



# Whitepaper (proposed)

October 20, 2018

*(DRAFT Version 0.03)*

# Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Vision</b>                              | <b>1</b>  |
| <b>2</b> | <b>AEON Features</b>                       | <b>2</b>  |
| 2.1      | Secure . . . . .                           | 2         |
| 2.2      | Lightweight . . . . .                      | 2         |
| 2.3      | Private and Untraceable . . . . .          | 2         |
| 2.4      | Low Barrier to Participation . . . . .     | 2         |
| <b>3</b> | <b>AEON Differentiation</b>                | <b>3</b>  |
| 3.1      | vs. Bitcoin . . . . .                      | 3         |
| 3.2      | vs. Litecoin . . . . .                     | 4         |
| 3.3      | vs. Monero . . . . .                       | 5         |
| 3.4      | vs. Dash . . . . .                         | 5         |
| 3.5      | vs. Zcash . . . . .                        | 6         |
| 3.6      | vs. Ripple . . . . .                       | 7         |
| <b>4</b> | <b>AEON Implementation</b>                 | <b>8</b>  |
| 4.1      | Achieving Trustless Transactions . . . . . | 8         |
| 4.2      | Achieving Anonymous Transactions . . . . . | 9         |
| 4.3      | Coin Minting Process . . . . .             | 11        |
| 4.4      | Transaction Fees . . . . .                 | 14        |
| <b>5</b> | <b>AEON Community</b>                      | <b>15</b> |
| 5.1      | Links . . . . .                            | 15        |
| 5.2      | Mining . . . . .                           | 15        |
| 5.3      | Exchanges . . . . .                        | 15        |
| 5.4      | Wallets . . . . .                          | 15        |
| 5.5      | Development Team . . . . .                 | 16        |
| 5.6      | Current Work and Future Plans . . . . .    | 16        |

## Disclaimer

This whitepaper does not provide a legally binding agreement. Neither the AEON development team, nor the community members, accept any legal liability arising from the use of AEON or the material contained in this whitepaper.

This whitepaper represents, at the date of the latest update, the current state and plans of the AEON community and developers. Since AEON is an open source project, details may change and should not be considered final.

# 1 Vision

Technology impacts our financial lives in new ways every day, and the pace of change is accelerating. In the first decade of the 21st century broadband internet became widely available, giving rise to the concept of online marketing and commerce. By 2015, mobile phone usage increased to rival desktop usage for online shopping. Researchers have estimated that by 2021 there may be over 2 billion mobile banking users.

**Truly, we are realizing a more convenient reality with our personal finances.**

This convenience, however, comes with many challenges. On any given day, it is not difficult to find a news story about financial accounts being hacked and/or personal identity information being stolen. And in spite of the technological advances, the current ecommerce solutions cannot solve the problems inherent with local currencies; such as the difficulty of transacting across national borders, and the occasions when centralized powers negatively impact economies via poor decisions or manipulation.

**Enter the concept of decentralized digital currency.**

Imagine a time in the not-so-distant future where personal financial management is not only convenient and mobile, but also secure, private, and impervious to national borders and centralized control.

AEON is about enabling this era, enabling an age where all people everywhere have the freedom to privately receive, spend, and manage their finances with whatever gadget they already own.

***This new era in personal finance is closer than you think...***

## 2 AEON Features

AEON stands for Anonymous Electronic ON-line Coin, and it was launched on June 6, 2014 at 6:00 PM UTC. The following features are critical to the vision of a digital currency for everyone.

### 2.1 Secure

AEON takes security seriously. Each transaction is secured with robust cryptography and distributed through a global peer-to-peer consensus network. The cryptographic implementation ensures that nobody is able to “steal” an online transaction, and a coin’s owner is unable to spend the coin more than once.

### 2.2 Lightweight

AEON seeks to be **mobile-friendly** by implementing, among other things, the following technical features:

- A lightweight Proof-of-Work algorithm
- Blockchain pruning
- Optional lightweight traceable transactions

With this intentional focus, AEON requires a smaller technology footprint than comparable crypto currencies, and the time to sync with the blockchain on lower end devices improves by a factor of 10.

### 2.3 Private and Untraceable

Privacy is paramount. Funds are transferred without the identifying information of the user becoming visible on the blockchain. In addition, the receiving wallet addresses are obfuscated with ring signature technology and non-repeating one-time addresses derived from the receiving public key. These measures make the blockchain highly resistant to analysis.

### 2.4 Low Barrier to Participation

Founded as an Open Source project, AEON is free to use without restriction, and 100% of funding is by voluntary community donations; there is no Development Tax imposed on miners. In addition, there was no premine or instamine (a practice by which the developers gain a large percentage of the coins before allowing other miners to be involved). The network is resistant to specialized hardware (ASICs), allowing more people to participate directly with their PC by mining or running a full node. Everyone is welcome to contribute to the ongoing effort, financially or otherwise.

NOTE: Many of the points referenced above are covered in more detail in section 4 *AEON Implementation*.

### 3 AEON Differentiation

With the astounding plethora of “alt coins” now available, it is worth noting how AEON differs from others, and specifically how it improves upon some of the similar offerings.

The first thing to note is that within the alt coin universe, there are different classes of blockchain and coin. There are **smart contract** blockchains (i.e. Ethereum) which provide a mechanism to manage complex transactions such as business contracts and decentralized application (“dApp”) hosting. There are also **token** coins (i.e. STEEM token) which supply a payment mechanism for use of a particular decentralized application or service.

AEON is a **currency** coin, intended to provide an alternative to local fiat currencies. Therefore, this section will provide comparisons only to other well-known currency coins.

(NOTE: for more details on the concepts in this section, see section 4 *AEON Implementation*.)

#### 3.1 vs. Bitcoin

Bitcoin is the best-known of all crypto currency blockchains, as it was the first to achieve a measure of success. There are considerable differences between AEON and Bitcoin, in the areas of privacy and usability.

##### 3.1.1 Privacy and Transaction Linkages

Regarding the critical feature of privacy, Bitcoin falls short of the AEON blockchain. In order to maintain privacy of individual expenditures, it must be exceedingly difficult for an outside party to link a transaction back to its owner.

Consider that each transaction consists of some *inputs* (coins which are being spent) and some *outputs* (one or more addresses which receive the spent coins). Additionally, each input in a transaction actually links to an output of a *previous* transaction, forming a set of transaction paths.

In Bitcoin, these transaction linkages are explicitly transparent on the blockchain. Any blockchain explorer can follow the graph, which has allowed for sophisticated analysis to de-anonymize transactions. This privacy issue is alleviated in various ways, such as creating a unique address for every transaction, using centralized “mixers” to randomly “mix up” several people’s Bitcoins, and employing methods to hide IP addresses when making transactions. The fact remains, however, that the Bitcoin inputs and outputs can be directly followed on the blockchain.

AEON resolves this privacy concern by *intentionally obscuring* transaction linkages on the blockchain. Every transaction has a default number of “decoy” input links (also known as **mixins**). Anyone making a transaction can request a higher number of decoy inputs, to increase anonymity. As the blockchain grows over time, the increasing number of decoy input links will make the overall graph of transactions exceedingly difficult, if not impossible, to correctly decipher.

##### 3.1.2 Mining and Barriers to Participation

Bitcoin uses a SHA-256 Proof-of-Work (PoW) algorithm which is dependent primarily on CPU power, and there are several specialized ASIC hardware devices made for mining Bitcoin. This

has driven the hashrate high enough that currently only ASIC hardware mining is profitable. The result is that the average person with a PC cannot readily participate in the transaction validation process of mining and acquiring Bitcoins.

AEON uses a CPU-friendly PoW algorithm that limits the advantage of GPU's and is ASIC resistant. This allows almost anyone with a PC to participate in mining and acquiring AEON.

### 3.1.3 General Usability and Transactions-Per-Second

Regarding usability and the vision of a lightweight digital currency for everyone, AEON has distinct advantages over Bitcoin.

The maximum blocksize of Bitcoin (1 MB) and the block creation time of 10 minutes limits the transactions-per-second (TPS) processing power to no more than 7 TPS. This low TPS severely hinders the ability of the Bitcoin blockchain to process transactions for the masses. While there are ways to remedy this limitation, the Bitcoin community has not achieved consensus on doing so. Thus, the coin has become more of a high-end investment with limited use as a currency, not unlike physical gold coins versus U.S. dollar bills.

AEON solves the TPS limitation by using an algorithm to automatically adjust the maximum block size up or down, based on the previous 100 blocks. This approach allows the AEON blockchain to self-adjust it's TPS throughput as transaction traffic increases and decreases over time.

## 3.2 vs. Litecoin

Litecoin was started as a fork of the Bitcoin code in 2011, with the goal of being a lighter-weight currency, offering low-cost transactions with fast confirmation status.

### 3.2.1 Privacy and Transaction Linkages

See the description of the privacy issues in section 3.1 *vs. Bitcoin*. Litecoin has the same issues as Bitcoin.

### 3.2.2 Mining and Barriers to Participation

Litecoin uses a Proof-of-Work algorithm called **scrypt** which depends not only on the CPU, but also on fast access to a memory area. This PoW makes it difficult to develop specialized ASIC hardware, and renders GPU's to be only about 10X faster than CPU's. This is a great improvement over Bitcoin, but still leaves mining largely in the hands of those who can purchase high end graphics cards or special built ASICS.

AEON actually uses an improved version of the scrypt algorithm which employs a larger memory area. The result is that AEON is even more resistant than Litecoin to specialized hardware, and the GPU cards do not have as great an advantage over the CPU. This ensures that CPU mining with an average PC is an option for everyone.

### 3.2.3 General Usability and Transactions-Per-Second

Being a "lightweight Bitcoin" it is no surprise that Litecoin is able to boast roughly 8 times the TPS of Bitcoin. This brings the maximum capacity of Litecoin up to 56 transactions per second.

For comparison, credit card processors typically see tens of thousands of transactions per second. While the Litecoin network can currently process transactions fast enough for its volume of users, at some point – long before Litecoin can become a currency for the masses – its TPS must be greatly increased.

See the prior section 3.1 *vs. Bitcoin* for a description of AEON’s solution to the TPS limitation.

### **3.3 vs. Monero**

It is public knowledge that AEON is a fork of the Monero project, and it continues to incorporate improvements directly from the Monero code base. In fact, the Development team for AEON consists largely of Monero developers who also work on AEON. Since Monero itself is well-known as a security/privacy coin, it requires some attention, to address exactly why AEON might be preferred.

#### **3.3.1 General Usability and Mobile-Friendliness**

The advantages that AEON has over Monero are in the area of being lightweight and mobile-friendly. AEON has chosen a different Proof-of-Work algorithm which requires half the CPU memory and allows for faster verification of the blockchain. The blockchain is pruned in a manner that keeps it smaller than Monero’s, resulting in faster blockchain synchronization. AEON also allows the option for a limited number of fast, low-fee transfers (which are more traceable on the blockchain) for non-sensitive payments. Monero, on the other hand, requires all payments to be fully anonymized which adds to the validation times and blockchain size.

All of these aspects, among others, put AEON in a better position to be the secure, private currency that can be used by the general public with cell phones and tablets on the go.

### **3.4 vs. Dash**

Dash stands for “digital cash” and is meant to work like physical cash when purchasing items online or in stores. Like AEON, Dash embraces the importance of Security and Privacy. There are some disadvantages, however, when comparing this coin to AEON.

#### **3.4.1 General Usability and Transactions-Per-Second**

In November, 2017, the Dash blockchain hard-forked to double it’s maximum blocksize, to 2 MB. That change allowed Dash to process roughly 48 transactions per second. For comparison, credit card processors typically see tens of thousands of transactions per second. At some point the Dash TPS must be increased again, and likely again after that. This continued increasing of TPS via disruptive blockchain modifications is not conducive to massive adoption.

See section 3.1 *vs. Bitcoin* for a description of AEON’s solution to the TPS limitation.

#### **3.4.2 Mining, Governance and Barriers to Participation**

Dash uses a Proof-of-Work algorithm which is dependent primarily on CPU power, and the network welcomes the use of specialized hardware for mining. This has driven the hashrate high enough that currently only ASIC hardware mining is profitable. The result is that the average person with

a PC cannot readily participate in the transaction validation process of mining.

Additionally, Dash implements a complex form of Governance consisting of a 2nd tier network node, called a Masternode. In order to own a Masternode, one must obtain and hold 1000 Dash. (At the time of this writing, this is an investment of roughly \$200,000 USD.) Only Masternode owners vote on proposed enhancements to the coin, as well as prioritize which projects get paid from the development fund. Similar to AEON, new coins are disbursed as a block reward when a miner successfully validates a block of transactions. But unlike AEON, the miner must split the block reward between the Masternodes and the Development Fund.

Because special hardware is required to mine Dash, and a large monetary investment is necessary to participate in the governance of the currency, the barriers to participation are much higher than with AEON's simple open source project model. Even to submit a proposal for a vote by the Masternode owners, costs a fee of 5 Dash (roughly \$1000 USD at the time of this writing). These factors work against a true decentralization for a currency.

AEON uses the traditional Open Source Model of participation and governance, which has been shown to work well for many large technology efforts for many years. It allows a diverse community to grow organically, which is an advantage for AEON's plans to become widely used by all walks of life.

### **3.5 vs. Zcash**

Zcash is another fork of the Bitcoin code base, with the intent of adding the element of privacy to the blockchain.

#### **3.5.1 Privacy and Shielded Transactions**

Zcash achieves privacy by using a cryptographic approach called "zero-knowledge cryptography" to create "shielded transactions". However, this is not the default option, and there is no limit to the number of non-private transactions in each block. A recent report by ICO research firm Satis Group ("Cryptoasset Market Coverage Initiation: Valuation", August 30, 2018) states:

"Only 5% of the Zcash network uses 'shielded' addresses currently, with the rest of the addresses being used for transactions functionally and technically no different than Bitcoin."

The paper concludes that since there are so many more addresses in the blockchain that are not private, the Zcash network as a whole is not fungible. Meaning the coins in any given wallet could possibly be traced back to their prior transactions. (This is important, because nobody wants to find out that the coins in their wallet were used previously to commit a crime, etc.)

In contrast, the research states specifically that Monero – and therefore we can conclude AEON as well – is a fungible network. Both Monero and AEON default to a private transaction, and AEON only allows at most 10% of the transactions in any block to be switched to non-private.

#### **3.5.2 Mining and Barriers to Participation**

Zcash went away from the Bitcoin PoW algorithm, and implemented the Equihash PoW algorithm, to provide ASIC resistance, and allow people to mine with their GPU's and CPU's. The problems



with the Equihash algorithm are that 1) it does not limit the advantage of GPU over CPU, and 2) an ASIC was recently developed which could mine Zcash, threatening the future viability of GPU and CPU mining. As of the date of this paper, the Zcash project has not created a fork of the blockchain to provide ASIC resistance once again.

AEON's PoW, as stated previously, is more CPU friendly, and more ASIC resistant. In addition, when an ASIC was successfully developed for the CryptoNight-Lite algorithm, the AEON developers quickly moved to fork the blockchain to regain ASIC resistance.

### 3.5.3 General Usability and Transactions-Per-Second

Zcash improved upon Bitcoin by doubling the maximum block size to 2 MB, and decreasing the block interval down to 2.5 minutes. However the transaction size is larger in Zcash, so the maximum TPS will only reach about 26, and could be far less if more of the transactions happen to be shielded. As with Bitcoin, the TPS throughput will need to be increased into the thousands before Zcash will become a currency used by the masses.

See section 3.1 *vs. Bitcoin* for a description of AEON's solution to the TPS limitation.

## 3.6 vs. Ripple

Of all the currencies discussed in this section, Ripple is one which may not belong. The Ripple blockchain is open source, but Ripple is also a private company. From their homepage: "Ripple connects banks, payment providers, digital asset exchanges and corporates via RippleNet to provide one frictionless experience to send money globally." Consider the ways in which Ripple's vision is different from AEON:

- Ripple does not decentralize the management of personal wealth; it seeks to strengthen the ability of central entities to control the movement of wealth on a global scale.
- Working with banks, Ripple does not provide privacy, but instead provides full traceability of funds.
- There is no mining process, by which individuals can receive coins for themselves. All coins have been produced, and the Ripple company releases a certain number of coins per month.

## 4 AEON Implementation

The implementation of AEON is derived from two other open source projects: **CryptoNote** and **Monero**.

The CryptoNote technology focuses on the ability to create crypto-currencies with untraceable transactions, CPU-friendly proof-of-work algorithm, and the ability of self-adjusting parameters such as block size and difficulty. Several crypto coins have been based on the CryptoNote technology.

Monero is one of the earliest crypto currencies to use the features of CryptoNote, and has grown to be the most popular with a market cap well within the top 20 crypto coins. AEON was started from the Monero code base, and modified only in ways that meet the specific vision and goals of the AEON community.

This section will provide an overview of the implementation of the AEON cryptocurrency.

### 4.1 Achieving Trustless Transactions

One of the goals for AEON transactions is to have the properties of *physical cash* payments, as opposed to electronic payments.

Consider the example of paying for a meal at a restaurant. With electronic payment (i.e. a credit card), there is a trusted 3rd party (i.e. Visa) which carries out the transaction for the payer and receiver. The trusted party must know both the payer's and receiver's identities and account information to settle the transaction. Additionally, the receiver may also receive the payer's name and partial account information.

In contrast, paying for a meal with cash is *trustless* (requires no trusted 3rd party to carry out the transaction). It is also *anonymous* in that it does not require the payer to give their name or any other personal information to the receiver.

To achieve trustless, decentralized transactions, AEON utilizes a proof of work “mining” process. For a definition of PoW, the Bitcoin Wiki at [https://en.bitcoin.it/wiki/Proof\\_of\\_work](https://en.bitcoin.it/wiki/Proof_of_work) offers this:

“A **proof of work** is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required *on average* before a valid proof of work is generated.”

The goal of the proof of work process, is to provide decentralization of both the distribution of coins and the validation of transactions. The difficult trial-and-error nature of producing the PoW is an effective means of randomizing which miner will create and correctly validate the next block of transactions, and receive the reward of new coins. This randomization ensures that the processing of transactions is spread indiscriminately over the entire network.

A disadvantage of the PoW function for many cryptocurrencies (including Bitcoin) is that it relies solely on processor speed, which allows high-end GPU's and specialized mining hardware (ASICs)

to have a great advantage in producing the correct proof of work. This condition leaves the majority of PC owners unable to participate in the mining process for coins, and creates an environment where relatively few miners control the network. Thus, the goal of decentralization is somewhat defeated.

An improved PoW algorithm, eventually called CryptoNight, was proposed in 2012 by the CryptoNote project. According to the CryptoNote whitepaper (<https://cryptonote.org/whitepaper.pdf>):

“Our primary goal is to close the gap between CPU (majority) and GPU/FPGA/ASIC (minority) miners. It is appropriate that some users can have a certain advantage over others, but their investments should grow at least linearly with the power. More generally, producing special-purpose devices has to be as less profitable as possible.”

The CryptoNight algorithm accomplishes this goal in 2 primary ways.

- It uses built-in CPU instructions, which are difficult to implement in specialized hardware.
- It relies on access to unpredictable locations in a 2 MB “scratchpad” of CPU memory, rather than relying solely on CPU processing speed.

These factors effectively limit the advantages of GPU’s over CPU’s and make it too costly to produce specialized ASIC hardware for mining.

For its proof of work, AEON implements a variation of this algorithm, called **CryptoNight-Lite**. As the name suggests, this is a lightweight version of the original algorithm, which utilizes a 1 MB scratchpad. This results in half the iterations needed to compute a hash, and half the required L3 cache CPU memory. Many lower end processors (on mobile devices) will have the required 1 MB of CPU cache, and multi-core CPU processors will see up to a 4X performance boost over the heavier CryptoNight algorithm.

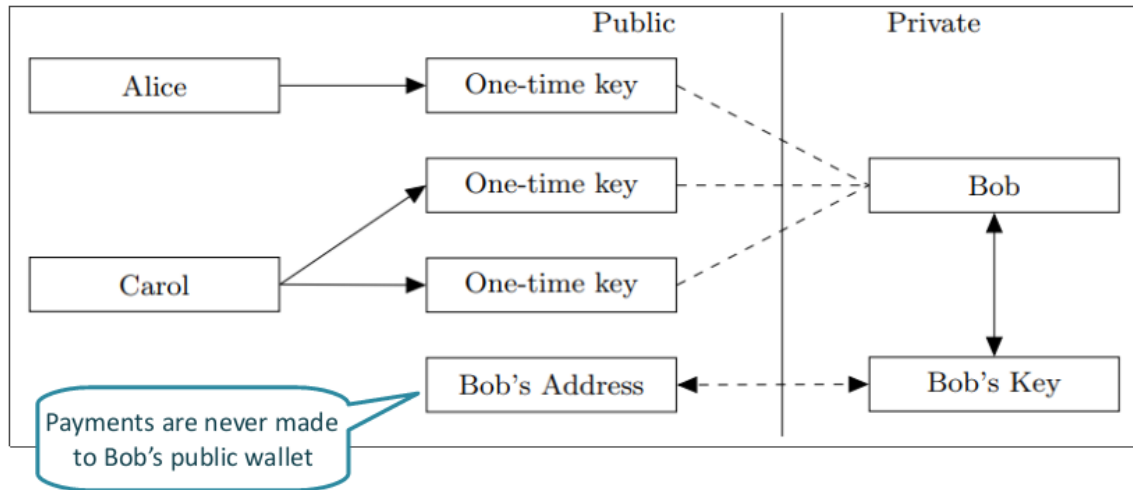
## 4.2 Achieving Anonymous Transactions

The previous section explained how the PoW algorithm creates a decentralized trustless network of miners to process transactions. To achieve anonymity, the payer’s and receiver’s identities and account (wallet) information must be kept hidden on the public blockchain.

### 4.2.1 One-Time-Use Keys

AEON uses the CryptoNote solution to receive payments at a one-time-use public key address, rather than the recipient’s public wallet address. The public key is generated by the sender, using both the recipient’s public wallet address and some random data. Once generated, funds are sent directly to this public key, which can be used only once. The recipient can later spend any received coins, by using a one-time-use private key (called a **ring signature**) which corresponds to the one-time public key.

The following picture, from the CryptoNote whitepaper, shows that the one-time public keys are never linked to the receiver’s public wallet address on the blockchain. This effectively keeps the receiving wallet anonymous.



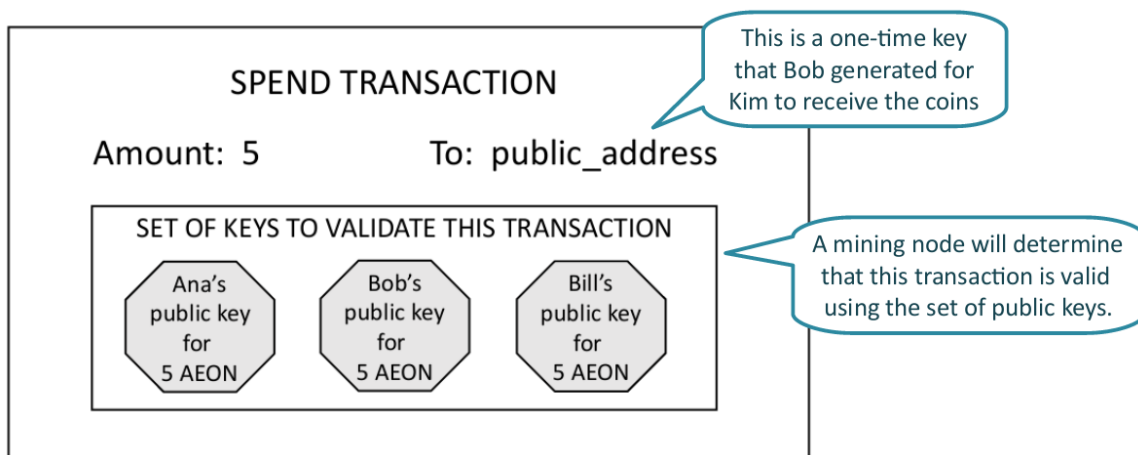
#### 4.2.2 One-Time Ring Signatures

After funds are received via a one-time public key, the recipient is able to spend the funds at any time, using a one-time ring signature. The goal of the ring signature is to keep the sending address anonymous on the blockchain.

In non-private implementations, the sender will “sign” their payment transaction with a private key that can be validated only by using the sender’s corresponding public key. Only the sender knows the private key, but the whole world can see that the sender’s public key was used to validate the transaction.

The idea behind the ring signature is straightforward: a sender produces a signature which can be validated by a *set* of public keys rather than a unique public key. The identity of the one who produced the signature is indistinguishable from the owners of the additional public keys within the set.

Consider an example: Bob wishes to send 5 AEON to Kim. The picture below shows the ring signature concept for this transaction on the blockchain, using a default ring size of 3.



Note in the example, that the 2 “decoy” public signatures are actually past transaction outputs

that are pulled from the AEON blockchain. Thus, all 3 inputs in the set are valid signed inputs for 5 AEON, but only Bob's is valid for *this* transaction. It is impossible for someone looking at this transaction on the blockchain to determine which of the 3 inputs was the valid one. Additionally, all 3 of the inputs will likely show up as decoys in multiple other transactions.

In the AEON blockchain, the total number of inputs, known as the **ring size**, is set to 3 by default. The sender may choose a different ring size for their transaction, and the selection of each decoy input is handled automatically by AEON. More than 3 inputs will result in a higher level of anonymity, but will require a higher transaction fee.

For non-sensitive transactions to be processed with a slightly lower fee, a ring size of 1 can be chosen. To preserve overall blockchain anonymity the number of such transactions is limited to no more than 10% of the transactions in each block. Additionally, a ring size of 2 is not allowed since it does not provide a high enough assurance against blockchain analysis.

### 4.2.3 Known Weaknesses

One possible attack against Anonymity is analysis based on the amounts sent in a transaction. If a bad actor knows, for example, that 0.9 coins have been sent at a certain time, then they may search for transactions containing 0.9 coins to attempt to identify a sender. This is negated by the use of one-time keys and other factors, but the visibility of the amounts on the blockchain is a downside.

Furthermore, as seen in the illustration in the previous section, the ring signature approach requires the specific amount of each of the inputs to match. For less common amounts, there will be fewer public keys available for decoys, reducing the level of anonymity.

The Monero development team has created a solution for these weaknesses, known as **Ring Confidential Transactions** (RingCT), which will obscure transaction amounts on the blockchain. The AEON community plans to adopt this solution as soon as it can be incorporated by the development team. There are more details on the new RingCT protocol in the Monero publication "Ring Confidential Transactions." (See <https://lab.getmonero.org/pubs/MRL-0005.pdf>.)

## 4.3 Coin Minting Process

As mentioned in section 4.1 *Achieving Trustless Transactions*, new AEON coins are distributed over time, to mining applications (called **nodes**), as a reward for calculating the correct Proof Of Work. This section will focus on the details of the coin distribution process.

### 4.3.1 Block Creation

One of the main functions of the mining node is to validate transactions as they are submitted to the network. For a transaction to be valid, it must pass several checks. The transaction must be properly formatted. The coins being spent must be "signed" by the valid owner of the coins. And the coins being spent must not have already been spent by their owner in a previous transaction (a **double spend**). As the node receives and validates transactions, it places them together in a collection, called a **block**.

As mentioned earlier in this paper, AEON implements an algorithm to automatically adjust the allowed block size up or down, based on the previous 100 blocks. This effectively allows miners

to include more transactions in each block when the network transaction rate requires it. Miners are not allowed to increase their block size indiscriminately, and are assessed a **reward penalty** if they create a block larger than the median size. Twice the median size is the largest block allowed. The reward penalty is calculated by the following formula:

$$Penalty = BaseReward * ((\frac{BlockSize}{M}) - 1)^2$$

where

*BaseReward* = the current block reward

*BlockSize* = the size of the new block

*M* = median block size for last 100 blocks

Governing the block size is necessary, to keep the transaction processing speed uniform across all nodes in the network.

#### 4.3.2 Block Time Interval

A single block of AEON transactions is added to the public blockchain once every 4 minutes, *on average*. This timing must be ensured by constantly adjusting the *difficulty* of the Proof Of Work calculation. Otherwise the addition of more miners to the network would result in calculating the correct PoW faster than the desired 4 minutes.

After a mining node assembles a single block of valid transactions, it races with other nodes to calculate the correct PoW. The node which calculates the correct PoW will broadcast its block to the other nodes it knows about, and they will also validate the entire block of transactions. Each node that accepts the block as valid will add the block to its copy of the public AEON blockchain, then broadcast the block to other nodes, and begin assembling a new block. This continues until all the network nodes add the block.

#### 4.3.3 Block Reward

When a mining node calculates a correct PoW and adds a block to the blockchain, it includes a transaction of new coins, paid to its own mining wallet. This payment of new coins is known as the **block reward**. The number of coins in the block reward decreases with each block on a smooth curve, known as the **emission curve**. Each reward is calculated based on the following formula:

$$Reward = \frac{M - A}{2^{18}}$$

where

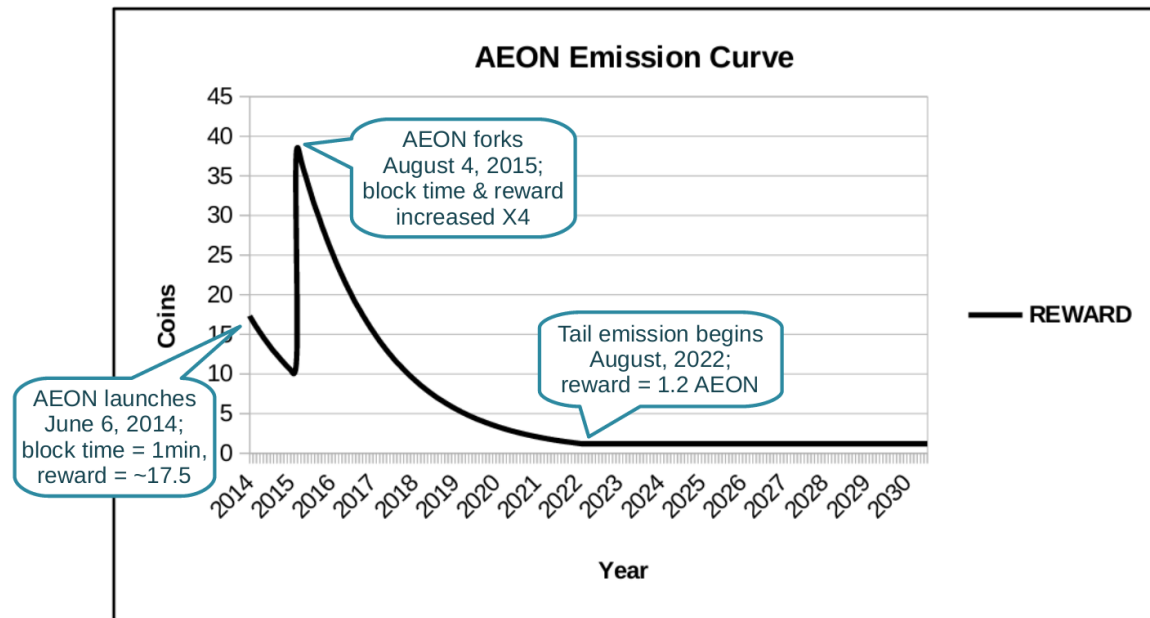
*A* = current supply in coins

*M* = maximum supply in coins =  $\frac{2^{64}-1}{10^{12}} = 18,446,744.073709551615$

Since the current supply of coins (A) increases with every new block, each successive reward will decrease by a small fraction of a coin. The reward continues to decrease until it equals 1.2 AEON per block. At that time, the initial emission curve will end, and the **tail emission** reward (1.2 AEON for each 4 minute block) will begin. The tail is estimated to begin in the July/August

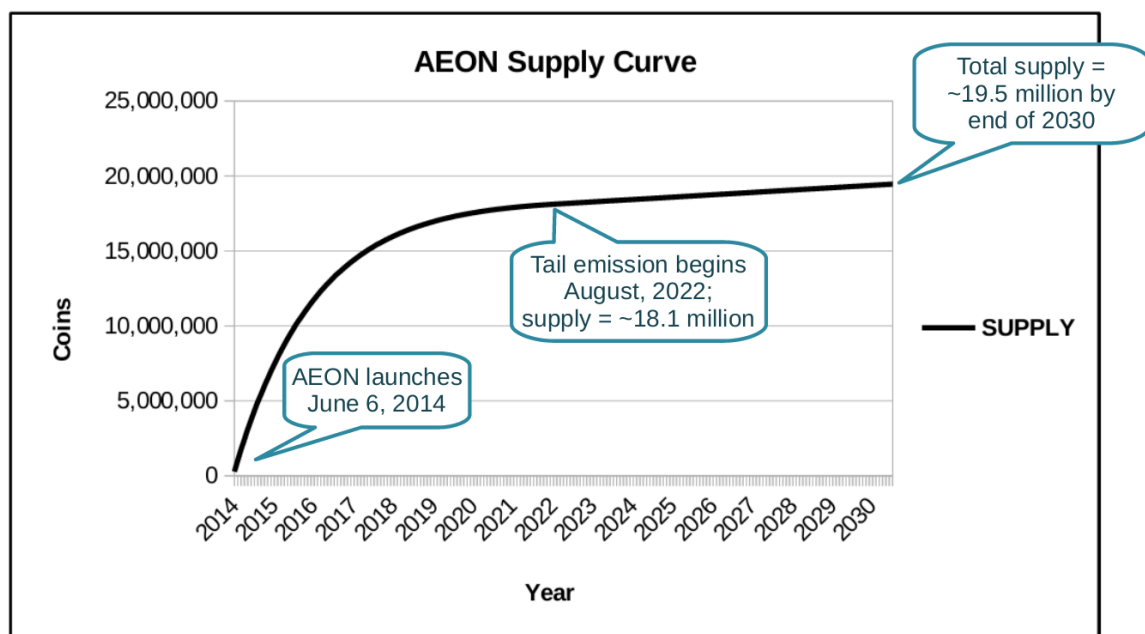
timeframe of 2022.

The following graph shows the number of AEON coins rewarded for each block over time.



Notice that the emission process was modified in 2015, to increase the block creation time from every 1 minute to every 4 minutes. The number of coins paid for each block was also increased by 4 times. This modification greatly reduced the number of block reward transactions on the block chain, while allowing the total number of coins emitted to remain constant.

The following graph shows the total supply of AEON coins over time. Notice that the supply increased smoothly, despite the hard fork mentioned above.



Note that the tail emission has no defined end, and provides an initial inflation rate of less than 1%. During this phase, the rate of inflation decreases as the supply of coins grows by a constant 157,680 AEON per year. By the year 2030, there will be roughly 19.5 million coins in total.

#### 4.4 Transaction Fees

For every transaction, the sender must pay a **transaction fee** in addition to the coins sent. This fee is paid to the miner who successfully calculates the PoW. Thus, the miner receives the Block Reward plus the sum of all transaction fees that were included in the block.

The transaction fee will be higher if the sender increases the priority of the transaction. This higher transaction fee will cause the mining nodes to prefer it when selecting transactions for the next block. Therefore, a transaction's priority, and consequently the speed at which it gets processed, is tied directly to its transaction fee.

The transaction fee will also be higher for transactions that contain more data, since the base fee is calculated on a per-kilobyte basis. (This increase does not impact the priority.) The amount of data in a transaction increases in the following scenarios:

- The amount sent consists of many small amounts that the sender received
- The sender increases the level of privacy, by requesting a higher ring size than the default

##### **Note on transaction fees, block size, and transaction throughput:**

When creating a block of transactions, if the sum of the transaction fees are greater than the block-size penalty, miners are likely to increase the number of transactions in a block. This approach allows the AEON blockchain to self-adjust its processing speed as transaction traffic changes over time, while also creating a dynamic market for transaction fees.



## 5 AEON Community

### 5.1 Links

#### 5.1.1 Social/Community

|                  |   |
|------------------|---|
| Website:         | <a href="https://www.aeon.cash/">https://www.aeon.cash/</a>   |
| BitcoinTalk ANN: | <a href="https://bitcointalk.org/index.php?topic=641696.0">https://bitcointalk.org/index.php?topic=641696.0</a> |
| Discord invite:  | <a href="https://discord.gg/TM8mEsx">https://discord.gg/TM8mEsx</a>   |
| Github:          | <a href="https://github.com/aeonix">https://github.com/aeonix</a> (source, binaries, wallets)                   |
| IRC:             | <a href="https://webchat.freenode.net">https://webchat.freenode.net</a> (channel: #aeon)                        |
| Medium blog:     | <a href="https://medium.com/@AEON_Community">https://medium.com/@AEON_Community</a>                             |
| Reddit:          | <a href="https://www.reddit.com/r/Aeon/">https://www.reddit.com/r/Aeon/</a>                                     |
| Telegram:        | <a href="https://telegram.me/AEONgroup">https://telegram.me/AEONgroup</a>                                       |
| Twitter:         | <a href="https://twitter.com/AeonCoin">https://twitter.com/AeonCoin</a>   |

#### 5.1.2 Block Explorers

|                      |  |
|----------------------|--|
| AeonBlocks:          | <a href="https://aeonblocks.com/">https://aeonblocks.com/</a>  |
| Onion Aeon:          | <a href="http://aeon.lol/">http://aeon.lol/</a> or <a href="http://162.210.173.150/">http://162.210.173.150/</a>                 |
| Onion Aeon Testnet:  | <a href="http://testnet.aeon.lol/">http://testnet.aeon.lol/</a> or <a href="http://162.210.173.151/">http://162.210.173.151/</a> |
| Onion Aeon Stagenet: | <a href="http://162.210.173.151:8083/">http://162.210.173.151:8083/</a>  |
| AEON Charts:         | <a href="https://stoffu.github.io/diff-chart/">https://stoffu.github.io/diff-chart/</a>  |

### 5.2 Mining

#### 5.2.1 Mining Applications

The most popular mining applications are **xmr-stak** and **xmrig**. For additional options, check with the community.

#### 5.2.2 Mining Pools

There are several AEON mining pools operating. It is recommended to join a small to medium sized pool, to spread out the hashes across the network as much as possible. Look on the community sites to find links to current AEON mining pools.

### 5.3 Exchanges

Visit the AEON website to find a current list of exchanges which trade AEON.

### 5.4 Wallets

**aeon-wallet-cli** is the default command-line wallet that comes with the AEON node daemon.

**Aeon GUI** is the official GUI wallet for the core AEON implementation.

**Aeon Monerujo** is a light mobile wallet for Android which connects to a remote node of your choosing, and supports QR Code scanning.

**Aeon Daemon** is a full node that runs on Android, and is available in the Google Play Store. It requires synchronizing the entire block chain to the device.

## 5.5 Development Team

Lead developer: smooth

Contributing developer: stoffu

## 5.6 Current Work and Future Plans

### 5.6.1 Work In 2018

#### Core Development:

- Implement RingCT logic. This is an improvement to ring signatures which also obscures the *amount* of a transaction on the blockchain.
- Implement the Bulletproofs improvement to RingCT. This will drastically reduce transaction sizes, making the blockchain more scalable.

#### Community Work:

- New Community Project Funding System
- AEONStats – extended network and usage stats for the blockchain
- Pay with AEON – payment gateways for popular eCommerce systems
- AEON gambling site
- AEON API – pay Bitcoin with AEON
- Various AEON How-To's

### 5.6.2 Future Plans

- Greater selection of wallets, including mobile and cold storage
- Community-funded marketing
- Additional exchange listings
- Additional AEON integrated services
- More AEON use cases