present time, both Monero and Wownero use Concise Linkable Spontaneous Anonymous Group (CLSAG) signatures as of October 2020[7, 10] which have provided a 10-25% transaction size reduction[7]. Here is a full list of signature schemes Monero has utilized [2]

[†1] Monero formerly used a ring size of 11, but this was changed to 16 as part of the v15 update[3].
[†2] $i$ refers to the index of the decoy response public key
[†3] $c$ is a created challenge which can only be proven using the private key.
[†4] $\pi$ is an index referring to the actual signer's public key $K_\pi$ in the ring $\mathcal{R}$.

1. Spontaneous Anonymous Group (SAG)
2. Back's Linkable Spontaneous Anonymous Group (bLSAG)
3. Multilayer Linkable Spontaneous Anonymous Group (ML-SAG)
4. Concise Linkable Spontaneous Anonymous Group (CLSAG)

## 5.5 RingCT

"RingCT", or Ring Confidential Transactions[46], extends the ring signature protocol to also keep transaction *amounts* private[7]. Much as stealth addresses and ring signatures hide the identity of transaction participants, RingCT obfusicates the amount of funds sent[7]. RingCT is build on Torben Pedersen's 1991 "Pedersen commitment" cryptographic scheme which is used to verify a secret's authenticity without disclosing any information about the secret[47].

The feature was added to Monero in the January 2017 v4 update and has been required since September of the same year. Updates have since been made to the protocol such the 2018 v8 and 2022 v15 updates which implemented improvements to the "Bulletproofs" validation protocol[3]. Wownero has utilized RingCT since launch with similar progressive updates upstreamed from Monero[10].

The signing process of a transaction using RingCT follows the steps outlined in the Ring Signature section with some additional steps for handling the transaction amounts. RingCT essentially creates a separate Penderson commitment for each member of the ring and only the holder of the recipients private key is able to discern the actual amount transfered[46]. For RingCT, two ring signatures are combined using Schnorr signatures[43] (later replaced by "Borromean ring signatures"). One of these is necessary to prove the sum is 0 and the other is used to prove the outputs are positive numbers[7]. To all external observers all transactions appear to be a commitment of 0 funds. Validation is done by confirming that all of the transaction's outputs are greater than zero using a range proof and proving that the sum of all outputs is zero (funds were neither created nor lost)[46].

### 5.5.1 Bulletproofs

The double ring signature scheme required for RingCT unfortunately resulted in a large transaction size and slow validation. This has been mitigated through the use of a new type of range proof called "Bulletproofs"[48]. Bulletproofs are much more efficient type of range proof and validation of a large data set generates a comparatively small proof which grows only logarithmically as the data size increases. Bulletproofs also have the ability to prove all transaction amounts at once without individual proofs of each output[7].

Bulletproofs were added to Monero in the v8 update on October 18th 2018[3] after a thorough audit process by three cryptography auditing organizations, *QuarksLab* and *Kudelski Security* and a third which requested to be kept unnamed[7]. Wownero's early Bulletproof implementation in the April 24th, 2018 "Busty Brazzers" update[10] ahead of the full audit may have helped to validate the bulletproofs implementation before addition to Monero.

Since implementation of bulletproofs Monero's average transaction size has decreased by over 80% which has been reflected in the transaction fees[7].

An improvement to the Bulletproofs protocol called "Bulletproof+" was later implemented to Monero as part of the September 13th, 2022 v15 update[3]. Bulletproofs+ provide even more efficient range proofs for RingCT transactions with even smaller, faster to generate, and faster to verify proofs[49]. This further reduces the transaction size and the computational burden on network nodes, making it possible for the blockchain to process

more transactions without sacrificing security or privacy. For a ring size of 16, transactions are 10.8% faster vs the original Bulletproofs[49]. This upgrade was also integrated into Wownero ahead of Monero on July 4, 2021, in the "Junkie Jeff" update.

### 5.6 Networking Privacy

Monero and Wownero's commitment to privacy extends past the blockchain. Networking protocols are also utilized to hide which IP address was used to send a transaction and even hide the usage of the currency entirely. These protocols can be integrated into the blockchain node software or a separate user-configured optional addition.

#### 5.6.1 Dandelion++

The nature of peer-to-peer node communication already makes discerning a transactions originating IP address quite difficult and would require an attacker to control a majority of nodes on the network[50]. Dandelion++[51] is a privacy-enhancing feature which makes this already difficult attack virtually impossible even for a government level attacker. As the name implies, Dandelion++ is an upgraded version of the original 2017 Dandelion protocol which makes it more effective in cases in which many nodes disobey the protocol or do not use the Dandelion protocol at all[51].

In an IP address identification attack carried out on network which uses conventional diffusion propagation *without* Dandelion++ an attacker who controls many nodes on the network can monitor the order in which each node receives a transaction from one of their peers and deduce where the transaction originated based on the timing in which each node receives the transaction. If the attacker is able to successfully determine which node first encountered the transaction they can find the IP address which forwarded it to that node[50]. By identifying the originating IP address, transactions can be linked despite features such as stealth addresses, subaddresses, or even entirely separate wallets. Against a state level attacker the IP address can be linked to the identity of the sender by the sender's internet service provider[50].

Dandelion++ mitigates this and obfuscates the diffusion order by propagating transactions in two phases determined by preset "epoch" intervals. Every epoch the node chooses whether to act as a "Stem" relay node or "Fluff" diffusion node until the next epoch, depending on a pseudo-random factor computed from a hash of the node identity and the epoch number[51].

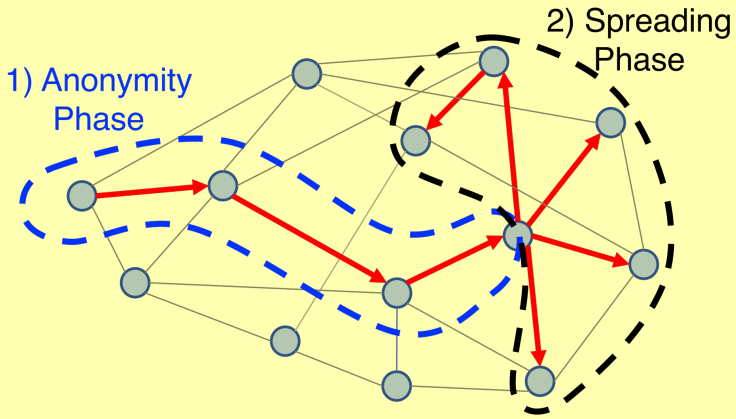


Figure 4: Phases of Dandelion Transaction Propagation
Image source: "Dandelion" protocol white paper[52]

**"Stem" Anonymity Phase** In this phase, a 4-regular[†1] anonymity graph of nodes are created (and re-generated every epoch)[51]. If the node is committing a new transaction of its own, it forwards the transaction along the same outbound edge in the anonymity graph[50].

Each time a node receives a stem-phase transaction from another node it relays transactions to two pseudorandomly chosen peers according to a map of incoming and outbound edges in the anonymity graph[51].

**"Fluff" Spreading Phase** In the spreading phase, the node propagates transactions over the network via the conventional diffusion method, transmitting the transaction to all of its connected nodes. This broadcasts the transaction to every outgoing connection with randomized communication times[52].

This two-stage method of propagation obfuscation makes an attacker unable to simply listen for the direction of a transaction. The stem phase nodes will have distributed the transaction randomly meaning the originating node of the fluff phase is not the source of the original transaction, and it is unknown how many hops along the stem the transaction underwent prior to mass propagation[50].

## 5.7 Local vs Remote Nodes

Because the Monero blockchain is quite large and can take a significant amount of time to sync (especially if using a mechanical hard drive) Monero wallets can connect to a "Remote node" rather than using a local node[7]. Remote nodes, also known as public nodes, are not without potential drawbacks, however. A malicious remote node can easily see your IP address (negating the effectiveness of Dandelion+) and associate it with the transaction, hide blocks to make it appear as though your wallet is up-to-date, and provide a list of already spent decoy addresses reducing the effectiveness of ring signatures[53].

Despite the potential privacy compromises, using a remote node always remains secure as nodes are unable to manipulate transactions or access your private keys[53]. Any concern of IP address transaction linking can be mitigated through the use of Tor, I2P, or a centralized VPN service such as "Mullvad VPN." Remote nodes are sometimes the only option for wallets on mobile devices such as phones, Chromebooks, or laptops with insufficient free storage space. Using a remote node and conventional wallet is still preferable to using a "light wallet" such as "MyMonero" as these wallets handle all synchronization on an external server which requires access to your private view key, which gives complete access to inbound transaction history, in addition to all the potential risks of a remote node[53].

Monero wallets, like the internally developed desktop wallet "Monero-Wallet-GUI," give the easy option of automatically configuring a local node or selection of a remote node. For Wownero there is very little need to use a remote node currently as, due to the lower transaction volume and more recent launch date, the blockchain database is much smaller..

### 5.7.1 TOR

"TOR," or "The Onion Router," is a technology originally developed by the U.S. Navy which provides users with *layers* of anonymity by routing traffic through many nodes and, theoretically, requiring an attacker to compromise all the nodes used to discern the original IP address of a user. Monero can optionally be integrated with Tor and setup tutorials are

[†1] a 4-regular graph is a graph in which every vertex is connected to exactly four other vertices.

provided in the Monero git repo documentation[3]. The Monero and Wownero daemons provides a convenient command flag to connect to a Tor proxy running on localhost

EX: `--tx-proxy tor,127.0.0.1:9050,10`

Wownero's popular "Wowlet"[16] wallet software uses Tor implicitly by default requiring no action on the part of the end user at all.

### 5.7.2 I2P

"I2P," or the "Invisible Internet Project," is another optional privacy protocol which can be used. There has been discussion and interest in future I2P integration with the Monero daemon, possibly through Kovri (discussed in section 5.7.3), however this has been delayed[54]. I2P is intended to protect you from passive network monitoring, so that anyone observing network traffic cannot tell that Monero is being used at all. The Monero developers prefer I2P over TOR because of its more decentralized routing protocol and asymmetric connections which mitigate 'timing attacks'[45]. Currently, the Wownero endorsed I2P router is i2p-zero[55]. As with Tor a command line flag is available to connect to an I2P proxy running on localhost

EX: `--tx-proxy i2p,127.0.0.1:90000`

### 5.7.3 Kovri

Kovri is a privacy-focused network layer that based on the I2P specification developed by the Monero Research Lab[54]. Kovri is not (yet) part of Monero however it may be added in a future update after a thorough evaluation and security audit[7]. Because of Wownero's historically less stringent testing requirements Kovri could be implemented into Wownero ahead of Monero.

Kovri aims to be an easy to use, maintain, and review I2P router with extended functionality such as a "hidden mode" which would make I2P usage harder to detect by an internet service provider[54]. That feature could help to make Monero and Wownero more available in totalitarian countries with a highly controlled internet. Kovri is a rewrite of I2P in C++, forked from the i2pd project, for higher performance and to remove dependence on a bulky Java runtime[54].

Their seems to be some hostility between I2P and Kovri developers as shown in the Kovri FAQ section "Why did you fork from i2pd?" [54]

> ... We wanted a positive community that encouraged collaboration for the betterment of the software; not negative, narcissist glory... [and] a lead developer who could lead; not someone who could ignore requests for responsible disclosure or tuck-tail-and-run when faced with collaborator conflict

Hopefully this disagreement will not jeopardize future development of either of these privacy-enhancing projects, however, the Kovri project may have been abandoned already as the last commit was 3 years ago and public enthusiasm towards the project has declined.

## 6 Conclusion

In conclusion, Wownero is a privacy-focused cryptocurrency, based on Monero but with a fixed supply, modifications to the block time, confirmation requirement, mining algorithm, emission profile, ring size, and its own unique software ecosystem and branding. In keeping with Monero's privacy and anonymity focused philosophy, Wownero's has many privacy features including stealth addresses, ring signatures, transaction amount hiding, network obfuscation, and integrations with proxy services such as TOR and I2P.

Wownero has faced challenges with mass adoption due to its privacy features reducing public exchange listings. Despite this, Wownero's development community is continuingly working on improving its software ecosystem of wallets and various integrations to make it more accessible, user-friendly, and useful.

Overall, Wownero is a promising cryptocurrency for those who value privacy, anonymity, and decentralization in their shitcoin transactions. Its unique features and development roadmap make it an interesting coin to follow, especially for those who are already familiar with Monero.

## References


[1] Monero Research Lab. *About Monero*. URL: https://www.getmonero.org/resources/about/. (accessed: April 23, 2023).

[2] Sarang Noether KOE Kurt M. Alonso. *Zero to Monero: Second Edition*. Distributed through getmonero.org. Apr. 2020. URL: https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf.

[3] Cryptonote developers The Monero Project. *Monero Git Repo*. URL: https://github.com/monero-project/monero. (accessed: April 24, 2023).

[4] Nicolas van Saberhagen. *CryptoNote v 2.0*. Tech. rep. Oct. 2013. URL: https://web.getmonero.org/resources/research-lab/pubs/cryptonote-whitepaper.pdf.

[5] Unknown. *Top-42 Cryptocurrencies by Merchant Acceptance*. URL: https://acceptedhere.io/stats/. (accessed: April 24, 2023).

[6] Monero Community Members. *A low-level explanation of the mechanics of Monero vs Bitcoin*. URL: https://www.monero.how/how-does-monero-work-details-in-plain-english. (accessed: April 23, 2023).

[7] Monero Research Lab. *Moneropedia*. URL: https://www.getmonero.org/resources/moneropedia/. (accessed: April 23, 2023).

[8] Monero Community Members. *How to prove a payment was made*. URL: https://www.getmonero.org/resources/user-guides/prove-payment.html. (accessed: April 25, 2023).

[9] Wownero Community Members. *Wownero Main Page*. URL: https://wownero.org. (accessed: April 23, 2023).

[10] Wownero Contributors. *Wownero Git Repo*. URL: https://git.wownero.com/wownero/wownero. (accessed: April 23, 2023).

[11] Wownero Community Members. *Introduction [To Wownero]*. URL: https://slime.cash/intro/. (accessed: April 24, 2023).

[12] John Murphy "jwinterm". *The homepage of John Winter Murphy*. URL: https://jwinterm.com/. (accessed: April 24, 2023).

[13] jwinterm. *Personal Communication With Wownero Developer*. Apr. 2023.

[14] Katelyn Peters. *MoneroV (XMV)*. URL: https://www.investopedia.com/tech/difference-between-monero-and-monerov/. (accessed: April 28, 2023).

[15] "equismic". *PSA: MoneroV is blatantly a scam made to enrich its makers*. URL: https://www.reddit.com/r/Monero/comments/7vcz78/psa_monerov_is_blatantly_a_scam_made_to_enrich/. (accessed: April 28, 2023).

[16] Feather Wallet Developers. *WOWlet: a free Wownero desktop wallet*. URL: https://wowlet.app/. (accessed: April 23, 2023).

[17] Wownero Community Members. *MuchWOW Blocks*. URL: https://muchwow.lol/. (accessed: April 23, 2023).

[18] "dsc". *SuchWOW*. URL: https://suchwow.xyz. (accessed: April 23, 2023).

[19] Wownero Community Members. *Wownero Forum*. URL: https://forum.wownero.com/. (accessed: April 24, 2023).

[20] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Tech. rep. 2008. URL: https://www.bitcoin.com/bitcoin.pdf.

[21] Linda Orenes-Lerma. *How Does a Blockchain Transaction Work?* URL: https://www.ledger.com/academy/how-does-a-blockchain-transaction-work. (accessed: April 26, 2023).

[22] NIST CS Resource Center. *NIST Computer Security Resource Center Glossary*. URL: https://csrc.nist.gov/glossary. (accessed: April 26, 2023).

[23] Wikipedia Users. *Wikipedia: Cryptocurrency*. URL: https://en.wikipedia.org/wiki/Cryptocurrency. (accessed: April 26, 2023).

[24] Monero Community Members. *How long do Monero transactions take?* URL: https://www.monero.how/how-long-do-monero-transactions-take. (accessed: April 26, 2023).

[25] "tevador" et al. *RandomX GitHub Repo*. URL: https://github.com/tevador/RandomX. (accessed: April 25, 2023).

[26] LocalMonero Site Maintainers. *Monero Blocks*. URL: https://localmonero.co/blocks. (accessed: April 26, 2023).

[27] Diego Salazar. *Monero Outputs Explained*. URL: https://localmonero.co/knowledge/monero-outputs. (accessed: April 26, 2023).

[28] Monero Research Lab. *Frequently Asked Questions*. URL: https://www.getmonero.org/get-started/faq/. (accessed: April 26, 2023).

[29] Jake Frankenfield. *Hard Fork: What It Is in Blockchain, How It Works, Why It Happens*. URL: https://www.investopedia.com/terms/h/hard-fork.asp. (accessed: April 26, 2023).

[30] Jake Frankenfield. *Ethereum Classic (ETC) Definition, History, Future*. URL: https://www.investopedia.com/terms/e/ethereum-classic.asp. (accessed: April 26, 2023).

[31] Seth For Privacy. *How Monero Uses Hard-Forks to Upgrade the Network*. URL: https://localmonero.co/knowledge/network-upgrades. (accessed: April 26, 2023).

[32] Jake Frankenfield. *Soft Fork*. URL: https://www.investopedia.com/terms/s/soft-fork.asp. (accessed: April 26, 2023).

[33] Jake Frankenfield. *What Are Consensus Mechanisms in Blockchain and Cryptocurrency?* URL: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp. (accessed: April 26, 2023).

[34] Diego Salazar. *Monero Mining: What Makes RandomX So Special*. URL: https://localmonero.co/knowledge/monero-mining-randomx. (accessed: April 28, 2023).

[35] Delton Rhodes. *CryptoNight: An Overview Of The CryptoNight Mining Algorithm*. URL: https://komodoplatform.com/en/academy/cryptonight/. (accessed: April 28, 2023).

[36] Ruisiang. *Monero(XMR) RandomX PoW Algorithm Explained*. URL: https://ruisiang.medium.com/monero-xmr-randomx-pow-algorithm-explained-d3cf95619717. (accessed: April 28, 2023).

[37] Unknown. *Elliptic Curve Digital Signature Algorithm - Wikipedia*. 2023. URL: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm. (accessed: May 6th, 2023).

[38] Piotr "Qertoip" WłOdarek. *[Monero] Standard Address*. 2023. URL: https://monerodocs.org/public-address/standard-address/. (accessed: May 6th, 2023).

[39] Daniel J. Bernstein. *Curve25519: new Diffie-Hellman speed records*. Tech. rep. URL: https://cr.yp.to/ecdh/curve25519-20060209.pdf.

[40] StackExchange Users "skaht" and "user141". *What is a stealth address? - Monero Stack Exchange*. 2016. URL: https://monero.stackexchange.com/questions/1500/what-is-a-stealth-address. (accessed: May 5th, 2023).

[41] "Seth For Privacy". *View Tags: How one Byte Will Reduce Monero Wallet Sync Times by 40%*. URL: https://localmonero.co/knowledge/view-tags-reduce-monero-sync-time. (accessed: April 26, 2023).

[42] Piotr 'Qertoip' WłOdarek. *[Monero] Subaddress*. 2023. URL: https://monerodocs.org/public-address/subaddress/. (accessed: May 6th, 2023).

[43] David Mandell Freeman. *Schnorr Identification and Signatures*. Tech. rep. Oct. 2011. URL: https://web.stanford.edu/class/cs259c/lectures/schnorr.pdf.

[44] Unknown. *Ring signature - Wikipedia*. 2023. URL: https://en.wikipedia.org/wiki/Ring_signature. (accessed: May 6th, 2023).

[45] Monero Community Members. *How does Monero's privacy work?* 2023. URL: https://www.monero.how/how-does-monero-privacy-work. (accessed: April 24, 2023).

[46] Shen Noether. *Ring Confidential Transactions*. Tech. rep. URL: https://eprint.iacr.org/2015/1098.pdf.

[47] Torben Pryds Pedersen. *Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing*. Tech. rep. 978-3-540-46766-3. Aarhus University, May 2001. URL: https://link.springer.com/chapter/10.1007/3-540-46766-1_9.

[48] Benedikt Bünz et al. *Bulletproofs: Short Proofs for Confidential Transactions and More*. Tech. rep. 2017. URL: https://eprint.iacr.org/2017/1066.pdf.

[49] Sarang Noether. *Bulletproofs+ in Monero*. Dec. 2020. URL: https://www.getmonero.org/2020/12/24/Bulletproofs+-in-Monero.html.

[50] Diego Salazar. *How Dandelion++ Keeps Monero's Transaction Origins Private*. Apr. 2020. URL: https://localmonero.co/knowledge/monero-dandelion. (accessed: May 8, 2023).

[51] Giulia Fanti et al. *Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees*. Tech. rep. arXiv:1805.11060. Carnegie Mellon University, May 2018. URL: https://arxiv.org/pdf/1805.11060.pdf.

[52] Shaileshh Bojja Venkatakrishnan, Giulia Fanti, and Pramod Viswanath. *Dandelion: Redesigning the Bitcoin Network for Anonymity*. Tech. rep. 2017. arXiv: 1701.04439 [cs.CR].

[53] Seth For Privacy. *How remote nodes impact Monero's privacy*. Feb. 2022. URL: https://localmonero.co/knowledge/remote-nodes-privacy. (accessed: May 8, 2023).

[54] Dimitris Apostolou. *Kovri Git Repo*. URL: https://gitlab.com/kovri-project/kovri-docs/-/blob/master/i18n/en/faq.md. (accessed: April 24, 2023).

[55] i2p-zero Developers "knaccc". *Wownero i2p-zero Git Repo*. URL: https://git.wownero.com/wownero/i2p-zero. (accessed: May 8, 2023).