EVTC White paper

EVTC
White paper

April 04, 2023

summary

'EVT Coin' is the Mainnet Coin of the Protocol block chain system. EVTC was issued for the purpose of usability in the 'EVENTO Platform'.

'EVENTO Platform' is an online relationship network that makes people around the world to meet every small business owners and venture companies pivoting '645 Game'.

EVT has the characteristics of thorough interchangeability. Individual people can join the 'EVENTO Game' only by securing a game coupon provided by a participating companies. In the 'EVENTO Game' system, nobody can play the game by paying hers(his) own game fee. There is no direct relationship between any individual game participant and game provider. Because a person who want to join this game can only play the 'EVENTO Game' through investment, consumption, and purchase via coin exchange center, the greater the aspiration for the game, the closer the relationship between an individual and the participating companies. When one company want to distribute game coupons to its customers for the promotion, that company must purchase EVT Coins from the exchange and provide it to the Kangaroo Foundation to get the game coupons from the Kangaroo Foundation. Game prize moneys are also paid in EVT coins. The awarded EVT coin leads to consumption, purchase, and investment by participating companies again, for participating companies also need EVT coins. It shall be mandatory that 70% (3.5 billion) of the total issued EVT coins can only be released to welfare organizations or families in crisis around the world. By doing so, EVT coin can firmly establish it's position as a sound global welfare coin. The ultimate goal of EVT Coin is to take care of the weakened or endangered neighbors through social networking, and to lead a transparent donation culture.

TABLE OF CONTENTS

TABLE OF CONTENTS

1. EVENTO Platform

EVENTO platform can be said to be a ‘world social platform’ that encompasses users participating in the game, small business owners, venture companies, and the socially endangered or weakened peoples pivoting ‘645 Game’. ‘645 Game’ is a universal game based on the lottery method that is already in use all over the world, guessing 6 digits out of 45 numbers. We named this game 'EVENTO Game', for it has many similarity to Netflix released globally mega hit Korean drama ' EVENTO Game'. For example, the first prize of 4.56 billion won is also a rearranged number of 645, and it takes a tournament method. However, the most important similarity is that we altogether do not stop in our field and keep try to exert good influences on the world society.

2. Business background

2-1) The number of winning game users shall be enormous.Everyone expects good luck in one’s whole life. Globally, the number of people participating in luck by chance game, like lottery games, etc. shall be very, very enormous. In Korea alone, the number is almost close to 10 million, so it would be very hard to estimate globally. If we can form a ‘world society’ that integrates these kinds of people into one platform, we can expect tremendous synergy effects.

2-2) A regional promotion platform for small business owners is needed.Competition in the same business area is inevitable in all market economy countries. Especially, small business owners have to fight fiercely to attract customers in their business area. For that reason, some companies building delivery app platforms are already monopolized and earning a huge amount of profits. Additionally, the reality is that companies in the distribution business are pouring out a lot of promotion costs through on and off-line. The amount of investing promotional costs in the right place at the right time determines sales performance. Moreover, in these days, due to the aftermath of Covid-19, local small businesses in all over the world are at their peak of difficulties, there is a strong need for social cooperation to overcome that.

2-3) Fostering venture companies for the 4th industrial revolutionA rapid inflection point has already come. Due to COVID-19, the world is facing closer to the era of the 4th industrial revolution.

Even existing companies who could not well be prepared for these trends, or venture companies built on the basis of suitable trendy items with excellent technology, once they failed to connect capital and consumer groups directly, they shall obviously become extinct. In this regards, creating a platform which constructs investment infrastructure for venture companies and connects global consumer groups directly shall be much evaluated.

2-4) Demands of the Welfare Era. In this era of the 4th industrial revolution, 'Humanity' shall become a prevailing key word and a main trend of this era. So 'all for one and one for all' welfare era must be realized embracing the whole world beyond the border of country. Now, birth of 'the platform for the purpose of welfare' (EVENTO Platform) is strongly demanded and it is expected to hit the whole world very strongly.

2-5) Age of Social CurrencyToday's flourishing Internet, SNS, and Mobile Systems are creating a new social trends that goes beyond borders of all countries. Moreover, with the progressing of t ranslation technology, language barriers are also being overcome, and a large majority of people is prepared to admit multi-cultural era. Reflecting this, Cryptocurrency as a social currency has already established itself as another monetary system that's coexisting with the traditional currency system. Depended on these trends, we were able to create the 'EVENTO platform'.

3. Purpose of EVT Coin Issuance

The purpose of the 'EVENTO platform' is to connect small and medium sized companies who are lack of marketing ability with customers easily, utilizing people's yearning for good luck via 645 games (a game to guess six numbers from 45 numbers) and by doing so, we can possibly embrace the socially endangered or weakened people all around the world. It shall become a 'borderless society' that does not stay in one country but encompasses the whole world at the same time. Moreover, the ultimate purpose of this mobile-based platform is the welfare of the socially alienated or marginalized classes. Since 70% of EVT Coin is designated to be released only for welfare purposes, not for business, that amount will surely be used for the socially endangered or weakened people . We, Kangaroo Foundation developed this platform solely for the 'Kangaroo Movement' meaning 'Realizing the society where the endangered or weakened people can jump for the future with us'.

4. Business Goals

1) Establishing platform membership of more than 100 million people world widely.

2) Realization of investment in venture companies worthing 4 trillion KRW(4 billion USD)

3) Realizing more than 1 trillion KRW(1 billion USD) social donations for the revival of the endangered or weakened people world widely.

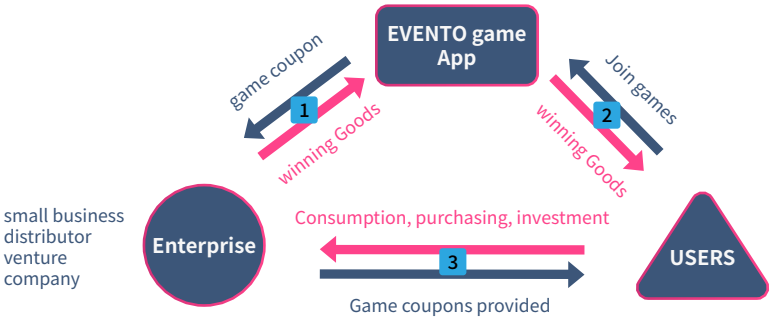
4) Issuance of 'EVT Coin(utility coin)' and make them current world widely so that one can use it commercially.

5) Making EVT Coin become a 'world welfare coin' and realizing a transparent donation culture

5. EVENTO Platform Description

5-1) Dominant Features and Advantages

'EVENTO Game' is a 645 lottery game. But, unlike the existing way of selecting the winner(users randomly selects 6 numbers first and final 6 numbers randomly decided on a last date), 6 winning numbers are selected randomly and shown to each user in advance and the system randomly selects 6 numbers each time when the users playing the game. Users can see the result of the the game immediately, so the users can have the advantage of being able to enter the game anytime, any where she(he) wants with their mobile phone. To prevent arbitrary manipulating the winning probability and the designation of the winner, 'EVENTO Game' developed a technology to generate numbers from hash values (patent application) applied with a block chain system (distributed information storage system), and totally blocked the source so that it could not be arbitrarily manipulated on a specific computer.This will be the world's first and fairest lottery game ever.
In addition, the 'EVENTO Game' is characterized as a platform-based game. In other words, it has a structure in which the participant cannot pay the game fee directly to the game service provider without going through the member companies. Users can be allowed to join the game only by coupons obtained by ① consuming in the local commercial area or ② purchasing from a distributor or ③ investing in venture companies, or ④ participating in corporate advertisements. The feature of 'EVENTO Game' is that it can be played only with gifts (coupons) obtained from social and economic activities cause gambling is a serious social problems that destroys the whole life of engaged people and family.



1 The company provides the winning product to the 'EVENTO platform' and Receive a game coupon proportional to the winning product from the platform.

2 Sales (investment) margin is provided as game coupons (gifts) to the Users propotion to the amount consumed, purchased, or invested in the business.

3 Individuals can use the game coupon they received as a gift to join the EVENTO Game Sign up to play a game, and can get prizes according to the rules (corporate provided by them).

※ Customers can also directly scan the QR mark on the game coupon or the company can send coupons to the customer's mobile phone.

5-2) Legal review

[Act on Special Cases concerning Speculative Behavior, Etc., Regulation and Punishment] (Enforced on January 1, 2021, Act No. 17689, hereinafter the 'Speculative Behavior Control Act') states, "The wealth or property gains and losses that were collected from various indivisuals are given to a specific person determined by the accidental result, the act of giving property gains or losses to that specific person is defined as a 'speculative act'". The important issue here is that wealth or property gains are collected from several people, but 'EVENTO Platform' is not collecting property or property interests from individuals. In the 'EVNETO Platform', there is no way for individuals to directly join the game, and game coupons (property you can participate by receiving prize profits; it is not a fixed profit such as points or discount coupons, but a reward for the probability that a difference may occur depending on whether you win or not). If this platform collects points (coupons) provided in neighborhoods across the country and provides them to one person with a probability, it will violate the 'Speculative Behavior Control Act'. But in EVENTO Platform, companies provides the right to join the game for users, equivalent to the amount paid by their customers (promised), this has been interpreted by the lawyers as not being speculative.

6. How to play

'EVENTO Game' is a ‘Delegation’ 645 game . This is the world's first attempt, and it is divided into 'Preliminary Level Game' and 'Upper Level Game’. When a user joins the game, she(he) enters into the 'Preliminary Level Game' first, where the user with 6 correct digits shall be born as 1st prize winner at a probability of 1 Vs. 25,000, 5 correct digits shall be 2nd place, 4 digits the 3rd place, and 3 digits the 4th place. The 1st prize winner shall be awarded EVENTO Coins worth of 456,000 KRW, and the 2nd~4th place shall be awarded each corresponding prize(a gift certificate from a local vendor). What is unusual here is the system of becoming a ‘Delegate’. This means that the 1st prize winner in the game will be given the status of a ‘delegate’. That person is entitled to participate in the 'Upper Level Game'. The 'Upper Level Game' consists of 4 Levels Game, ‘100 Game' when 100 delegates are full, ‘1,000 Game' when total delegates reaches 1,000, and ‘10,000 Game’ when 10,000 delegates, finally, ‘40,000 Game’ when 40,000 delegates are full. Once one become a delegate, she(he) shall be invited to all levels of games, and one selected winner in each level of game shall be given the corresponding prize.

Top 100 game

100 delegates
Award : Corredponding 4,560,000 KRW

Top 1,000 game

1,000 delegates
Award : Corredponding 45,600,000 KRW

Top 10,000 game

10,000 delegates
Award : Corredponding 456,000,000 KRW

FINAL GAME

40,000 delegates
Award : Corredponding 4,560,000,000 KRW

※ Displayed in KRW is just for the purpose of understanding, actually the corresponding EVT Coins shall be given as a prize not in cash after deducting ‘taxes and other necessary costs(10%)’ from the prize amount.

EVTC

One of the unique feature of 'EVENTO Game' among the game methods is the use of QR code in non-face-to-face situations. Once the main company prints (stores) a QR code which specifies the game numbers for each advertisement or product, the user can get the corresponding ‘EVENTO Game’ chances when they take a picture with their mobile phone.

6-1) Token Structure

Since the ‘EVENTO platform’ is a platform where users and business entities from all over the world can join, joining entities shall provide their own winning products. In that case, it shall cause a great confusion. To prevent those kinds of confusion, we use encrypted currency as a common product of the ‘EVENTO platform’. In order to distribute game coupons to their customers, companies must provide us with a winning product equivalent to that amount of ‘EVT Coin'. Although ‘EVT Coin' is based on the Main Net, it is not a mining type coin, but an already issued 5 billion tokens. Firstly, only 5% of the tokens are released to contributors, and the rests are locked and stored. And every time an operating corporation in each country is established, 0.1% is allocated to 100 countries and released to that country. The remaining 70%, other than those kept by the founder Team, shall be released to welfare organizations around the world through the decision of ‘Releasing Committee’ (members : Founder Team, Advisory lawyers, Accountants, and Board of Directors of Kangaroo Foundation)’. This is because the ‘EVENTO platform’ is aiming for solid social solidarity including social welfare. Since the mining method is ultimately owned by the capitalist, ‘EVENTO Coin (EVTC)’ adopted the issued token method for the socially underprivileged. Whenever the committee decides to release EVT Coins, those coins shall be used for social welfare organizations or individuals in the blind spot of welfare.

6-2) How to Join the Platform : Business Entities

Companies around the world should sign up as members 0f the ‘EVENTO platform’ in order to meet the demands of users who want to join ‘EVETO Games’ or to secure those users as their customers. A specific manager page is given to the registered member companies. ① Game coupon status page ② Advertising video file upload page ③ Advertisement exposure data page ④ QR code automatic generating page, etc. A certain amount of coins are purchased from the exchange center and send to us, and we shall put game coupons in proportion to the amount of tokens deposited in the company's game coupon wallet.

Companies can send game coupons to their customers directly from their wallets, or generate a QR code so that when the customer scans the QR code, the specified number shall be sent to the customer's wallet. Every time a customer plays a game, the company is possible to maximize the promotional effect of the company by displaying the visual advertising files.

6-3) How to Join the Platform : Venture companies

Venture companies who want investment from users of the 'EVENTO platform', must provide company information to us, and we will decide whether to register as an investee company or not through expertise reviewing. Registered venture companies are posted on the 'EVENTO Platform', and users and member companies of the EVENTO platform decide whether to invest or not, based on probability of venture company and the degree of game coupons offered.Venture companies provide investors with game coupons as proportion as to the invested amount, and obtain advertising opportunities as many as the number provided from the company. In the ecosystem of the 'EVENTO platform', venture companies can secure investment, publicity, and acquiring customers all at the once, increasing the probability of success.

7. EVENTO Technical Description

7-1) Lottery number by blockchain hash value

A block contains various information such as transaction history, block creation time, and node value, and it is made into a hash value. And using this hash value of fixed position, 6 digits are digitized through the open official logic. This number will be linked with the hash value, SEQ, and the 6-digit number will be transparently disclosed using this hash value. Since many hash values are needed in a short time, hash values are generated in advance through multiple node servers, and then the hash value is stored to extract the only single first-place value and reveal the first-place number. The lottery is a SEQ random lottery, and the corresponding link number value of SEQ is matched with the lottery number and the result is shown. The lottery number of the hash value is opened in the form of hiding the hash values of the corresponding value in the random SEQ. This process is logicized and repeated in the form of a tournament to complete the EVNETO game tournament.

7-2) Mainnet Summary

The mainnet of EVNETO virtual currency is CryptoNote based. It is a blockchain that is grouped before the public key is received, making it impossible to identify the sender, but it is also the protocol we chose because of its fast and practical advantages.

Most of the basic functions of blockchain cryptocurrencies are similar. With security and transparency, anyone can make reliable and secure transactions. However, like Bitcoin or Ethereum, POW (Proof of Work) mining can cause environmental destruction due to huge electrical energy consumption, so we did not adopt this method and adopted a more future-oriented technology.
We built our own mainnet and repeated a lot of R&D and testing to build a safer and faster mainnet node with the characteristics of the current block chain. In addition, we are building a convergence system in various fields of society by creating and providing various DAPPs. The advantage of EVENTO is that it is more stable and faster than existing cryptocurrencies, and advertising platforms, investment platforms, shopping malls, live commerce, metaverse, and history tracking system. , and payment systems, etc., provide fast linkage and perfect compatibility. In addition, distributing additional functions based on our extensive experience with overseas global exchanges, and we are continuously developing and distributing additional functions in the form of layer 2.

7-3) Cryptonote Technical Details

7.3.1) Untraceable Transactions

We propose a completely anonymous transaction method that satisfies both non-traceability and connectionless conditions. The key part here is autonomy. The sender does not need to cooperate with other users or trusted third parties for the transaction, so each participant transacts independently.

7.3.2) Elliptic curve parameters

We are going to use EdDSA, and this is D.J. Developed by Bernstein. Similar to Bitcoin's ECDSA, it is based on the elliptic curve logarithm problem, and our method may be applied 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 $E(\mathbb{F}_q) \to E(\mathbb{F}_q)$.

7-3.3) term

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 that of Bitcoin. Transaction output is possible, and it can be signed with the corresponding private key and sent to another address. The difference with Bitcoin is that when a user has a unique private and public key, the sender sends the recipient's address and random data Based on this, a one-time public key is generated. In this way, transactions to the same recipient are done through a one-time public key. It is not sent directly to a specific address, and only legitimate recipients can receive funds by restoring this portion of the private key. Recipients can spend their funds using the ring signature, maintaining anonymity while retaining ownership. Details of the protocol are described in the next section.

7-3.4) Unconnected Payments

A traditional Bitcoin address, once issued, becomes an abstract identifier for payments to be made, tying the two together, and ties to the recipient's pseudonyms. If someone wants to receive an untied transaction, they must send their address to the sender over a private channel. If a person wants to receive multiple transactions that are not authenticated as the same person, they must produce all the different addresses and not disclose them under their own pseudonyms.

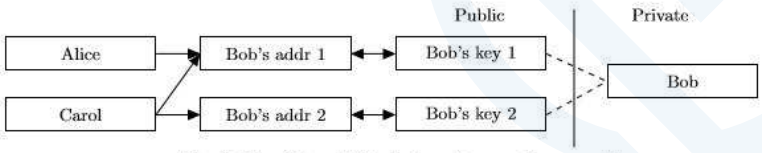


Fig. 2. Traditional Bitcoin keys/transactions model.

We propose a way for users to publish a single address and to issue a single address to receive unconnected payments unconditionally. Each CryptoNote output is basically a public key method, and is generated from the receiver's address and sender's random data. The main difference with Bitcoin is that every destination key is unique by default (unless the same sender sends the same data to the same recipient). So there is no problem with “address reuse” in this way, Third parties cannot verify transmissions to specific addresses)

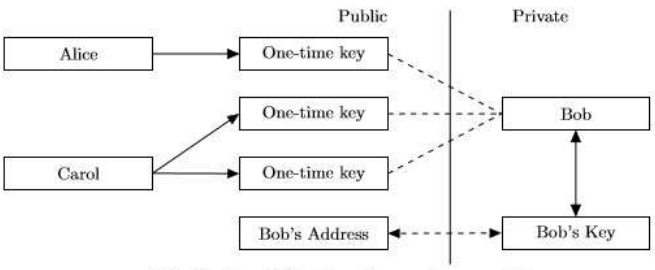


Fig. 3. CryptoNote keys/transactions model.

First, the sender shares the secret of his data using a Diffie-Hellman exchange, and gets half the recipient's address. It then calculates a one-time destination key using the shared secret and the other half of the address. In this two-step process, the recipient needs to prepare two different ed-keys, so a typical CryptoNote address is almost twice as long as a Bitcoin wallet address. The receiver must also perform a Diffie-Hellman exchange to decrypt the corresponding secret key.
A typical trading process is as follows:1. Bob has published his standard address, and Alice wants to send him digital money. Alice parses the address and gets Bob's public key (A,B)2. Alice generates a random r (one of 1, -2) and calculates a one-time public key. 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 exchange) Another public key can also be used to produce different outputs (different recipient keys ((Ai, Bi) will yield different Pi for the same r)

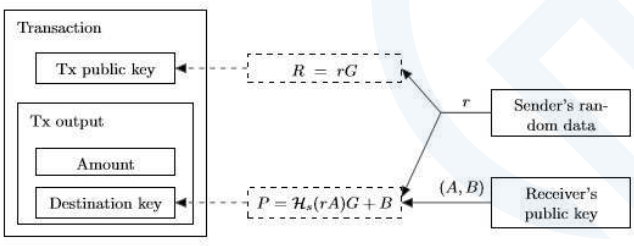


Fig. 4. Standard transaction structure.

4. Alice sends a transaction.

5. Bob checks the transaction using the private key (a,b), and calculates P0 = Hs(aR)G + B. If the transaction is between Alice and Bob, then aR = arG = rA and P' = P.

6. Bob can get the corresponding one-time private key. x = Hs(aR) + b. So P = xG, and by signing with x, we can send the output when we want.

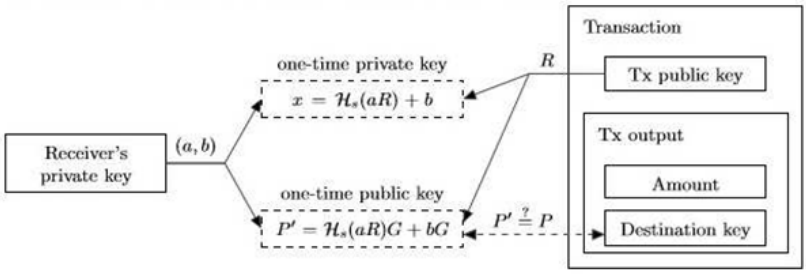


Fig. 5. Incoming transaction check.

As a result, Bob will be paid in cryptocurrencies, and a one-time public key that cannot be linked to a third party is utilized. Additionally, *Bob "recognizes" his own transaction (step 5), effectively using only half of his personal information (a, B). This pair is also known as a tracking key and can be passed on to a third party (Carol). Bob can delegate the progress of the new transaction to Carol. This is especially useful when bandwidth is low or performance is poor (smartphone, hardware wallet, etc.) To verify a transaction sent by Bob to Bob's address, he either reveals r, or uses a zero-knowledge protocol to prove that he knows r (for example, he can sign a transaction with r). If Bob wants a reachable and searchable address, he can publish the tracking key or use the omitted address. This address means only one public ec-key, the rest the protocol requires is derived as follows: a = Hs(B) and A = Hs(B)G. In both cases, everyone knows that Bob has received the transaction. But, of course, without knowing the secret key b, no one can spend those funds.

7-3.5) disposable ring signature

Based on a one-time ring signature, users have unconditional disconnection. Unfortunately, cryptographic signatures in common cryptocurrencies allow individual senders and recipients to gain traceability. The solution is to use a signature method that is differentiated from existing electronic money.First of all, I will explain the ring signature algorithm separately from electronic money. One-time ring signature contains 4 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 $\mathcal{S} = \mathcal{S}' \cup \{P_s\}$.

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 creates a signature that can be checked against a set of multiple public keys, rather than one specific public key. Unless the owner issues a second signature using the same key pair, the signer's identity is indistinguishable among the same set of public keys.

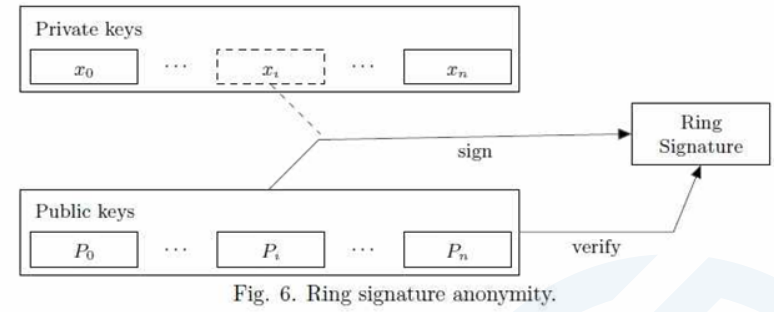


Fig. 6. Ring signature anonymity.

GEN: Th00e signer chooses a random private key x ∈ [1,l−1] and computes the corresponding public key P = xG. In addition, we need to compute another public key I = xHp(P), which is called "key image".SIG: The signer utilizes the technology to generate a one-time ring signature along with a non-interactive zero-knowledge proof. The signer selects a random subset S0 from other users' public keys Pi, their own keypari (x,P), and key image I. Let the signer's secret index in S (his public key is Ps) 0 ≤ s ≤ n. The signer is a random {qi | Choose i = 0...n} and from (1...l) {wi | i = 0...n,i 6= s}, applied to the following transformations:

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

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

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 inverse transformation, verifiers can check signatures

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

As a result, the verifier finds the picture above, and if the equation holds, it runs the algorithm LNK. Otherwise, the verifier will reject the signature. LNK: The verifier checks whether I was used in a previous signature. Multiple uses would suggest that the two signatures were made from the same secret key. Meaning of the protocol: By applying the L transform, the signer proves that such x is at least Pi=xG.

To make the proof non-repeatable, set the key image to I=xHp(P). The signer uses the same coefficients (ri,ci) to prove that the almost identical proposition “knows that such x is at least Hp(Pi)=I·x^-1”. If the correspondence from x to I is injection If it is a mapping, 1. No one can restore the public key from the key image, and the signer is unknown. You cannot produce two signatures with different Is and the same x.

7-3.6)

7-3.6.1) Standard CryptoNote Transactions

By combining the two methods of connectionless public key and non-traceable ring signature, Bob has an advanced level of privacy compared to the original Bitcoin method. Bob only needs one private key (a,b), and by revealing (A,B), he can send and receive anonymous transactions. To validate each transaction, Bob additionally issues only two elliptic curves, adding one per output to verify that it is Bob's own transaction. Bob restores a one-time keypair (pi, Pi) for each output and stores it in his wallet. Only a single transaction can be identified as an input of the same owner.ring As for the signature, Bob's input can be effectively kept anonymous. It is difficult to infer who the transaction belongs to, and Alice, the former owner of the th, has no information like other third-party observers. If Bob sends n outgoing outputs for the same amount and shuffles them, then Bob himself (no one else) has no way of knowing which of these payments was sent. The output can be utilized as an ambiguity factor in thousands of signatures, and cannot be hidden. By checking from a set of already used key images, a double spend check occurs in the LNK phase. Bob can set his own ambiguity degree. n=1 means that there is a 50% chance that he sent the output. When n=99, it represents a probability of 1%. The resulting signature increases linearly by O(n+1). Therefore, if Bob's cost of anonymity increases, the transaction fee increases. Also, Bob can set n=0 and create his own ring signature with just one component. But in this case he has no guarantee of anonymity at all.

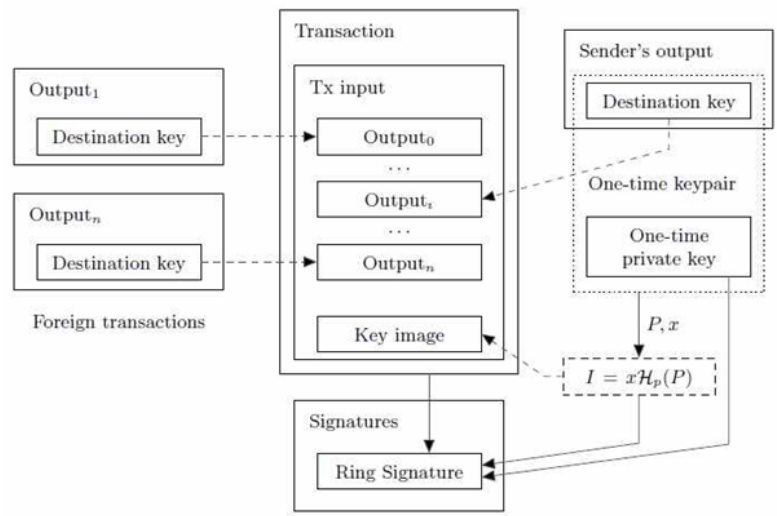


Fig. 7. Ring signature generation in a standard transaction.

7-3.6.2) Equalized Proof-of-work

In this part, we would like to propose a new proof-of-work algorithm. This is to bridge the gap between CPU (majority) miners and GPU/FPGA/ASIC (minority) miners. While it is appropriate for some miners to gain the upper hand, their investment should increase at least linearly with respect to power. In general, special-purpose devices (note: ASICs, etc.) should be as profitable as possible.

7-3.6.3)Related works

The original Bitcoin proof-of-work protocol used the CPU-focused pricing function SHA-256. It is mainly composed of basic logical operators and is perfectly suitable for multicore/conveyer application because it changes according to the processing speed of the processor.

However, modern computers are limited not only by the number of operations per second, but also by the size of memory. The difference in speed between processors can be significant, but not much in memory size.A function that determines a price based on memory was first introduced by Abadi and was defined as “a function whose computation time is mainly determined by the time of access to memory”.

The core idea is to create an algorithm that allocates a scratchpad, a large block of data, into memory (such as ram) that can be accessed relatively slowly, and within it "performs an unpredictable sequence of locations access". The block must be large enough to save it rather than recalculating it for each access. This algorithm must avoid internal parallelism, so N concurrent threads must require N times as much memory. Dwork has researched and codified this approach, which allows Another way, “Mbound” could be born. F.Coelho suggested the most effective solution “Hokkaido”. Currently, the commonly used method of pseudo-random searches within large arrays is called “scrypt”.(C. Percival) Unlike the previous functions, it focuses on the core derivation, and there is a difference from the proof-of-work system. Despite these facts, scrypt can serve our purpose, which is that it works well as a pricing function in partial hash transformation problems. An example is SHA-256 in Bitcoin. Currently, scrypt has already been applied to Litecoin, and has been applied to some other Bitcoin forks as well. However, this application is not actually a memory-based approach. “Memory access time / total time” does not have enough space, as it only uses 128KB. This allows GPU miners to mine almost 10 times more efficiently, and there is a good chance that inexpensive yet highly efficient equipment will emerge. Moreover, by writing the script, every block on the scratchpad will be replaced with the old one. , so memory size and CPU speed move in inverse proportion to each other. For example, every second block can be saved, and all other blocks can be recomputed in a slow manner only if necessary. Pseudo-random indexes are distributed in batches, so the expected value of recalculation of additional blocks is 1/2N (N is the number of iterations). Due to constant time operations such as preparing the scratchpad and hashing it for every iteration, the overall computation time increases by less than half. An additional recalculation of N is required to reduce memory usage by 2/3. Reducing 9/10 would require an additional recalculation of 4.5. In summary, if you store only 1/s of all blocks, it will increase less than multiplying by (s-1)/2. In other words, a CPU 200 times faster than a modern CPU can only store 320 bytes of scratchpad.

7-3.6.4) Proposal of a new algorithm

We propose a new memory-bound algorithm for the proof-of-work pricing function. It relies on random access to slow memory, emphasizing latency dependencies. Unlike scripts, everynew block (64 bytes long) depends on all previous blocks. As a result, a memory saver (“memory-saver”) will exponentially increase computational speed. Our algorithm requires around 2MB per instance for the following reasons. Suitable for L3 cache per core on modern CPUs, This is a specification of CPUs that will become mainstream in a few years. For a modern ASIC pipeline, 1MB of internal memory is inadequate. It can handle instances of uddn tnqor on the GPU concurrently, but GDDR5 memory is slower than the CPU's L3 cache, and the bandwidth is less. It is wide, but the random access speed is low.

As the scratchpad expands, it will inevitably increase iterative computations and increase the overall time. In an unreliable p2p network, a large amount of computation can remain a serious vulnerability, since the node is obliged to check the proof-of-work of every new block. If a node spends a significant amount of time evaluating each hash, it is vulnerable to Ddos attacks due to fake objects full of random working data (nonce value). The upper bound of CryptoNote e-coin is MSupply = 2 ^54 −1 atomic units. These are technical limits and are not calculated in an intuitive way that “N coins are enough”. To keep the issuance process stable, the following formula is used for block rewards. BaseReward = (MSupply − A) >> 18where A stands for the amount of previously produced coins.

7-3.7) Modifiable parameters

7-3.7.1) Difficulty

Cryptonote changes the difficulty for every block. When the network hash rate rapidly grows or decreases, the response time is inevitably lowered, and it is fixed at a constant block rate. In the original Bitcoin method, the target period and the actual period between the last 2016 blocks are compared, and this is applied as a multiplier for the current difficulty. The disadvantage of this Bitcoin method is that the difficulty increases rapidly. The basic algorithm of CryptoNote is to add up all the work calculated by the node and divide it by the time they spend. The unit of work corresponds to the difficulty value of each block. However, it is difficult to determine the exact time interval between blocks due to inaccuracy and unreliability in time stamping. If a user switches the time stamp to the future, the next interval will decrease or even be negative. I think there will be very few such cases, I'll just clean up the time stamp and clean up the excess (around 20%) and the remaining values range from 80% of the time value spent for the corresponding block.

7-3.7.2) size limit

Users pay for storing the blockchain and have voting rights corresponding to their size. Every miner must choose a trade-off between a balance of revenue and cost, a balance between fees and their own “soft-limit” on creating blocks. In addition, the core rule on the maximum block size is essential to prevent forgery transactions. However, these values must be modifiable.
Assuming Mn is an intermediate value for N block sizes, then the “hard-limit” for accepting blocks is 2 MN. This prevents bloating of the blockchain and allows it to grow slowly over time. Transaction size does not need to be explicitly limited. It depends on the size of the block, and if someone wants to send a huge transaction using hundreds of inputs/outputs (or have a large abstraction in the ring signature), they can proceed with the transaction by paying a sufficient fee.

7-3.7.3) Transaction Script

CryptoNote has a very minimal script subsystem. The sender specifies a specific expression $\Phi = f(x1, x2, \ldots, xn)$, where n is the number of destination public key C:\Users\ddd\AppData\Local\Temp\Hnc\BinD . Only 5 binary operators are supported, min, max, sum, mul, cmp. When the recipients consume this expenditure, they produce a signature of $0 \leq k \leq n$ and send it to the transaction input. The verification process simply evaluates s Φ with xi = 1 to check a valid signature for the public key Pi , confirming that Xi=0. The verifier accepts proof if $\Phi > 0$.

Despite the simplicity, in this way you can cope with all possible cases.

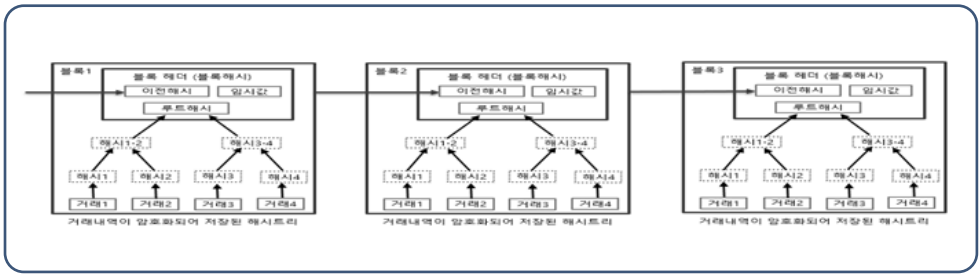
o Multi-/threshold signatures. Bitcoin-style “M ro out of N” multi signatures (receivers supply valid signatures with at least $0 \leq M \leq N$) $\Phi = x1+x2+\ldots+xN \geq M$ weighted threshold signature (some keys may be more important than others) is $\Phi = w1 \cdot x1 + w2 \cdot x2 + \ldots$ It can be expressed as + $wN \cdot xN \geq wM$. The master key corresponds to $\Phi = \max(M \cdot x, x1 + x2 + \ldots + xN) \geq M$. In this way, complex situations can be expressed simply.

o Password protection. Having a secret cipher is equivalent to having knowledge of the private key, deterministically derived from cipher k=KDF(s). So the recipient can prove that he knows the password by providing another signature under k key. The sender simply adds the corresponding public key to its output. This approach is significantly safer than the “transaction puzzle” used in Bitcoin.

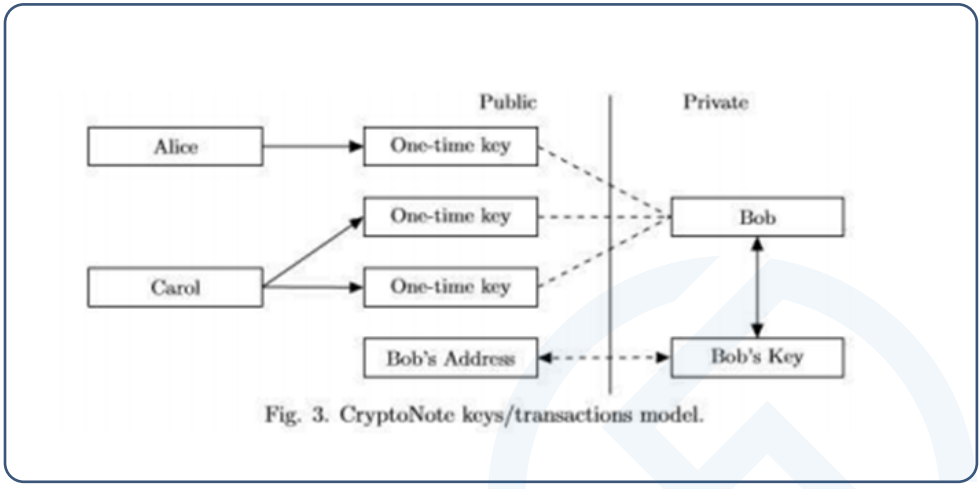
o Degenerate cases. In a situation where $\Phi = 1$, anyone can use the money. In the case of $\Phi = 0$, it indicates that the corresponding output is permanently unavailable. If the output script integrated with the public key is too large for the sender, a special output type can be used.

The receiver will send this data as his input while the sender just supplies a hash to it. This approach is similar to Bitcoin’s “pay-to-hash” approach. Instead of adding new script commands, we deal with these cases at the data structure level.

7-3.8) Core composition diagram



<Block chain process diagram>



<CryptoNote Crypto/Transaction Process Diagram>

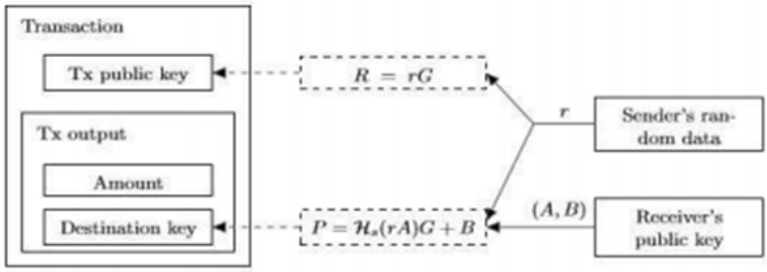


Fig. 4. Standard transaction structure.

<Standard Transaction Structure Diagram>

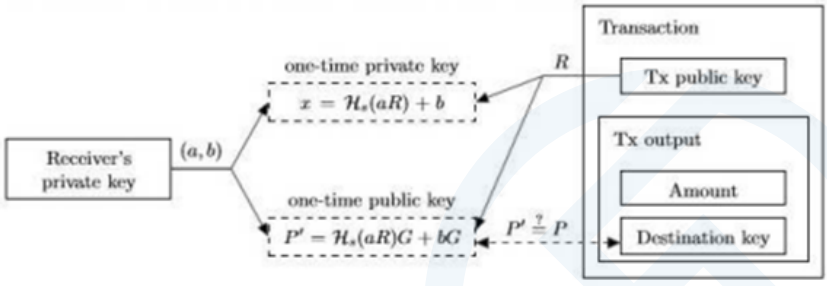


Fig. 5. Incoming transaction check.

<Transaction Confirmation Diagram>

8. Domestic User Attracting Strategy

8-1) University Campaign

We will recruit, educate, and manage students of 336 universities in Korea who will promote the 'EVENTO platform' so that it can quickly attract 2.5 million students. We will speed up the spread by providing game coupons as an option to students who introduce our platform applications to others.

8-2) Organizational and Labor Union alliances

Since the 'EVENTO platform' can attract high level of public interest and guarantee benefits for individual users, the formation of relationships such as partnerships and agreements with social groups, union groups, and consumer groups will be activated.

8-3) SNS Marketing

We plan to set the advertising cost and entrust it to a specialized marketing company until the target number of 1 million members is secured.

8-4) Introduction Marketing

During a certain promotional period, game coupons shall be provided to the introducer who introduced the application, inducing self-spreading at the same time.

8-5) Newspaper & advertising agency alliance

The dilemma for newspapers is the declining subscribers. Due to the development of the Internet and SNS, the dependence on newspapers has decreased, and therefore the advertising effect in paper newspapers has also decreased, leading to a decrease in advertising revenue. As a solution to this, the QR code game system of the 'EVENTO platform' is expected to play a certain role by inserting QR code equipped with a certain game coupon provided by the advertising company for each newspaper advertisement. When the user scan QR Code on the advertisement, the 'EVENTO Game' opens and the advertising starts. Since the game can only be played the specified number of times on a first-come, first-served basis, users might subscribe to the newspaper to obtain the game coupon in the newspaper for free. Advertisers will target their advertising exposure effects and video advertising effects, for more people will scan the QR code than the specified number of game coupons. By actively utilizing this system in the early stage, we will be able to continuously increase the number of members of our platform while satisfying all newspapers, advertisers, and readers, we expect.

9. Organization

9-1) Domestic Organization

9-1-1) Business Division

As the main body in charge of domestic business, holding the responsibility and authority for partnerships, agreements and small business recruitment and management, individual member recruiting and management, and opening and managing agencies under it's subordinates.

9-1-2) Distributor

One agency per 70,000 population (705 agencies in total) shall be designated. The agency performs its role by being delegated the responsibilities and authority of the business headquarters in the region. For agency contracts, certain conditions are set(down payment conditions, agency rights, etc.) and interests come from various fields. Taking one of the profits for an example, each time a member in the agency area plays a game, 10 won is distributed to the agency owner. (If about 1,000 people out of 70,000 play the game 200 times a month, the agency's revenue shall be 2 million won a month)

9-2) Global Organization

We will establishes an operating corporation that will act as a 'business headquarters' in each country, globally . The entity shall obtain 30% of the shares, and the rest is held by the contractors in that country, and 5 million of 'EVT Coins' shall be provided to that operating corporation.
The down payment of the operating corporations in each country shall be set based on the price of 5 million coins at the time of establishing.

10. Business Entity and Partners

10-1) Entity : Kangaroo Foundation

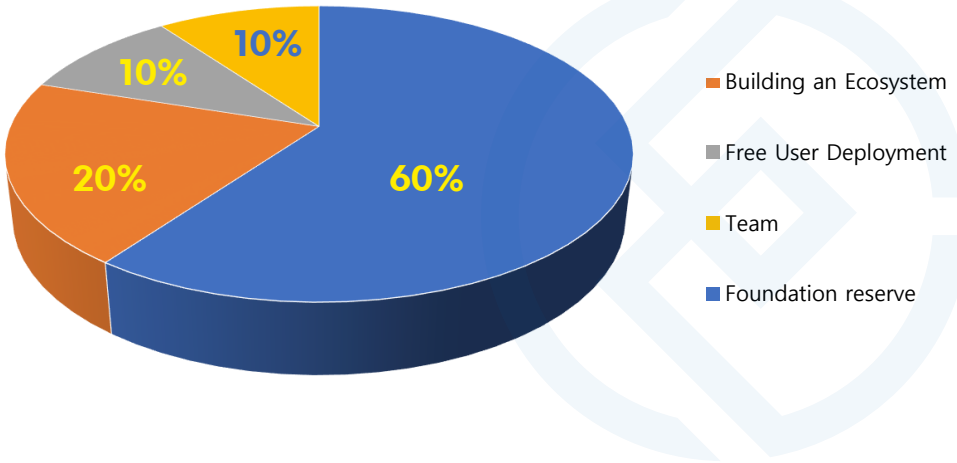
The Kangaroo Foundation was established to aim ; 1. preventing bullying from peer groups 2. promoting a solid and healthy community by providing daily life contents for childrens of families in crisis. As Kangaroo, the only animal that jumps with its cubs among animals, we are promoting the "Kangaroo Campaign : Creating a Society that Embraces Our Weak Neighbors and Jumps".
In order to realize this purpose, cooperation with the local business district is essential. Since 2009, we have been continuously seeking solidarity with local small businesses. All profits from the operation of this platform will be used for childrens in crisis around the world.

10-2) Partner: Wannabe Chainsoft Co.

As a registered venture company, Wannabe Chainsoft Co. is developing programs and blockchain systems. This company developed the 'EVENTO Platform' and donated it to the Kangaroo Foundation. By developing the world's first Block Ceiling software to build the 'IPFS node center' much more effectively than before, it has the ability to open and operate the fastest and most efficient 'IPFS node center'. Wannabe Chainsoft Co. agreed to donate 50% of the IPFS node center's profits to the Kangaroo Foundation under the deep consensus with 'Kangaroo Campaign'.

11. Token Issuance Overview

- Total issuance : 50,000,000,000
- 80% 40,000,000,000 Incineration
- 20% 10,000,000,000 Using the Ecosystem



12. Roadmap

July 2016 : Non-exclusive license agreement for patents related to EVENTO GAME
(No.10-0962275)

Feb. 2019 : Established Kangaroo Foundation (registered as a non-profit corporation)

May 2021 : Start of EVENTO platform development
-Squid 645 Game Application / Blockchain Mainnet (EVT Coin) /
Coin Exchange / Kangaroo Mall
-Development Responsibility: Wannabe Chain Platform

Nov. 2021 : Beta version of EVENTO Platform releasing

Nov. 2021 : Applying for Listing on EVT Coin Korea Exchange (Cordax) &
Multinational Exchanges (Digifinex, Cucoin)
-EVENTO platform development completed, open ceremony
: The Raum Hotel, Seoul)
-Strategic Alliance with VISA card – Issuance of EVENTO VISA card

Dec. 2021 : listing on Korean and multinational exchanges
- Simultaneous opening in 10 countries around the world
- Collaboration with Korean organizations and franchise companies
(2.5 million free game coupons)
-Secure over 50,000 members

Jan. 2022 : Preparation/Application for listing on top Multinational/Korean exchanges
-Simultaneous opening in 30 countries around the world

Q1 2022 : Be listed on top Multinational/Korean exchanges
- Simultaneous opening in 100 countries around the world
- 1 million members worldwide
- Achieved 10 million games per day

14. Vision

[Vision : Step1] Networking
Networking of small business owners, venture companies, and peoples around the world through 'EVENTO GAME' in a mobile platform
Securing active currency of EVT coin

[Vision : Step 2] Distribution
Securing competitiveness by discount and game coupons distribution : Increasing Sales volume and expecting dramatic increase in online currency of 'EVT Coin'.

[Vision : Step 3] Welfare
Expanding social contribution by gradual releasing of the locked 'EVT Coin' (70%) at the time of increasing platform membership and spreading the usability of EVT coin – Building a gradual image as a donation coin to the people of around the world
Securing status as a donation coin at near future.

[Vision : Step 4] Multi-platform
Building a multi-platform in all areas of life (delivery, entertainment, metaverse, carbon neutrality, welfare, ecosystem…), building a beautiful and happy global environment by collaborating with venture companies that have systematically sponsored and nurtured by this platform.

Helping the endangered peoples of our time and enduring sacrifices for them is a noble life that everyone, regardless of race, country, or religion, must pursue. And it's also the way to make people feel the most happiest moments. We look forward to and hope that the 'EVENTO Platform' shall create a global community without borders. 'EVENTO Platform' is just the beginning of forming a global community, and we will continue to develop and apply new platforms and technologies that allow peoples continually and incessantly enjoy the various benefits of this platform while connected through the 'EVENTO Platform'.

15. LEGAL CONSIDERATIONS AND DISCLAIMER

1) This white paper was made for the purpose of providing specific information on the direction and eco-system of 'EVNETO Platform' to corporations, institutions, groups and individuals with which the 'EVNETO Platform' Team or Kangaroo Foundation has formed or is going to form a partnership.

2) The statements, information, and contents contained in this white paper contain the current EVT

platform's progress and future prediction information and contents based on the current trend at the time of writing. Since such forward-looking information and contents do not include related laws, regulations, policies, unknown risks, and various other variables, it should be recognized that the contents and results expressed in this white paper may appear materially different from reality.

3) This white paper has no legal effect to bind 'EVENTO Platform' partners, participants and users, and the contents of the white paper are part of the 'EVENTO Platform' at any time without being bound by anyone or for any reason. Contents may be changed, modified, added, or deleted, and there is no obligation to notify the contents of changes, modifications, additions, and deletions.

4) This white paper is absolutely not an advice on investment, law, regulation, accounting, tax, finance, etc., and none of the contents of this white paper solicit or suggest a transaction or investment contract. In addition, the contents of this white paper are not securities, stocks, equity debts, rentals, or similar related to the 'EVENTO Platform', nor are they intended to induce sales or purchases of the 'EVENTO Platform'. Therefore, the 'EVENTO Platform Team', 'Kangaroo Foundation', and Project-linked corporations are not responsible for any matters to everyone who reads this white paper.

5) When participating in, using, or purchasing a project as an institution, group, or individual that has or plans to form a partnership, 'EVENTO Coin' means a blockchain-type token and is for the issuance of a blockchain-type token, and no voting rights are granted. must be recognized.

6) Even if any form of legal damage, such as loss, damage, debt, or other financial damage, occurs as an institution, group, or individual that has formed or plans to form a partnership, makes a decision, or uses this white paper after reading this white paper, 'EVNETO Platform Team', 'Kangaroo Foundation', and Project-linked corporations shall not bear any responsibility for compensation, or any other kind of reponsibilities. In addition, in relation to the issuance and operation of 'EVT Coin', since the business risk borne by the 'EVT Platform Team', 'Kangaroo Foundation', and the project-linked corporation also does not belong to the 'EVT Coin' holder, so 'EVT Coin' holders also cannot enjoy economic benefits linked to the business performance or pay in return of 'EVT Coin'.

7) 'EVT Coin' may transfer the issuance and operating entity of 'EVT Coin' to overseas without the consent of the 'EVT Coin' holders due to changes of the business purpose, and the transferred overseas entity may be exclusively responsible for the issuance and operation of 'EVT Coin'.

8) 'EVT Coin' shall not be provided, distributed, resold, or transferred to citizens, natural persons, or corporations (hereinafter referred to as "prohibited persons") in those areas where cryptocurrency

trading is prohibited or restricted by laws, policies, etc.

9) If a corporation, institution, organization, or natural person who intends to purchase 'EVT Coin' is presumed to be prohibited from participating, or if the information provided to the 'EVENTO Platform Team', 'Kangaroo Foundation', and Project-linked corporation were insufficient, inaccurate or misleading, it would be denied or canceled at any time. In addition, please be aware that transactions may be restricted and may be canceled or invalidated at any time in cases of a prohibited person purchasing 'EVT Coin', and a participant's purchasing through illegal or unauthorized channel.

10) A legal entity, institution, organization, or natural person wishing to purchase 'EVT Coin' must check whether 'EVT Coin' can be legally purchased in their area and resell 'EVT Coin' to other purchasers in a specific area all by themselves, and this white paper does not provide any kind of basis for judgment on such matters. In addition, it is to be noted that all liability arising from the intervention of the prohibited person rests with the prohibited person and the legal person, institution, organization or natural person who provides, distributes, resells, or transfers to the prohibited person.

11) In the future, according to the natural expansion of 'EVT Coin', when listing or not is to be decided, the 'EVT Coin' holder does not have the right to specify or request the time, method, result, etc., only the 'EVT Platform Team', 'Kangaroo Foundation', and Project-linked corporations shall be in full authority and responsibility of decision making about listing or not.

12) In the future, even if the new EVT platform is implemented for the purpose of creating an ecosystem according to the direction of 'EVT Coin' and the realization of better values, all related matters belong to the responsibility and authority of the 'EVT Platform Team', 'Kangaroo Foundation', and Project-linked corporations.

13) In the future, if there is a matter to determine whether, when and how 'EVT Coin' will be airdropped, as well as the subject and quantity of airdrop, all related matters will be decided by the 'EVT Platform Team', 'Kangaroo Foundation', and Project-linked corporations. 'EVT Coin' holders do not have the right to designate or demand the time, method, subject and quantity, etc. of the airdrop even when the airdrop is performed.

14) Based on the direction and philosophical value of 'EVT Coin', the 'EVT Platform Team', 'Kangaroo Foundation', and Project-linked corporations do their best to contribute to the spread of the blockchain ecosystem in the donation area through games, and to make our society reborn as a more bright and healthy society.