ATX Coin

(All Together eXchange Coin)

White Paper

ATXC Ver. 1.4

Semtember 12, 2024

A T X C

Table of Contents

1. Private Sale
2. ATX Coin Distribution Roadmap

IV. ATX Coin Platform

1. Peer-to-Peer
2. Neutral Service
3. User-provided

V. Ecosystem Formation & Cryptocurrency Volatility

1. Ecosystem Formation
2. Integration with Visa Card
3. Protection Against Volatility

VI. Decentralization Roadmap

VII. Asset Due Diligence

VIII. Potential Risks of ATX Coin and Disclaimers

I. Understanding CryptoNote Technology

1. Introduction

Bitcoin successfully realized peer-to-peer (p2p) electronic cash, and both experts and the public have assessed public transactions and proof-of-work methods as reliable models. The user base of digital currency continues to grow. Consumers are drawn to its low fees and anonymity, and businesses appreciate the predictable and decentralized issuance. Ultimately, Bitcoin proved that electronic currency could be as simple as cash and as convenient as a credit card.

However, 15 years after its launch, cryptocurrency has not yet become mainstream. Several reasons include the following.

(1) Poor user experience and steep learning curve
(2) Lack of incentives for non-professionals to participate
(3) Significant price volatility
(4) Criticism from the media
(5) Privacy concerns
(6) Lack of payment finality
(7) Legal uncertainty regarding forks and hacking incidents

The inability to quickly address these drawbacks hinders Bitcoin's adoption. In some cases, starting a new project is more efficient than improving an existing one.

This document proposes solutions to Bitcoin's main issues and aims to foster healthy competition in the digital currency system. Through our electronic currency "CryptoNote," cryptocurrency can be revolutionized.

2. Bitcoin's Drawbacks and Possible Solutions

A. Transaction Traceability

In digital currencies, privacy and anonymity are essential. Transactions between individuals should remain hidden from third parties, in contrast to traditional financial institutions. T. Okamoto and K. Ohta described six characteristics of an ideal digital currency, one of which is “privacy, emphasizing that the relationship between users and their purchases must be invisible to others.“ To satisfy the concept of a completely anonymous digital currency, two properties are necessary.

Untraceability

In each receiving transaction, the sender cannot be determined.

Unlinkability

It cannot be proven that two arbitrary outgoing transactions were sent to the same person.

Unfortunately, Bitcoin fails in untraceability. Since all transactions by network participants are public, both the sender and final recipient can be identified. Even when indirect transactions occur, tracing techniques can reveal the sender and receiver.

Bitcoin also seems to fail in meeting the second property. A detailed blockchain analysis by some researchers has revealed the possibility of identifying relationships between Bitcoin network users and their transactions. While many methods have been disputed, there remains a high chance that hidden personal information could be exposed from the public database.

Bitcoin fails to satisfy both properties outlined above, making it an electronic currency system with a false sense of anonymity. Two direct solutions—using “money laundering services“ and intermediaries between open transactions—require third parties, which is a drawback.

Recently, I. Miers proposed a new scheme. “Zerocoin” employs a one-way cryptographic accumulator, allowing users to convert Bitcoin into

Zerocoin, which can be transferred using proof of anonymous ownership instead of a digital signature and public key. However, this method requires significant data size, making it impractical, as early Bitcoin transactions were 30kb (currently up to 4MB). I. Miers predicted that this method might be ignored by most Bitcoin users.

B. The Functioning of Proof-of-Work

Bitcoin's founder, Satoshi Nakamoto, described decision-making in proof-of-work as "one CPU, one vote," advocating for CPU-based pricing (double SHA-256). Users vote based on transaction records, and this process ensures the proper functioning of the system.

However, this model has two major security flaws. First, in order for honest users to maintain control, 51% of the network's mining power is required. Second, for the system to evolve (e.g., bug fixes, security updates), the majority of users must support and agree on changes, as they need to update their wallet software. This voting system is also used in surveys regarding the introduction of certain features.

This model helps to understand the properties of proof-of-work pricing. It should prevent any particular participant in the network from holding too much power. General hardware and expensive custom devices should be equal, but this equality has been lost with the advent of high-performance GPUs and ASICs, which outperform high-performance CPUs using the SHA-256 algorithm employed in Bitcoin.

In Bitcoin, GPU and ASIC miners often have more voting power than CPU owners, which creates a discrepancy in actual voting power. This violates the "one CPU, one vote" principle.

Some argue that since many participants are involved in decision-making,

this issue is not a matter of security, but rather of the honesty of decision-making participants. However, a counterargument exists due to the possibility of low-cost, mining-optimized hardware. For example, imagine a malicious miner using cheap hardware while the global hash rate declines. Even if temporarily, this miner could potentially execute a chain fork and double-spending attack. This document will explain the sufficient potential for such a scenario.

C. Irregular Creation

Bitcoin's generation speed is predetermined. When each block is mined, a fixed amount of coins is awarded, and this reward is programmed to halve approximately every four years. The original intent was to have a smooth exponential decay, but in reality, the pattern is piecewise linear, which can cause issues at certain breakpoints in Bitcoin's infrastructure.

When such problems occur, the rewards are cut in half compared to previous levels. The difference between 12.5 and 6.25 BTC (expected in 2020) may seem manageable. However, the halving from 50 to 25 BTC, which occurred on November 28, 2012, was viewed as quite disruptive in the mining industry. A graph from that time shows a sharp decline in the network hash rate towards the end of November, directly following the halving of rewards. This created the perfect moment for a malicious actor to launch a double-spending attack.

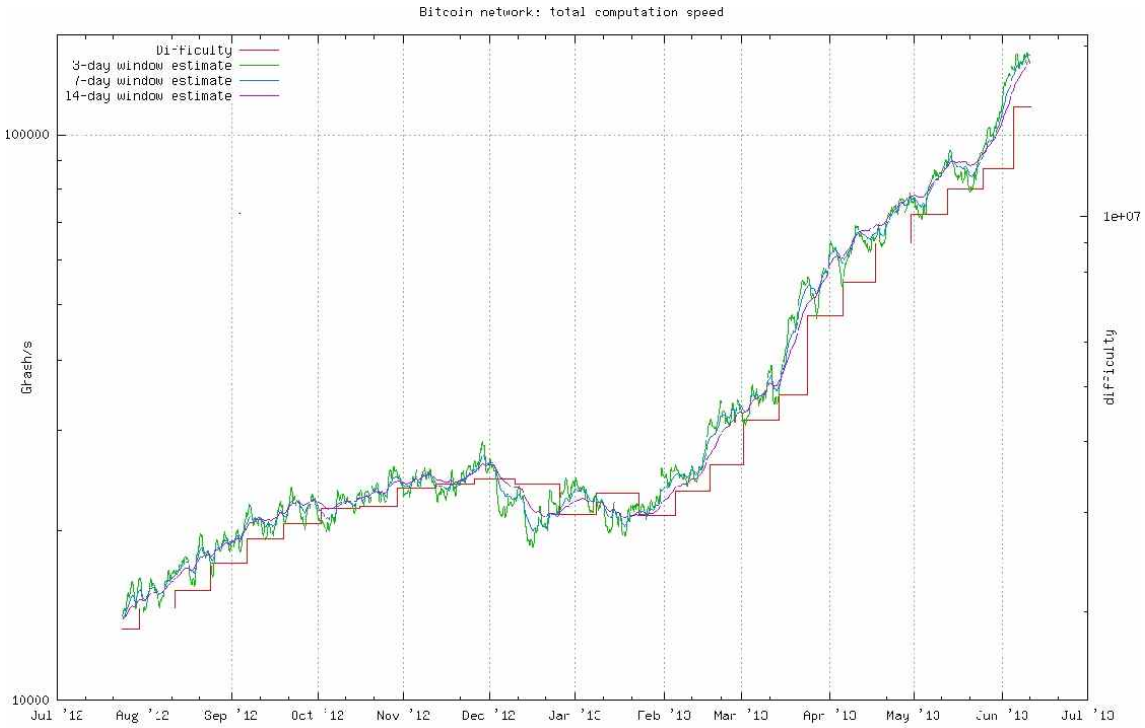


Fig. 1. Bitcoin hashrate chart
(source: http://bitcoin.sipa.be)

D. Difficulty of Modifications (Hardcoded Constants)

Bitcoin has the disadvantage of being difficult to modify, with inherent issues in its original design (such as block frequency, maximum currency supply, and number of confirmations). The most significant problem is the inability to quickly address shortcomings. Failure to make timely modifications could lead to disastrous consequences.

One hardcoded issue is the block size limit of 250KB, which was sufficient to handle around 10,000 standard transactions. By early 2013, transaction volumes had reached this level, leading to a consensus to raise the limit, which was implemented in wallet version 0.8. However, this change resulted in a 24-block chain split and a double-spending attack. Although the Bitcoin protocol itself did not contain bugs, the database engine had problems. If the artificial block size limit had not existed, stress testing could have revealed the issue earlier.

Hardcoded constants also encourage centralization. While Bitcoin is peer-to-peer, most nodes rely on official clients created by a specific group, which can influence protocol changes. Most people accept these changes regardless of their accuracy. In some cases, decision-making processes led to heated debates and even boycotts, indicating that parts of the community and developers may oppose certain changes. This suggests that using a protocol with user-configurable variables could be a more logical solution.

E. Extensive Scripts

Bitcoin's scripting system is vast and includes many complex functions. While it can potentially generate intricate transactions, some functions have been restricted for security reasons, and others have never been used at all. The majority of Bitcoin transactions, including the sender and recipient parts, use the following script.

<sig> <pubKey> OP DUP OP HASH160 <pubKeyHash> OP EQUALVERIFY OP CHECKSIG.

This script is 164 bytes long, and its sole purpose is to verify that the recipient possesses the cryptographic key necessary to confirm their signature.

3. CryptoNote Technology

A. Untraceable Transactions

We propose a fully anonymous transaction method that meets both untraceability and unlinkability criteria. The core feature here is autonomy. A sender does not need to cooperate with another user or trusted third party for transactions, allowing participants to independently conduct trades.

B.. Elliptic Curve Parameters

We intend to use the EdDSA (Edwards-Curve Digital Signature Algorithm), developed by D.J. Bernstein. Like Bitcoin's ECDSA (Elliptic Curve Digital Signature Algorithm), it is based on the elliptic curve logarithm problem and is slightly faster than ECDSA, potentially applicable to Bitcoin in the future.

The general parameters are as follows.

q: a prime number; $q = 2^{255} - 19$;

d: an element of $\mathbb{F}_q$; $d = -121665/121666$;

E: an elliptic curve equation; $-x^2 + y^2 = 1 + dx^2y^2$;

G: a base point; $G = (x, -4/5)$;

l: a prime order of the base point; $l = 2^{252} + 27742317777372353535851937790883648493$;

$\mathcal{H}_s$: a cryptographic hash function $\{0,1\}^* \to \mathbb{F}_q$;

$\mathcal{H}_p$: a deterministic hash function $E(\mathbb{F}_q) \to E(\mathbb{F}_q)$.

C. Terminology

private ec-key is a standard elliptic curve private key: a number $a \in [1, l-1]$;

public ec-key is a standard elliptic curve public key: a point $A = aG$;

one-time keypair is a pair of private and public ec-keys;

private user key is a pair (a, b) of two different private ec-keys;

tracking key is a pair (a, B) of private and public ec-key (where $B = bG$ and $a \neq b$);

public user key is a pair (A, B) of two public ec-keys derived from (a, b);

standard address is a representation of a public user key given into human friendly string with error correction;

truncated address is a representation of the second half (point B) of a public user key given into human friendly string with error correction.

The transaction structure is similar to Bitcoin's. Transaction outputs are possible, and users can sign them with corresponding private keys to send to another address.

Unlike Bitcoin, when a user has a unique private and public key, the sender can generate a one-time public key based on the recipient's address and random data. This way, transactions to the same recipient are carried

out through one-time public keys. Transactions are not sent directly to specific addresses, and only the rightful recipient can restore the private key to receive funds. The recipient can spend the funds using ring signatures, maintaining anonymity while proving ownership. Details of the protocol are discussed in the following sections.

D. Unlinkable Payments

In traditional Bitcoin addresses, once issued, they become abstract identifiers to which money can be sent, linking the recipient's pseudonym. If someone wants to receive unlinkable transactions, they must privately transmit their address to the sender through a private channel. If someone wants to receive multiple transactions without proving they are the same person, they must generate different addresses and not disclose them under the same pseudonym.

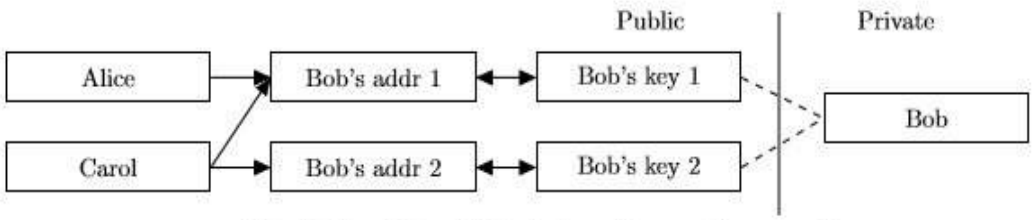


Fig. 2. Traditional Bitcoin keys/transactions model.

We propose a method allowing users to publish a single address while receiving unlinkable payments unconditionally. Each CryptoNote output is essentially a public key derived from the recipient's address and random data from the sender. The main difference from Bitcoin is that all destination keys are unique by default (except when the same sender sends the same data to the same recipient). Thus, "address reuse" is not an issue, and a third party cannot verify any transaction to a particular address.

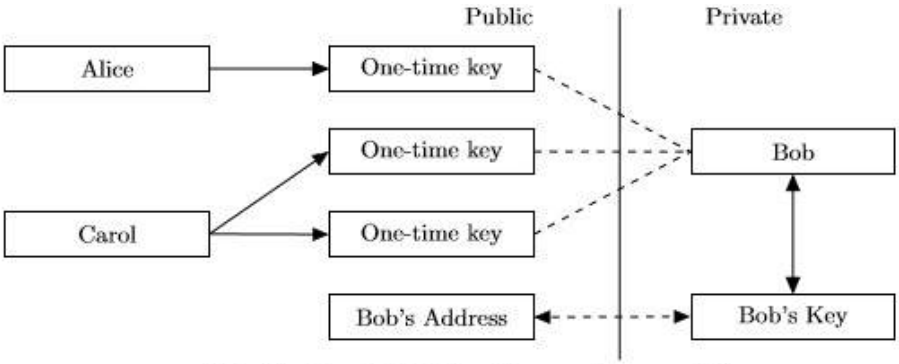


Fig. 3. CryptoNote keys/transactions model.

First, the sender shares their secret through Diffie-Hellman exchange, obtaining half of the recipient's address. Then, using the shared secret and the other half of the address, the sender calculates a one-time destination key. In this two-step process, the recipient must prepare two different ed-keys, so a typical CryptoNote address is almost twice as long as a Bitcoin wallet address. The recipient must also perform a Diffie-Hellman exchange to decrypt the corresponding secret key.

The general transaction process is as follows.

1. Bob publishes his standard address, and Alice wants to send digital currency to Bob. Alice analyzes the address and retrieves Bob's public key (A, B).
2. Alice generates a random value r(one of the two: 1,-2) and calculates a one-time public key. The public key P = Hs(rA)G + B.
3. Alice uses P as the destination key for the output and interprets the R value. R=rG(part of the Diffie-Hellman) Another output can be generated using another public key. (If the recipient's keys differ (Ai, Bi), different Pi will be derived even with the same r.)

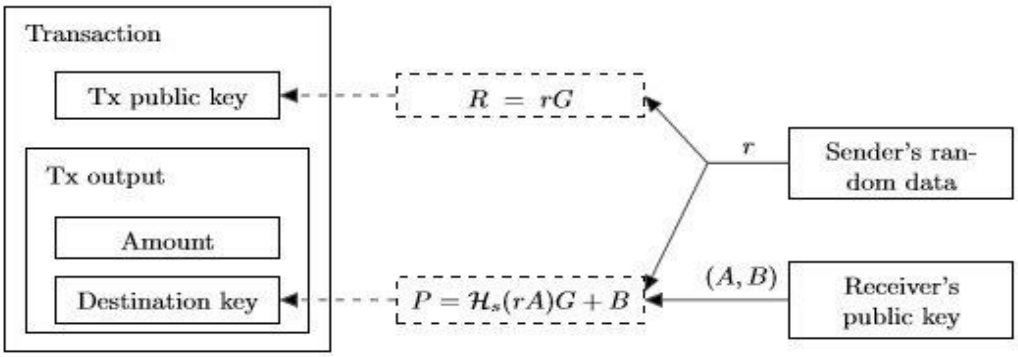


Fig. 4. Standard transaction structure.

4. Alice sends the transaction.

5. Bob checks the transaction with his private keys (a,b) calculating P0 = Hs(aR)G + B. If it is Alice and Bob' s transaction, then aR = arG = rA and P' = P.

6. Bob retrieves the corresponding one-time private key x = Hs(aR) + b. Thus, P = xG, and by signing with x, Bob can transfer the output whenever he wishes.

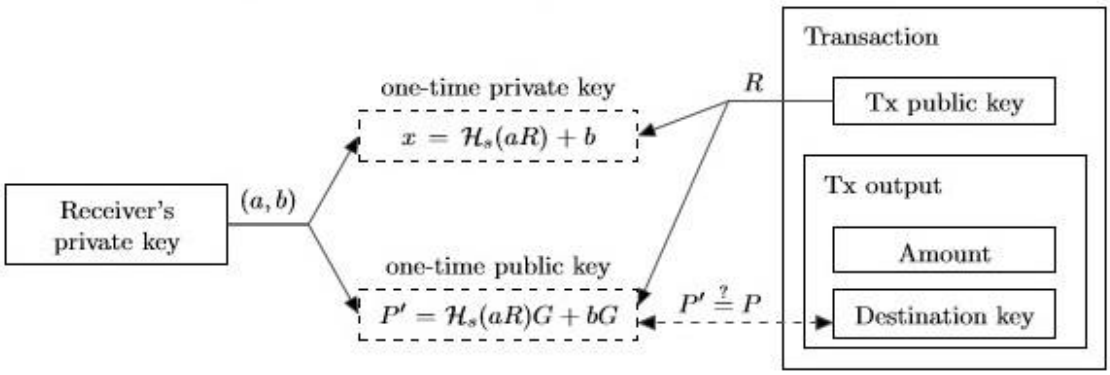


Fig. 5. Incoming transaction check.

Consequently, Bob receives digital currency, and a one-time public key that cannot be linked by a third party is used. Additionally,

* When Bob "recognizes" his own transaction (step 5), he only uses half of his personal information (a, B). This pair, also known as a tracking key,

can be delegated to a third party (Carol). Bob can delegate progress on a new transaction to Carol, which is useful, especially in cases of low bandwidth or poor performance (smartphones, hardware wallets, etc.). Carol does not need to be fully trusted since she cannot know the one-time secret key without Bob's private key.

* If Alice wants to prove that she sent the transaction to Bob's address, she can reveal r or use a zero-knowledge protocol to prove that she knows r (e.g., by signing the transaction with r).

* If Bob wants a traceable and auditable address, he can reveal his tracking key or use an abbreviated address, which only consists of one public EC key. The protocol will derive the rest as follows: a = Hs(B), and A = Hs(B)G. In both cases, it will be known that Bob received the transaction, but no one can spend the funds without knowing the secret key b.

E. One-Time Ring Signatures

Based on one-time ring signatures, users achieve unconditional unlinkability. Unfortunately, traditional cryptographic signatures in typical cryptocurrencies make it possible to trace individual senders and receivers. We aim to solve this issue by employing a different signature method from what has been used in other electronic money systems.
To explain this separate from electronic currency, a one-time ring signature algorithm consists of four algorithms (GEN, SIG, VER, LNK):

GEN: takes public parameters and outputs an ec-pair (P, x) and a public key I.

SIG: takes a message m, a set $\mathcal{S}'$ of public keys $\{P_i\}_{i \neq s}$, a pair (P_s, x_s) and outputs a signature σ and a set $\mathcal{S} = S' \cup \{P_s\}$.

VER: takes a message m, a set $\mathcal{S}$, a signature σ and outputs "true" or "false".

LNK: takes a set $\mathcal{I} = \{I_i\}$, a signature σ and outputs "linked" or "indep".

The idea behind the protocol is fairly simple: A user generates a signature that can be verified against not just one specific public key but a set of public keys. As long as the owner does not issue a second signature using the same key pair, the identity of the signer remains indistinguishable from the other public keys in the set.

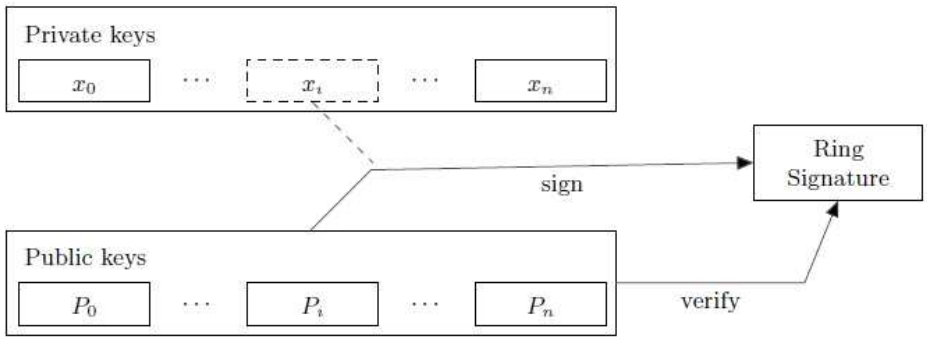


Fig. 6. Ring signature anonymity.

GEN: The signer selects a random secret key x ∈ [1,l−1] and computes the corresponding public key P = xG. Additionally, they compute another public key I = xHp(P), known as the “key image.“

SIG: The signer uses the technique to create a one-time ring signature with a non-interactive zero-knowledge proof. The signer chooses a random subset S0 from the public keys Pi, their own key pair (x, P), and the key image I. The signer’s secret index in the set S (where the public key is Ps) is 0 ≤ s ≤ n.

The signer selects a random set of {qi ¦ i = 0...n} from (1...l) and {wi ¦ i = 0...n,i 6= s} from another range, applying the following transformation.

$$L_i = \begin{cases} q_i G, & \text{if } i = s \\ q_i G + w_i P_i, & \text{if } i \neq s \end{cases}$$

$$R_i = \begin{cases} q_i \mathcal{H}_p(P_i), & \text{if } i = s \\ q_i \mathcal{H}_p(P_i) + w_i I, & \text{if } i \neq s \end{cases}$$

The next step is getting the non-interactive *challenge*:

$$c = \mathcal{H}_s(m, L_1, \ldots, L_n, R_1, \ldots, R_n)$$

Finally the signer computes the *response*:

$$c_i = \begin{cases} w_i, & \text{if } i \neq s \\ c - \sum_{i=0}^{n} c_i \mod l, & \text{if } i = s \end{cases}$$

$$r_i = \begin{cases} q_i, & \text{if } i \neq s \\ q_s - c_s x \mod l, & \text{if } i = s \end{cases}$$

The resulting signature is $\sigma = (I, c_1, \ldots, c_n, r_1, \ldots, r_n)$.

VER: Using the inverse transformation, the verifier can check the signature.

$$\begin{cases} L'_i = r_i G + c_i P_i \\ R'_i = r_i \mathcal{H}_p(P_i) + c_i I \end{cases}$$

The verifier checks whether the following equation holds.

$$\sum_{i=0}^{n} c_i \stackrel{?}{=} \mathcal{H}_s(m, L'_0, \ldots, L'_n, R'_0, \ldots, R'_n) \mod l$$

If the equation holds, the algorithm LNK is executed, and if it doesn't, the verifier rejects the signature.

LNK: The verifier checks whether the key image I has been used in a previous signature. If so, it indicates that the two signatures were made using the same secret key.

Protocol Significance: By applying the L transformation, the signer proves

that x corresponds to Pi=xG. The key image is set as I=xHp(P) to prevent the proof from being forged. The signer proves another proposition, "I know such x that at least Hp(Pi)=I · xˆ-1."

If the mapping from x to I is an injection,

1. No one can recover the public key from the key image, so the signer' s identity remains unknown.
2. The signer cannot generate two signatures with different Is using the same x.

F. Standard CryptoNote Transaction

By combining the two methods—unlinkable public keys and untraceable ring signatures—Bob achieves a higher level of privacy than the original Bitcoin system. Bob only needs one pair of private keys (a, b), and by publishing (A, B), he can send and receive anonymous transactions.

To validate each transaction, Bob only needs to publish two elliptic curve points and add one for each output to verify whether the transaction belongs to him. Bob can recover the one-time key pair (p_i, P_i) for each output and store them in his wallet. Only in the case of a single transaction can the same owner's input be confirmed.

Bob' s input in ring signatures effectively maintains his anonymity. It is challenging to infer who owns the transaction, and even the previous owner, Alice, remains in the dark like any third-party observer.

If Bob transmits several outputs of the same amount to external sources and mixes them, he (or anyone else) cannot know which payment was sent. Outputs can serve as an ambiguity factor among thousands of signatures and can be utilized for hiding purposes. The double-spending check occurs during the LNK step by referencing the set of already-used key images.

Bob can set the level of ambiguity himself. If n=1, it means there is a 50% chance that he sent the output. If n=99, the probability drops to 1%. The resulting signature size increases linearly to O(n+1). Therefore, as Bob's anonymity improves, the transaction fee increases. Bob can also set n=0, using just one component for his ring signature, but in this case, he sacrifices anonymity completely.

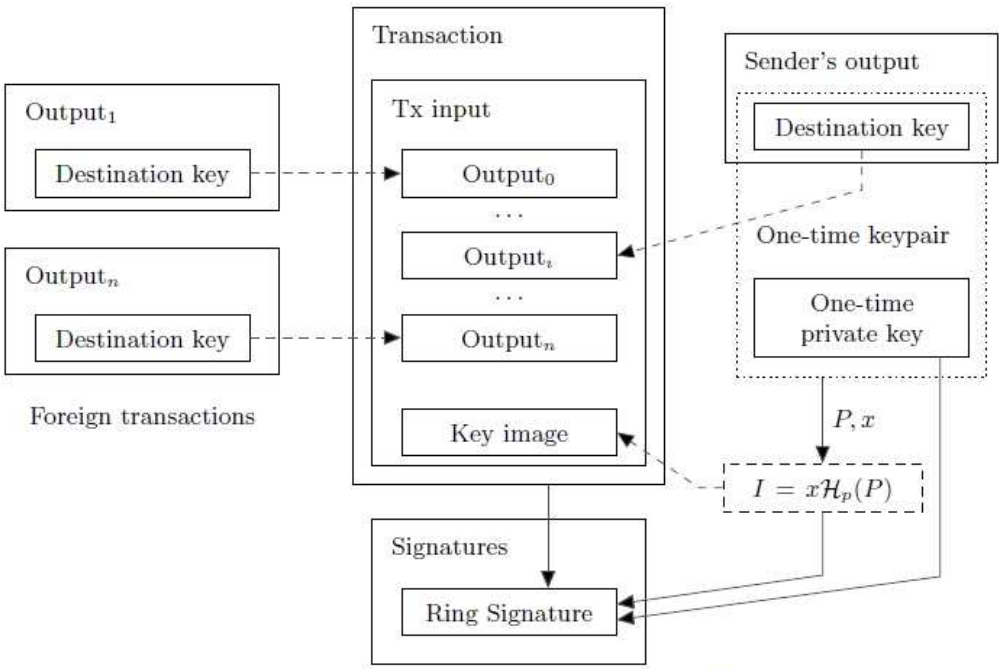


Fig. 7. Ring signature generation in a standard transaction.

G. Equalized Proof-of-Work

In this section, we propose a new proof-of-work algorithm. This algorithm is designed to reduce the disparity between CPU (majority) miners and GPU/FPGA/ASIC (minority) miners. While it is appropriate for some miners to hold an advantage, their investment should increase at least linearly in relation to their power. Generally, the production of specialized devices (e.g., ASIC) should be minimally profitable.

a. Associated Work

In Bitcoin’s original proof-of-work protocol, the pricing function SHA-256 was focused on CPU-based work. It consists mainly of basic logical operators, so its speed is dependent on the processor’s calculation speed, making it perfectly suited for multicore or pipeline applications.

However, modern computers are limited not only by the number of operations per second but also by memory size. The difference in speed between processors can be substantial, but computers are less constrained by memory size.

Memory-bound pricing functions were first introduced by Abadi, defined as “functions whose calculation time is primarily determined by the time spent accessing memory.“ The key idea is to allocate a large block of data (scratchpad) to relatively slow-access memory (e.g., RAM) and perform “accesses to an unpredictable sequence of locations“ within it. The block must be large enough that it is more efficient to store than to recalculate for each access. This algorithm must prevent internal parallelism, meaning that N simultaneous threads would require N times as much memory.

Dwork studied and systematized this approach, which led to the development of another type of pricing function, “Mbound.“ F. Coelho proposed the most effective solution, “Hokkaido.“

The current widely-used function for pseudo-random searches within large arrays is known as “scrypt,“ introduced by C. Percival. Unlike previous functions, scrypt focuses on key derivation and exhibits differences from proof-of-work systems. Nevertheless, scrypt meets our purpose, as it works well as a pricing function in the context of partial hash conversion problems (such as Bitcoin’s SHA-256).

Scrypt is already applied in Litecoin and some other Bitcoin forks. However, this is not truly a memory-bound approach. The “memory access time / total time“ ratio is insufficient, as it only uses 128KB. As a result, GPU

miners can mine nearly 10 times more efficiently, and the potential for cheaper, more efficient mining equipment remains high.

Moreover, due to scrypt's structure, where each block in the scratchpad depends on the previous block, memory size and CPU speed work in inverse proportion. For example, every second block can be stored, and others can be recomputed slowly when necessary. Pseudo-random indices are distributed uniformly, so the expected number of additional recomputations per block is 1/2N is the number of iterations). The overall computation time increases by less than half due to constant time operations like preparing the scratchpad and hashing for each iteration. To reduce memory usage by 2/3, N additional recomputations are needed. To reduce by 9/10, 4.5 additional recomputations are required. In summary, if only 1/s of all blocks are stored, the total computation time increases by less than (s－1)/2. In other words, even a CPU 200 times faster than current chips can only store 320 bytes of scratchpad.

b. Proposal for a New Algorithm

We propose a new memory-bound algorithm for setting proof-of-work pricing functions. This algorithm relies on slow memory access and emphasizes latency. Unlike scrypt, all new blocks (64 bytes in length) depend on all previous blocks. Consequently, "memory savers" will exponentially increase computational speed.

Our algorithm requires approximately 2MB of memory per instance for the following reasons.

1. It matches modern processors' L3 cache, which will be mainstream within a few years.
2. 1MB of internal memory is insufficient for the latest ASIC pipelines.

3. GPUs can handle hundreds of tasks simultaneously but are limited in other ways; for example, GDDR5 memory is slower than CPU L3 cache and, while offering higher bandwidth, has lower random access speeds.
4. As the scratchpad size increases, recomputation time necessarily increases, thus increasing total time. In a peer-to-peer network with low trust, high computational demand can remain a significant vulnerability since nodes must verify the proof-of-work of each new block. If node checks take a substantial amount of time per hash evaluation, nodes become susceptible to DDoS attacks filled with fake objects (nonce values).

H. Additional Benefits

a. Stable Currency Issuance

CryptoNote's electronic coin has an upper bound of MSupply = 2^54 -1 atomic units. This is a technical limit and was not calculated intuitively as "enough coins."

To maintain stability during the issuance process, the following formula is used for block rewards.

BaseReward = (MSupply − A) >> 18

Here, A represents the total amount of previously generated coins.

b. Modifiable Parameters

i. Difficulty

In CryptoNote, difficulty is adjusted after every block. The reaction time to a sudden increase or decrease in network hash rate is minimized, keeping the block rate constant. In the original Bitcoin method, the target period between the last 2016 blocks is compared to the actual time, and the resulting multiplier is applied to the current difficulty. This leads to

significant jumps in difficulty in Bitcoin.

CryptoNote's base algorithm sums all work done by nodes and divides it by the time spent. The unit of work corresponds to the difficulty value of each block. However, due to the inaccuracy and unreliability of timestamps, it is difficult to know the exact time intervals between blocks. If a user shifts the timestamp into the future, the time difference will decrease or even become negative. While rare, this issue is addressed by cleaning up the timestamps and discarding outliers (about 20%). The remaining time values correspond to 80% of the actual time spent between blocks.

ii. Size Limitation

Users vote on the size of the blockchain they store, as they are paying for it. All miners must choose between balancing revenue and the cost of creating a block, finding a balance for their "soft-limit" of block size. However, a hard limit on maximum block size is essential to prevent spam transactions. This value should be adjustable.

Let Mn be the median block size for the last N blocks. Then the "hard limit" for accepting blocks is 2 · Mn. This prevents blockchain bloating while allowing it to grow gradually over time.

Transaction size does not need to be explicitly limited. It depends on the block size. If someone wants to send a massive transaction using hundreds of inputs/outputs (or achieve high ambiguity in ring signatures), they can do so by paying sufficient transaction fees.

c. Transaction Script

CryptoNote features a minimalized scripting subsystem. The sender defines an expression Φ = f (x1, x2, . . . , xn), where n is the number of destination public keys. Only five binary operators are supported: min, max, sum, mul, cmp. When recipients want to spend this payment, they generate $0 \leq k \leq n$ valid signatures and send them as transaction input. The

verification process evaluates Φ with xi = 1, checks valid signatures for public keys Pi, and ensures that Xi=0. If $\Phi > 0$, the verifier accepts the proof.

Despite its simplicity, this approach can handle all cases.

- Multi-/Threshold Signatures: Bitcoin-style "N-of-M multisig" (the recipient must provide at least $0 \leq M \leq N$ valid signatures) is expressed as $\Phi = x1+x2+...+xN \geq M$ (we use standard algebraic notation). Weighted threshold signatures (some keys are more important than others) are expressed as $\Phi = w1 \cdot x1 + w2 \cdot x2 + ... + wN \cdot xN \geq wM$. A master key corresponds to $\Phi = \max(M \cdot x, x1 + x2 + ... + xN) \geq M$. Complex scenarios can thus be expressed simply.

- Password Protection: Holding a password is equivalent to knowing the private key, deterministically derived from the password k=KDF(s). Therefore, the recipient can prove they know the password by providing another signature under key k. The sender simply adds the corresponding public key to their output. This method is significantly more secure than the "transaction puzzle" used in Bitcoin.

- Degenerate Cases: If $\Phi = 1$, anyone can spend the funds. If $\Phi = 0$, the output is unusable forever.

If the combined output script with the public key is too large for the sender, a special output type can be used. The sender provides only a hash, while the recipient sends the data with their input. This approach is similar to Bitcoin's "pay-to-hash." Instead of adding new script commands, such cases are handled at the data structure level.

I. Conclusion

We examined Bitcoin's main shortcomings and proposed potential alternatives. These advantages and our continuous development have led to the creation of the new electronic currency system, CryptoNote, which will

serve as a strong competitor to Bitcoin.

According to Nobel laureate Friedrich Hayek, the coexistence of multiple independent currencies can bring positive effects. Each currency's issuer (or developer) competes to attract users by improving features. Like any other good, currencies have unique strengths and weaknesses, and the most convenient and trusted currency will command the highest demand. If a coin surpasses Bitcoin, it will encourage Bitcoin's developers to accelerate its improvements.

We do not believe that CryptoNote will fully replace Bitcoin. Having two or more strong currencies is a good thing. It is natural for various projects to exist simultaneously in the electronic currency market.

II. Understanding ATX Coin

1. Overview

ATX Coin is designed as a differentiated strategy to overcome the limitations that arise when applying virtual assets to real-life scenarios by incorporating blockchain technology into existing payment methods, ensuring trust.

ATX Coin strives to rapidly gain users by listing on international exchanges and expanding its business scope, with the ultimate goal of implementing a payment ecosystem in partnership with VISA cards. Through partnerships with various companies in sectors such as shopping, healthcare, travel, and fashion, ATX Coin aims to establish itself as an integrated virtual asset for payments.

ATX Coin gradually strengthens its payment system on the platform and enables decentralized services. In addition to acting as a bridge between various cryptocurrencies, it plans to create a strong rewards system to reinforce network effects and activate user curation and user-mediation for

incentives.

ATX Coin aims to raise a fund of 5 billion KRW by issuing 100,000,000,000 [100 billion] coins. The funds raised will be used to integrate the business money (pay) and the virtual currency payment system, provide liquidity to cryptocurrency, expand functionality, and launch aggressive global services through marketing, global translation, and infrastructure.

ATX Coin is the ultimate link between cryptocurrency and the real world. Through the CryptoNote base, which ensures untraceable transactions, CryptoNote uses ring signatures to make it impossible to identify the sender. The coin is backed by an advanced human services industry, which is projected to be worth about 1 trillion dollars globally. Coins can be exchanged on the platform and traded for items or value with real-world skilled technology and functionality.

The coin provides continuous demand and revenue streams for the platform. By gradually integrating traditional currency payment gateways, ATX Coin aims to become a legitimate gateway to the cryptocurrency system, strengthening the entire ecosystem and accelerating adoption as a reserve currency.

ATX Coin sales provide users with the opportunity to secure ATX Coin at discounted prices.

2. Key Features

The ATX Coin platform is a fully functional business marketplace consisting of a B2B and P2P service with Android apps and web-based services. ATX Coin includes tasks used in business operations and digital marketing.

1) Customers can instantly connect and pay for services locally and globally without service fees (or minimal fees). ATX Coin supports most B2B services and P2P services focused on business operations and digital

marketing.

2) As a service provider, users can offer technology and services to other users and receive ATX Coins. Service providers can use ATX Coins in the app or exchange them and instantly send them via P2P transactions.

“Enable the acquisition and transaction of business-related items through cryptocurrency”

"ATX Coin will accelerate the adoption of cryptocurrency in business operations.”

Ⅲ. Coin Sale

ATX Coin has issued precisely 100,000,000,000 [100 billion] coins. Of these, 10,000,000,000 [10 billion] will be used in exchange with the “ModuCoin.” The coins used for the sale amount to 50,000,000 [50 million]. The ATX Coins will be distributed after the private sale.

1. Private Sale

50,000,000 [50 million] ATX Coins will be sold to strategic investors who see long-term value in the project.

The private sale will be conducted in three phases: Private Sale Phase 1, Private Sale Phase 2, and Private Sale Phase 3, from late September 2024

to late November 2024.

The sale of ATX Coin will be conducted through regional and national distributors who contribute to the ATX Coin community in various ways.

The ICO and main sale are planned to take place over 30 days or until sold out, though this has not been finalized.

Any unsold coins at the end of the sale will be transferred to reserves.

* Sale Price: The coins will be sold based on the fluctuating KRW [Korean Won] exchange rate.

The initially provided coins will be restricted from sale for six months (or a period determined by the foundation's regulations).

The reward pools in various forms will be used to encourage users on the platform, as detailed below.

2. ATX Coin Distribution Roadmap

ATX Coin will be exchanged with ModuCoin at a certain ratio for use on the ModuCoin platform. This quantity will be limited to 1/10 of the total issuance, or 10,000,000,000 [10 billion] coins. Beyond this, ATX Coin will be distributed for the following purposes.

1) To cover full or partial costs of stem cell treatment at hospitals partnered with the foundation.

2) To compensate for rewards within the platform, where some or all of the compensation will be paid in ATX Coin.

3) To allow the use of ATX Coin in the platform's shopping mall for purchasing goods or services.

4) To be used as a medium of value exchange, allowing service providers to charge fees in ATX Coin.

5) To function as a store of value by enabling service providers to store payment assets in the ATX Coin wallet.

ATX Coin can be settled in US dollars (USDT) via licensed third parties. To integrate the payment methods within the ATX Coin ecosystem proposed in this white paper, ATX Coin will require additional licensing and regulatory approvals through third parties.

The distribution roadmap for points 1 and 2 may occur simultaneously or in sequence, according to the foundation's regulations.

IV. ATX Coin Platform

ATX Coin will be available for circulation starting in January 2025, after beta testing in October 2024. However, this timing may vary depending on market conditions.

ATX Coin will establish a user base of existing shoppers to ensure successful circulation in the market.

1. Peer-to-Peer

ATX Coin is a peer-to-peer platform where customers can directly select service providers, bypassing third parties, and communicate with them. This platform will provide fast and secure payment services.

2. Neutral Service

ATX Coin is suitable for a wide range of services, from professional to hourly services. It offers various services and technologies to users.

ATX Coin provides flexible capabilities to handle mobile services, offline services, one-time tasks, and periodic group bookings. With this versatility, ATX Coin will play a central role in the cyber world that "Modu Together" aims to create.

3. Stem Cell Treatment Coin

Overseas customers must pay the full amount in ATX Coin to receive stem cell treatment at hospitals partnered with the foundation. As of 2022, the global stem cell therapy market was valued at $5.8 billion (around 7.8 trillion KRW) and is expected to grow by 16.6% annually, reaching $19.1 billion (about 25.8 trillion KRW) by 2030. The foundation will take maximum measures to respond to sharp fluctuations in ATX Coin prices due to the surge in demand in the global market.

V. Ecosystem Formation & Cryptocurrency Volatility

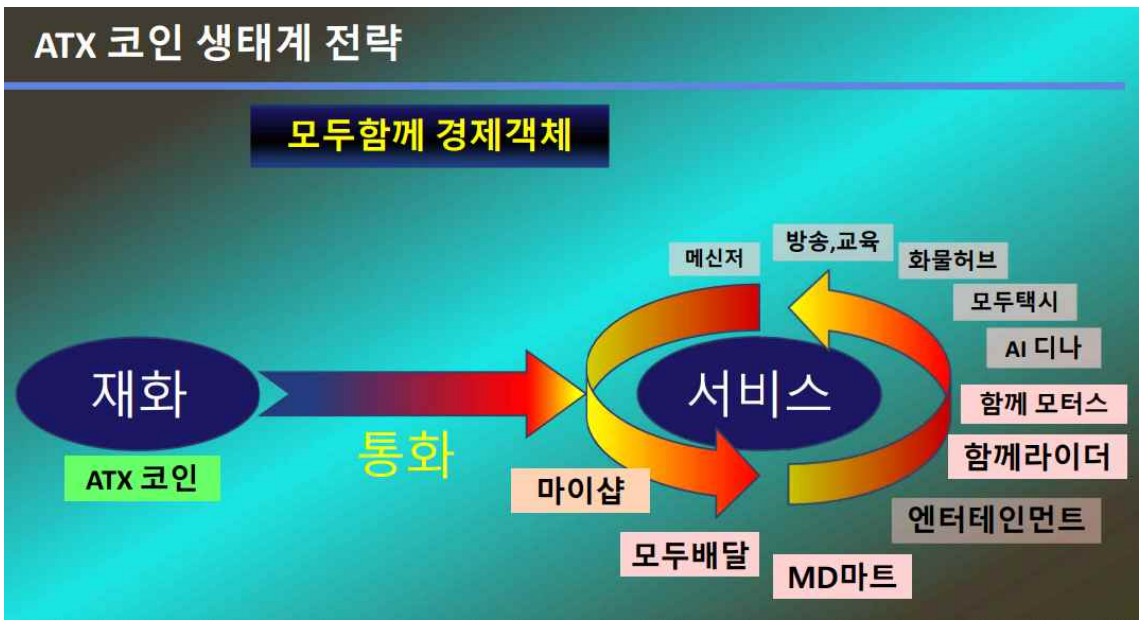
1. Ecosystem Formation

Because ATX Coin operates on its own mainnet, it has advantages in terms of transaction and trading speed, as well as lower fees. This allows for safer use, offering features such as decentralized exchange, browser-based access, open source, wallet encryption, transparency, accountability, multi-party security, and reporting functions.

Unlike Bitcoin, which experiences sharp price fluctuations, ATX Coin has relatively stable prices, making transactions safer and more convenient.

ATX Coin is distributed through exchanges, and users can freely move it on any exchange where ATX Coin is listed. It is also a convenient virtual asset that can be used at all global affiliates.

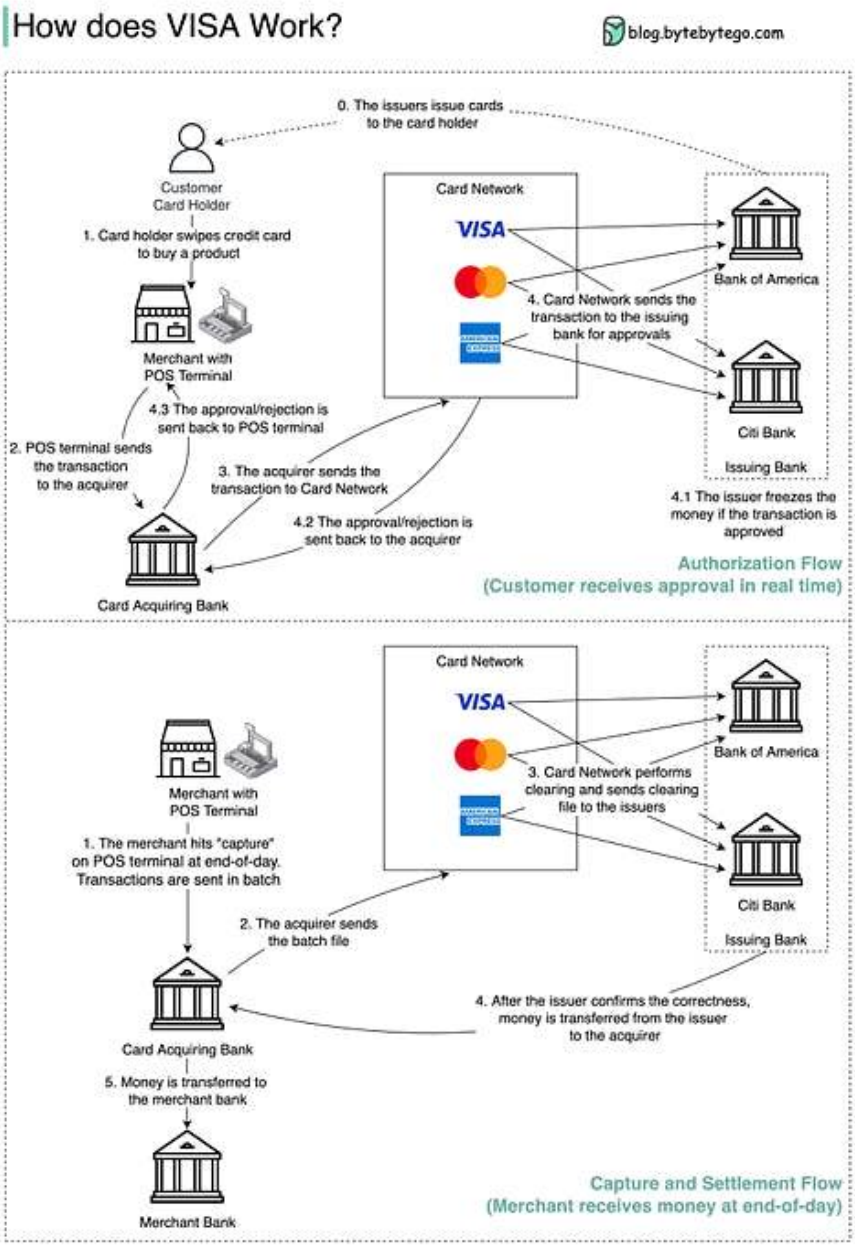
To ensure use in real-life situations, ATX Coin introduces an on/offline wallet system that allows real-time payments in both online and offline stores. This system is not only more convenient than existing payment methods but also offers various events and discount benefits.



2. Integration with Visa Card

As the global economic downturn continues, people are increasingly seeking

safe assets, and the cryptocurrency market is gradually gaining momentum. The cryptocurrency exchanges and related industries are working to build environments where cryptocurrencies can be used more efficiently, drawing public attention. Furthermore, various industries are rapidly expanding the use of cryptocurrencies by implementing systems that incorporate them into their applications. In line with this trend, a patented technology that integrates cryptocurrencies with credit cards has been completed, allowing "instant cash payments via a PG system" both online and offline. This technology connects physical cards issued by credit card companies to the cryptocurrency wallets in exchanges, enabling cryptocurrency usage in real-world transactions.



The introduction of Visa cards linked with cryptocurrencies marks a shift in the perception of cryptocurrencies from mere assets bought and sold in exchanges (and often seen as speculative) to a recognized form of currency.

Customers with a Visa card issued by the exchange can load over 10

different cryptocurrencies and use them anywhere in the world (in over 180 countries).

3. Protection Against Volatility

While the cryptocurrency market offers significant profitability, it is also highly volatile. Due to this volatility, investors may struggle to balance potential gains with risks. Coins with inherent scarcity are not favored as a preferred cryptocurrency due to the price fluctuations caused by speculation.

ATX Coin plans to hedge against volatility by utilizing proven hedging contracts to preserve and maintain the value of ATX Coin. While the coin is being used as a cryptocurrency, its value is guaranteed.

Correct market prices can only be achieved by aggregating and eliminating abnormal values.

4. Dedicated Exchange (Xemii Exchange)

ATX Coin will be listed on an exchange designed specifically to suit the coin's characteristics: the Xemii Exchange. This exchange will form its own payment system. Xemii Exchange exceeds the functionality of existing exchanges and meets customer needs through a new business model linked

with Visa cards. This enables online and offline payments. The system supports secure transactions without the exchange intervening in trades between investors, reducing the risk of delisting. Additionally, the exchange supports peer-to-peer transactions, fulfilling the original purpose of cryptocurrency.

VI. Decentralization Roadmap

ATX Coin recognizes that decentralization is key to scalability and the adoption of cryptocurrencies, and has developed a decentralized roadmap to achieve these goals. This roadmap is provided for informational purposes only.

Q3 2024	Completion and disclosure of the ecosystem for stem cell treatment coins
Q4 2024	Private Sale (Wallet Campaign Launch)
Q1 2025	Start of ModuCoin Swap
Q2 2025	Completion of Staking/Governance Model
Q3 2025	1st phase of Merchant Recruitment for Coin Usage

VII. Asset Due Diligence

ATX Coin will become a new blockchain-based virtual asset in the world's top investments, shopping, and digital marketing sectors. ATX Coin, with its active user base, high-level matching capabilities, multilingual support, decentralization, and rewarding system, represents the first true global service platform to combine meritocracy with cryptocurrency.

VIII. Potential Risks of ATX Coin and Disclaimers

General Coin Information

ATX Coin is a security token with a profit distribution mechanism. Participants in the coin sale must read the entire white paper before participating, understanding the risks involved. Participation in the coin sale is subject to the terms and conditions of the ATX Coin sale and purchase.

Technical Risks

ATX Coin contracts are based on the CryptoNote standard. Every effort has been made to ensure there are no technical errors in the contract, and Mainnet 3.0 is being prepared. Participants must familiarize themselves with blockchain technology to understand this risk. They must also understand the risks related to storing and transmitting private keys.

Hacking and Criminal Activity

The ATX Coin contract address will be provided through http://www.moduch.com. In relation to holding and managing coins, attempts have been made to deceive coin holders into transferring funds to incorrect or fraudulent addresses through computer and email server hacking. This includes social engineering. ATX Coin implements all best security practices to prevent such attacks. Participants must make all reasonable efforts to handle the correct contract address and follow ATX Coin's instructions. Participants must not use external contract addresses posted elsewhere and should follow all security best practices as directed by ATX Coin.

Tax and Regulatory Risks

Coin purchasers must conduct their own due diligence to ensure that they comply with all local laws regarding taxes, securities, and other regulations in their jurisdiction related to virtual currencies. ATX Coin sales may be subject to additional future regulations.

Refunds

Refunds will not be processed. Once a sale is made, it is final and cannot be canceled.

Important Disclaimer

ATX Coin is not a security and does not represent ownership. Therefore, the contents of this white paper should not be used as financial promotion. ATX Coin will operate according to the plans outlined in this white paper (subject to reasonable and objective decision-making that may lead to changes).

By participating in the ATX Coin project, you confirm and fully understand the following and agree to the legal disclaimer below.

1. ATX Coin does not constitute securities in any jurisdiction.
2. Nothing in this white paper is used to solicit or invite investment in any form.
3. The contents of this white paper must not be interpreted arbitrarily or misunderstood. (Including ATX Coin, exchanges, and related platforms)
4. All information contained in this white paper and any future announcements from ATX Coin should not be interpreted as any form of guaranteed profit or benefit, regardless of timing.
5. You acknowledge the inherent risks associated with virtual currencies, including significant price volatility and the unique risks of the virtual currency market, which may include financial losses.
6. There may be risks associated with the operation of ATX Coin's business, the sale of virtual currencies, and related matters.
7. The business of ATX Coin is still in development and may undergo changes after the launch.
8. ATX Coin may send you emails from time to time. These emails will not

request confidential information. Be aware of potential fraud, phishing attempts, and malicious approaches. Do not respond to unofficial inquiries.

9. ATX Coin's business may be interrupted for various reasons, such as lack of public interest or insufficient funds for solution development.

10. Holding ATX Coin does not grant ownership or equity in its businesses.

By acquiring ATX Coin, you acknowledge that you have clearly understood and agreed to the above legal disclaimers for the mutual benefit of both you and ATX Coin.

- End -