REVV COIN

Independent transaction method and various mining methods / New multi-concept currency platform

2017. 06.

Contents

1. REVV Coin Integrated Platform

2. Technical Approach of REVV Coin

3. Other Issues

4. Additional Data

5. Reference

1. REVV Coin Integrated Platform

Background for Introduction and Proposal

In the present world, many coins are being created and being disappeared.

Conventional coins have many problems, but the biggest problem is the fact that the limitations are beginning to appear, which all began due to simple development, undifferentiated mining method, and the policy-less distribution method.

In addition, it does not implement the original purpose and function of virtual money properly, and the choices of users are also narrow.

The initial purpose of designing and developing the virtual currency stemmed from the idea of making the ideal currency by eliminating the problems of the existing fiat money. Therefore, everyone knows that virtual money should be replaced with real money. However, the coin's history is so short that it has not been able to materialize this method yet, or many coins seem don't know how to.

In view of the infinite possibilities of coin development, it is not possible to solve the realistic problems, due to similar features, undifferentiated interface, users' demands for new coin platform are increasing. Many people would have thought about the ideal virtual currency platform, how it would be and what features would it will have.

Coins can be easily created by anyone, but spreading, promoting, acknowledging, circulating, and retaining is a difficult area for anyone to do.
Existing coins try to apply the developed coin system to the real world. However, **REVV coin is designed in a reverse structure that allows the realistic area to be naturally applied to the coin area.**
In order for coin to be applied to real life, reputation of coin, promotion and realization factor, necessity and many users need to be secured accordingly. On the contrary, **the reverse structure method is a method in which the user's actual life pattern and system of reality are naturally incorporated into the aspects (recognition, mining, use, substitution) of the coin.**

We define the virtual coin like this. The process of making a coin is similar. Marketing and strategy are the key. "How to mined, how to use it, where to use it, who to trade, what is the most important realization?"

The REVV coin is the best realistic virtual currency that has begun with the intention of solving many of these problems and trying to get closer to reality.
In addition, REVV coin is a mining machine that purchases and operates a mining machine at a high cost and pursues reasonable mining with low cost and effort, .

Anyone can easily use the application if the coin system is built into the behavior pattern, I will be able to position myself as a coin with the highest recognition.

REVV Coin is a realistic virtual currency designed with an offline platform that can use and use various coins in various places, and a circulation structure in which the platform is replicated and spread.

1. REVV Coin Integrated Platform

What is REVV Coin?

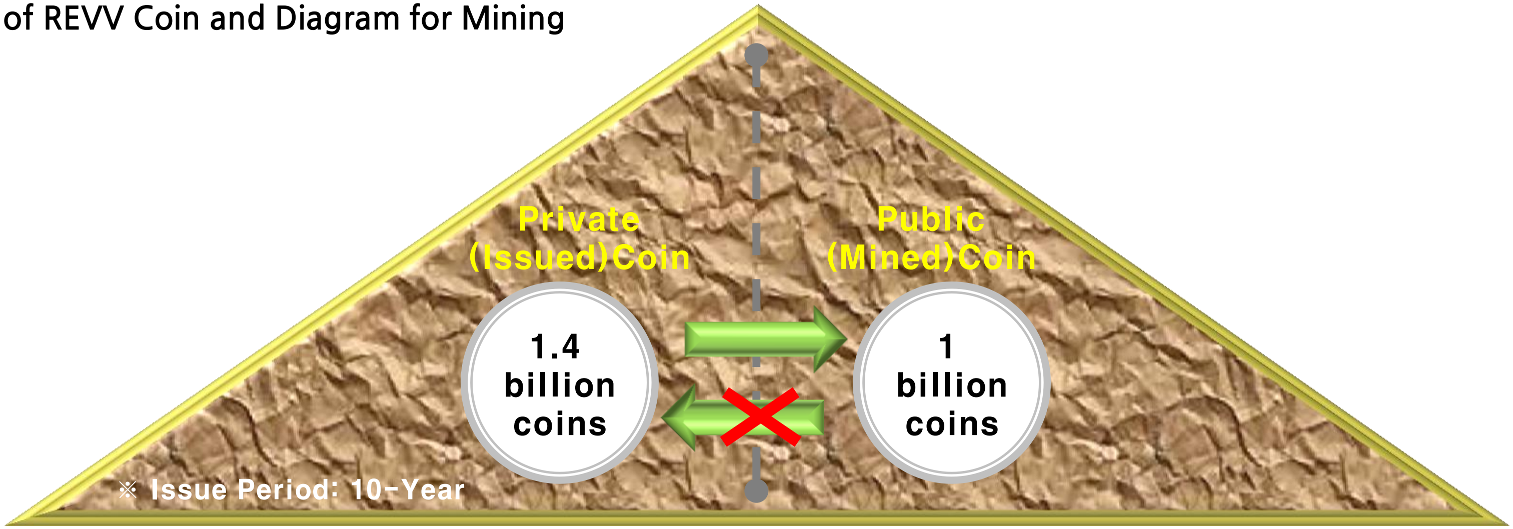
REVV Coin is MULTI PAY COIN. Coin unit is REC. It is a multi-purpose, versatile, multi-function, various types of coins that has mining and payment system.

There are different uses and purposes of each coin, and various mining system including mining method is introduced. Users can maintain the coins in REVV coin E-wallet, and can use the coins everywhere in diverse fields.

The REVV coin has a total reserve of 2.4 billion units. It is a coin developed on the basis of block chain, but the coin buried for public mining is 1 billion, and the remaining 1.4 billion will be used as a (private) issuing coin.

The difficulty of mining (Private) issued coin and public mining coin will be in one direction. The difficulty of public mining coin is affected the number of (non-public) coins issued, but the (non-public) issuing coin is not influenced by the difficulty according to the mining amount of the open mining coin or the amount of remaining reserves. However, the (non-public) issuing coin is issued independently and is influenced by its own difficulty level. Here, the difficulty of the (non-public) issuing coin is calculated and issued according to the price of the coin, the remaining amount, and the period, and the basic formula is applied, but the variable is followed. For example, the amount of coins issued per lot of lottery sales changes, then the remaining coins may be prolonged according to the 10 years of issuance rate. They are linked to each other according to the volume issued by other types of mining.

■ Issuance of REVV Coin and Diagram for Mining

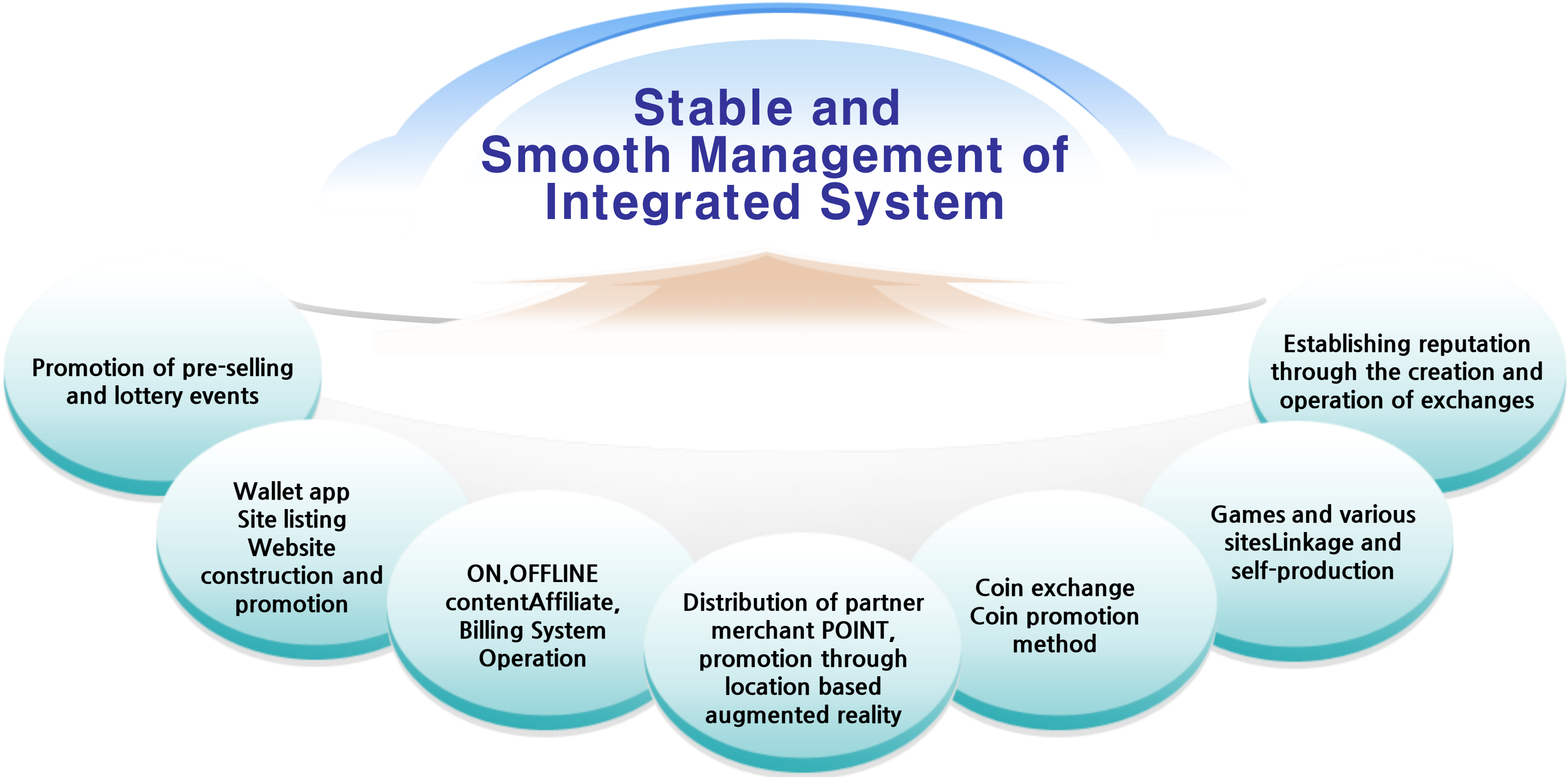


1. REVV Coin Integrated Platform

What is REVV Coin?

(Private) Some or all of the sales proceeds generated by the issuing coin are used for the construction and expansion of various payment systems of the coin. The profits we earned will be used as re-investment to create virtuous cycle.

■ REVV Coin Promotion and Management Strategy



Stable and Smooth Management of Integrated System

Promotion of pre-selling and lottery events

Wallet app Site listing Website construction and promotion

ON.OFFLINE contentAffiliate, Billing System Operation

Distribution of partner merchant POINT, promotion through location based augmented reality

Coin exchange Coin promotion method

Games and various sitesLinkage and self-production

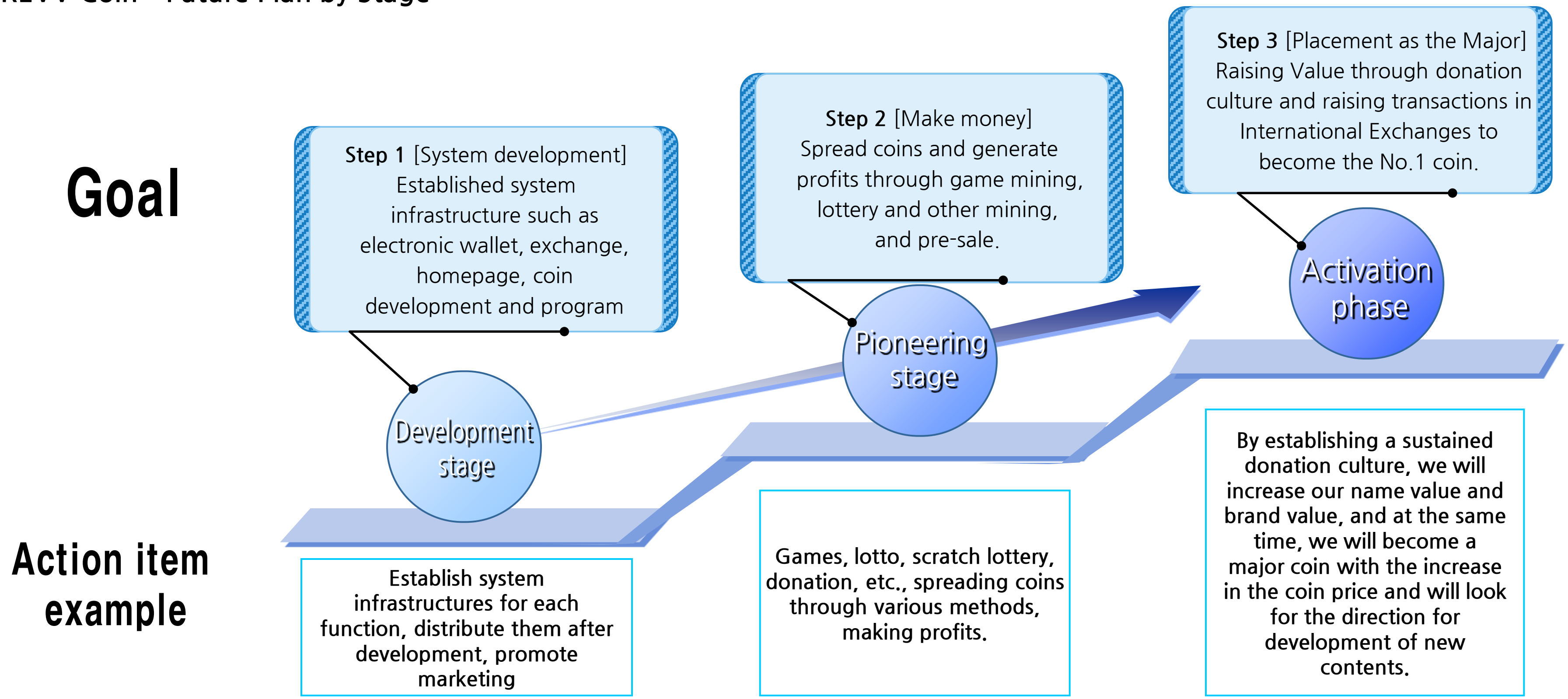
Establishing reputation through the creation and operation of exchanges

1. REVV Coin Integrated Platform

What is REVV Coin?

The REVV coin, which is differentiated and specialized, introduces a reinvestment system for securing lots of users and raising reputation, applying the real life based patterns to the coin mining format. REVV Coin will become excellently settled and expanded.

- REVV Coin - Future Plan by Stage



Goal

Step 1 [System development] Established system infrastructure such as electronic wallet, exchange, homepage, coin development and program

Step 2 [Make money] Spread coins and generate profits through game mining, lottery and other mining, and pre-sale.

Step 3 [Placement as the Major] Raising Value through donation culture and raising transactions in International Exchanges to become the No.1 coin.

Action item example

Establish system infrastructures for each function, distribute them after development, promote marketing

Games, lotto, scratch lottery, donation, etc., spreading coins through various methods, making profits.

By establishing a sustained donation culture, we will increase our name value and brand value, and at the same time, we will become a major coin with the increase in the coin price and will look for the direction for development of new contents.

1. REVV Coin Integrated Platform

REVV Coin E-Wallet

The coin's electronic purse is run with a wallet created on the exchanges and public mining. However, the REVV coin can create one additional electronic wallet.
The REVV Coin's electronic wallet is an electronic wallet, but it is an integrated platform of a new concept coin that is multi-functional and can be mined through independent transaction methods that perform various functions.
The REVV coin purse is created and operated in a block chain fashion rather than a simple on / off line application.
It is usually downloaded from a market where general applications can be downloaded (eg, Google, Huawei, etc.), and is operated after installation.
It is operated by P2P-based distributed database at runtime and operates on the basis of public key cryptography. You can also scan and download the QR code in the purse holder's wallet.
The downloaded file can be downloaded from the REVV coin purse platform, and a small-sized application with the function to be mounted on the platform is downloaded into the platform. The small function application is socketed so that it can be attached and detached at any time. Further, it is also possible to use the portable storage device (REVV USB) after the user removes the storage device (REVV USB) for users who have difficulty in executing the application because the memory capacity of the mobile phone is small.
In case of REVV USB, it has its own security key and thanks to the dual memory backup system, it can prevent leakage of personal information and other security problems. REVV USB is designed to enable you to connect and run small, functional applications.

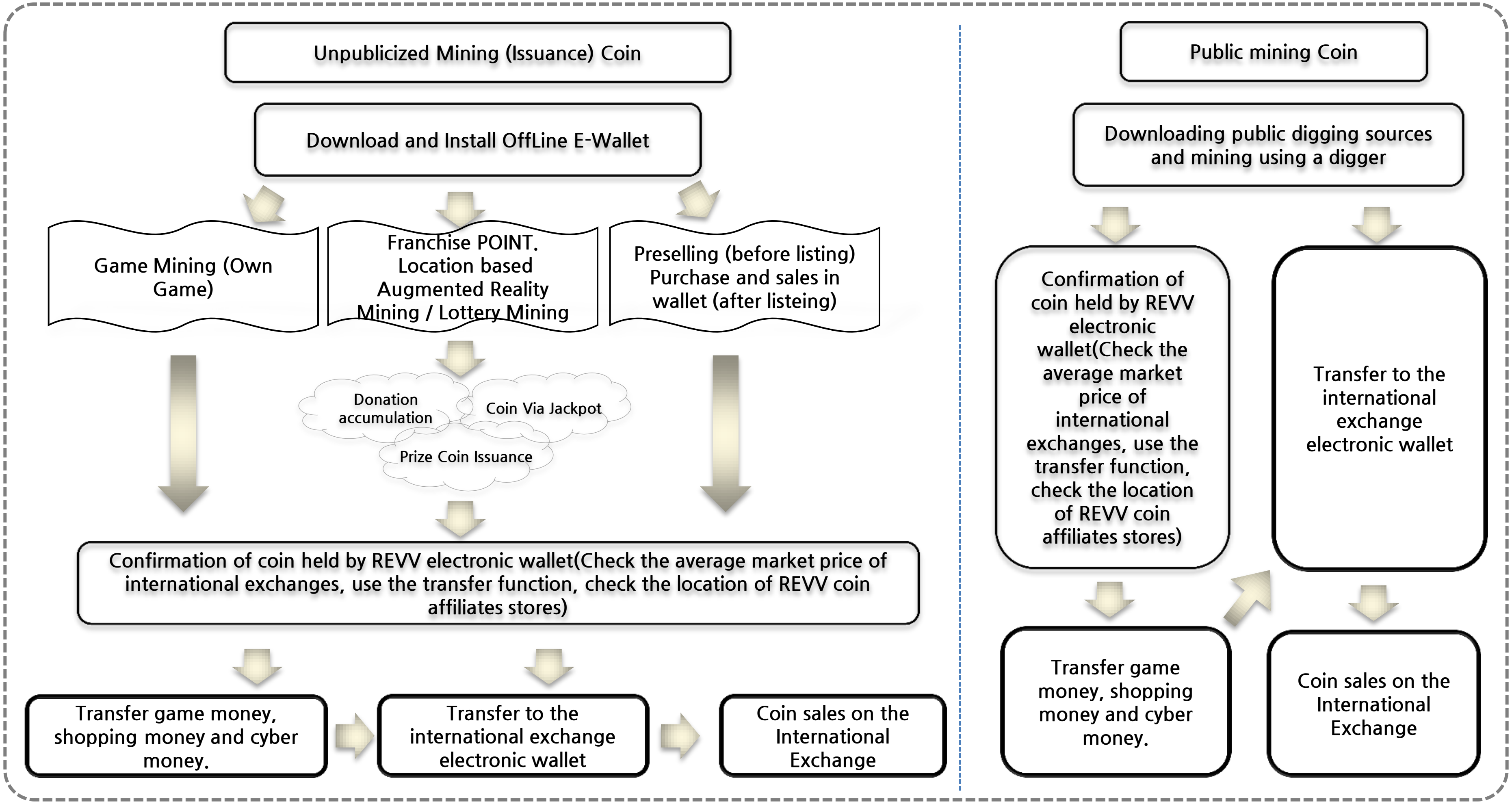
REVV Coin is the function of the electronic wallet and the functional application of the small unit are as follows:

1) Coin transfer and transaction between users, exchange wallet
2) Affiliate contents - game mining, lottery mining, event mining, jackpot mining, location linked mining, affiliate POINT mining, coin exchange mining
3) COIN OFFLINE payment system - direct store, affiliate store (including POINT mining shop)
4) Donation contents
5) Affiliate ON-LINE contents payment system - Game, shopping mall, image contents, etc.

1. REVV Coin Integrated Platform

REVV Coin E-Wallet

Flow Diagram of Coin Mining



Unpublicized Mining (Issuance) Coin

Download and Install OffLine E-Wallet

Game Mining (Own Game)

Franchise POINT. Location based Augmented Reality Mining / Lottery Mining

Preselling (before listing) Purchase and sales in wallet (after listeing)

Donation accumulation

Coin Via Jackpot

Prize Coin Issuance

Confirmation of coin held by REVV electronic wallet(Check the average market price of international exchanges, use the transfer function, check the location of REVV coin affiliates stores)

Transfer game money, shopping money and cyber money.

Transfer to the international exchange electronic wallet

Coin sales on the International Exchange

Public mining Coin

Downloading public digging sources and mining using a digger

Confirmation of coin held by REVV electronic wallet(Check the average market price of international exchanges, use the transfer function, check the location of REVV coin affiliates stores)

Transfer to the international exchange electronic wallet

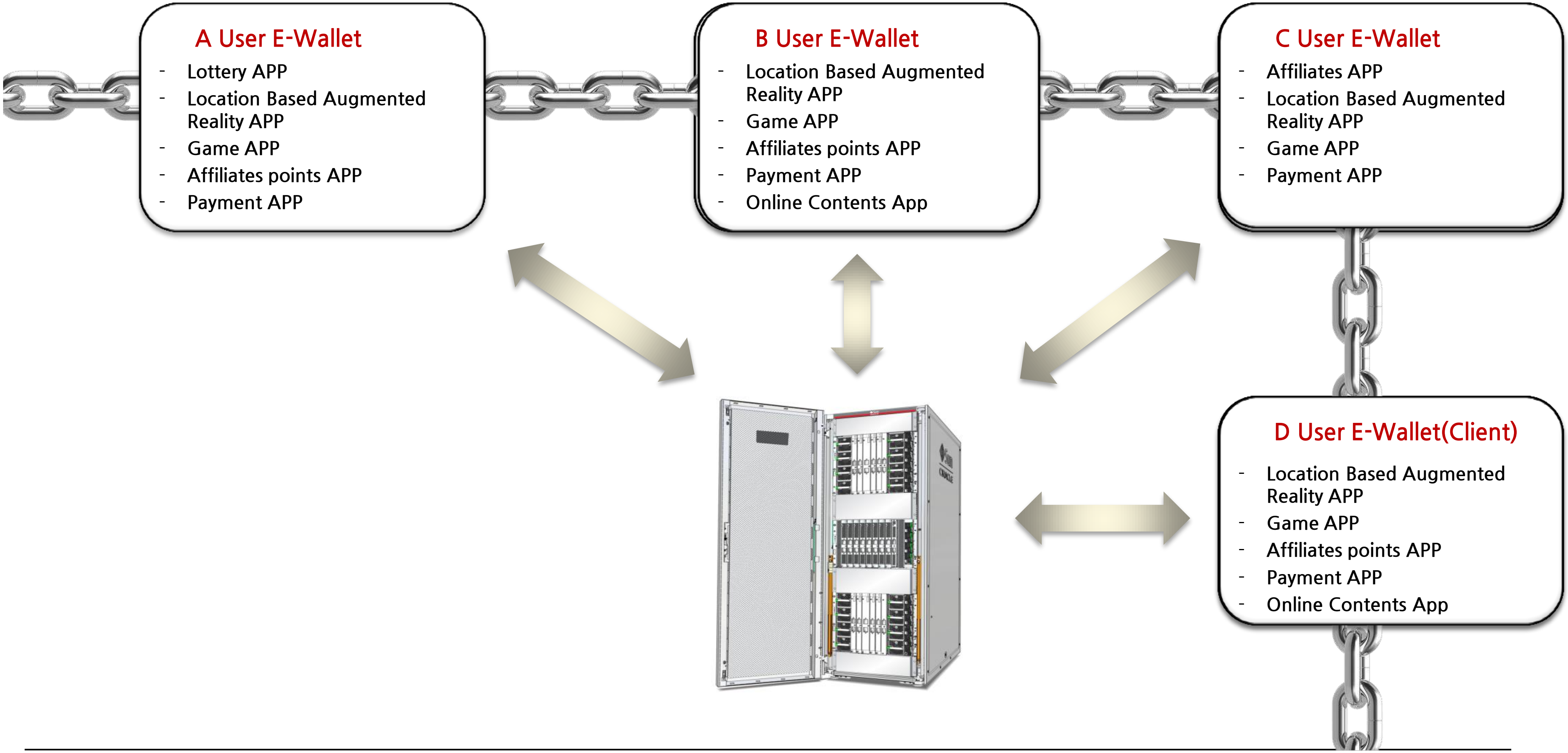
Transfer game money, shopping money and cyber money.

Coin sales on the International Exchange

1. REVV Coin Integrated Platform

REVV Coin E-Wallet

■ E-Wallet Interconnect Diagram



A User E-Wallet

- Lottery APP
- Location Based Augmented Reality APP
- Game APP
- Affiliates points APP
- Payment APP

B User E-Wallet

- Location Based Augmented Reality APP
- Game APP
- Affiliates points APP
- Payment APP
- Online Contents App

C User E-Wallet

- Affiliates APP
- Location Based Augmented Reality APP
- Game APP
- Payment APP

D User E-Wallet(Client)

- Location Based Augmented Reality APP
- Game APP
- Affiliates points APP
- Payment APP
- Online Contents App

1. REVV Coin Integrated Platform

Transfer & Transactions

It is possible to make transactions between users who own electronic wallet, and the listing quotation of the exchange in the relevant country is applied. Although it is a small private exchange, the REVV coin relay cash and coin to prevent bad transactions. There is a small commission charged for each transaction.

The transfer can be transferred to the REVV coin purse between individual users and to the electronic purse of the International Exchange. Transactions can be traded between electronic wallets.

It is possible to transfer and remit the coins to the users of REVV COIN if the users apply payment transfer application on small unit applications. Transmission time is reflected in real time, and errors and transactions by attacker are not reflected and automatically recovered.

1. REVV Coin Integrated Platform

Smaller Unit Applications and Contents

◎ Game Mining Application

The user installs a game mining application in a small unit function application in the REVV coin wallet and proceeds the game developed in the REVV coin to perform mining. If you play the game, you will have to pay an additional fee (rental fee) and you can play the game in a certain period. However, there is no time restriction of game mining within the period, and the coins mined through the game are stored in the user's REVV coin purse.

The difficulty level of the game mining does not depend on the number of coins issued, but the ratio of conversion to the coin can be adjusted. This adjustment is applied according to the price of the coin and the quantities of the mined coins.

There are 1 - 4 types of mining games, and it is done by developing additional coin-linked game by securing the affiliates via reinvesting the profits. When winning the game, the game point increases and a certain amount of game points can be switched to REVV coin. However, the conversion fee is 1%.

The maximum number of coins for game mining is fixed.

◎ Lottery Mining Application

The user installs the lottery mining application among the small unit function applications in the REVV coin wallet and receives the lottery ticket provided by the REVV coin. If the player wins, he receives the coin for prize.
The lottery type is Lotto type and scratch type. If you win the lottery, part of the coin that is paid will be donated to the welfare organization affiliated with REVV coin, or the donation organization designated by the user.
Lottery tickets are sold for a period of 10 years. Lotteries that have not been sold for a period of 10 years will be sold through extension and some will be used for jackpots and events.
Some of the sales proceeds will be used to establish direct OFFLINE stores for REVV coins, and sales generated from the stores will be reinvested for the establishment of new stores. Thus, this amount of money is used as the substitute money for those who do not own the coins. In addition, due to the expansion of the coin usage, the transaction becomes active, which serves as a factor to differentiate REVV coin and increase the price of the coin. Finally, it will grow as the leader in the coin industry.

Coins issued as lottery have some influence on the difficulty of coins buried in public mining, but they do not play a major role.

1. REVV Coin Integrated Platform

Smaller Unit Applications and Contents

◎ Event Mining Application

The user can use the Event Mining Application among small unit function applications in the REVV E-wallet.

Event mining is similar to pre-sale coin sales, rather than actual mining by event-driven mining method. This is mining provided to the users of the lottery mining.

Event mining will be announced in the REVV electronic wallet if there are global issues and events. Due to the nature of the event, it will be conducted twice a month or once a month.

◎ Jackpot Mining Application

The user can apply the jackpot only by installing the jackpot mining application among the small function application in the REVV e-wallet.

Jackpot mining is proceeded with the remaining amount of coins generated due to the lottery issuance. This is similar to pre-sale coin sales, rather than actual mining by event-driven mining method. Jackpot mining is held once every month.

The recipient of Jackpot is classified into three stages. The number of recipients in each stage share the total number of remaining coins in the stage.

Part of the winning lottery mining, event mining, and jackpot mining REVV coins will be deducted to use as donation coin, which will be sent to the organization designated by the miner.

◎ Location-Based Augmented Reality Mining Application

The user can use the location-based AR mining by installing the location-based augmented reality mining application among the small unit functional applications in the REVV coin e-Wallet.

Based on the location-based augmented reality system, the coin for location-based augmented reality is issued in a fixed quantity and distributed periodically to the streets, sightseeing spots and densely populated areas of affiliated stores. It installs and executes the corresponding APP of the coin purse of REVV, notifies the user when the coin is found at the user's location, and operates the application and mined within 10 seconds.

Smaller Unit Applications and Contents

◎ Affiliates POINT Mining Application

The user can use the affiliates' POINT mining application among small unit function applications in REVV E-Wallet.

It is equipped with the POINT mining application of the affiliates to raise reputation and promotion for those countries that do not use REVV coin.

Affiliates POINT mining is installed on the REVV coin purse on the cell phone of the owner or manager of the affiliated store. This means that the merchant pays the goods, services, and services to the merchant and pays the coins in the same way as the POINT where the merchandise is accumulated. In this case, the REVV coin purse of the merchant is the coin address of the customer's electronic purse or QR Code, and barcode, and the authenticated data is executed in an automatic manner, which is confirmed and paid by the electronic wallet of the REVV coin. The restriction on the number of applications per day of visiting customers and the limitation of the merchant business owners will be added to prevent illegal and illegal coin issuance. If you do not have an REVV coin purse, you can download it from the QR code attached to the merchant or from the web or app that you can download.

The franchisee, after a certain period of time, will become a franchisee with a differentiated strategy from other competing franchise. As a result, the affiliated franchisee stores the coins through mining and purchasing. Eventually, it will increase the reputation and value of REVV coin, and market price will become a chance for the affiliates to change into the franchise that receive REVV coin for payment and settlement.

The quantity of REVV coins is automatically applied to the REVV electronic wallet. The quantity of REVV coins issued varies with difficulty depending on the price and the number of remaining coins.

◎ Coin Exchange Mining Application

The user can use the coin exchange mining application among the small unit function applications in REVV E-wallet.

Coin exchange mining can be done by putting the coin in the coin collector placed at a certain place (specific place) or location. Then, if you enter the cell phone number, the address where you can download the REVV coin purse to the mobile phone will be returned. After connecting the returned information value and downloading the coin exchange mining application and installing it, you will receive the REVV coin after you go through the personal authentication procedure. Currently, many countries in the world are not producing coins, and coins are disappearing. However, the coins kept by each individual are not used yet, and coins are always left even after you exchange coins to paper money. You can access the REVV coin homepage to check the information about REVV coin promotional materials, REVV coin electronic wallet, donation, and various uses. This is strategy to spread the usage of the coin.

Affiliate ON.OFFLINE Contents Payment System

◎ Affiliate OFFLINE Contents Payment System

As part of the revenues (sales) generated by the lottery mining, we will establish stores (affiliates) in each country, and the store is constructed as a coin store which can be paid with COIN. This becomes the place where REVV coins are used and has a great influence on the expansion of coins. REVV coins are recognized as a real virtual currency by many users recognizing, holding, and trading, and the securing of coins. The proceeds from the store will be reused in the establishment of additional stores, except for the operating expenses, and will try to expand the awareness of the coin. Also, introduction of the coin settlement system of the affiliated merchant described above will play an important role.

◎ Affiliate ONLINE Contents Payment System

Affiliate ONLINE content payment system plays the same role as OFFLINE payment system, but there are some differences. Among the applications of the REVV electronic wallet, the payment application is divided into the billing system of the affiliated game, the shopping mall payment system and the video billing system. In the case of the affiliated game payment system, the REVV coin contained in the REVV e-wallet can be directly paid. This allows automatic linkage and calculation of quotes and quantity, etc., and the game is divided into a game developed in-house and an affiliate game in REVV coin.

The shopping mall billing system enables verification and purchasing in connection with affiliated shopping mall, REVV coin electronic wallet, REVV coin homepage, and each shopping mall homepage, and enables settlement (transfer) in REVV coin electronic wallet to be linked at the time of payment. The price applies equally to the game payment system.

In the case of a video billing system, for example, a system in which an REVV coin is replaced with an item that replaces a role such as "online balloon" is applied. This also plays an important role in ensuring the use of the REVV coin and expanding the base.

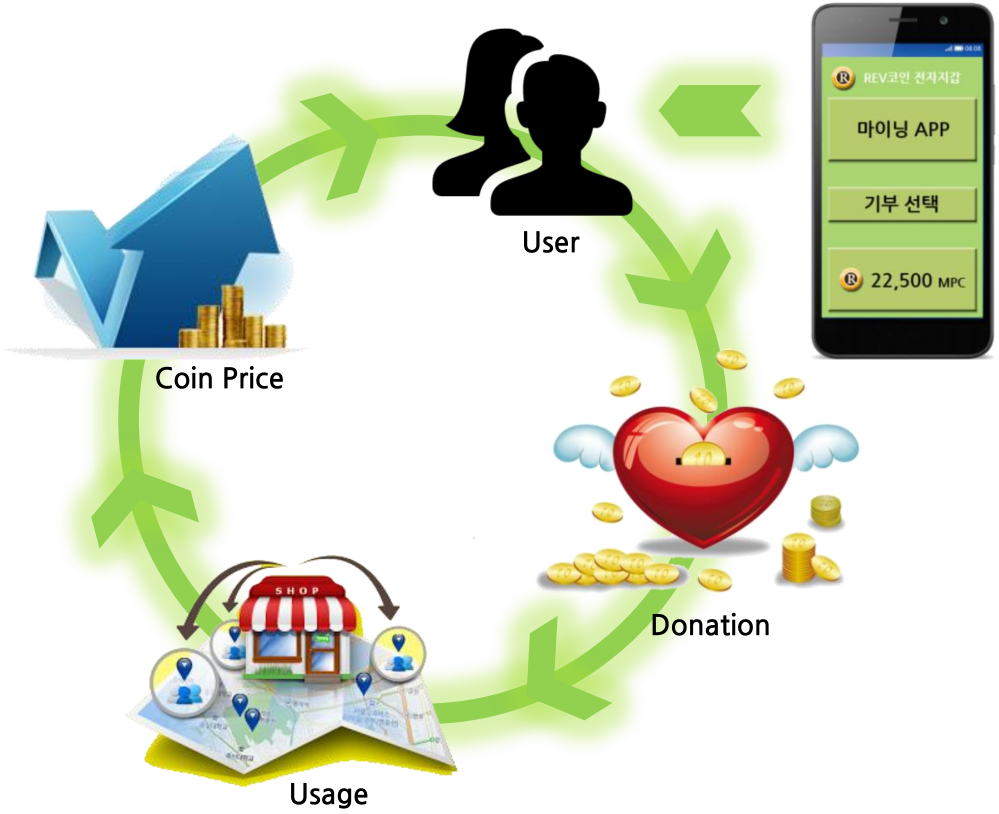
1. REVV Coin Integrated Platform

Donation

Coin is money. It is also a currency with the purpose of speculation and investment.
The spirit of the REVV coin has the spirit of giving. Before functioning as a currency, it functions as a link between people and people.
Then, as a coin that everyone knows and uses, we believe that it should function as a link between different people, giving and caring.
At the heart of this is the donation spirit and role of the REVV coin.
REVV coin applied donation culture.
Donations to the society of "sharing" and "together" lead each other.
This is the ideal reality that REVV coins wants to shape.

Donations are made through sponsorship contracts with donation organizations and welfare organizations in each country.
This group is registered on the REVV homepage, and the user selects and donates to the organization.
Donations will be donated as REVV coins.
After downloading and installing, you will run donations related applications and receive donations.
Affiliated donors and welfare organizations listed on the REVV coin homepage are users. REVV coin can be donated in the E-Wallet.

Donations will be made to the REVV coin at the user's discretion, but part of the revenues from the lottery sale, jackpot, and event of the REVV coin will be paid in cash.
If you are a donated group or individual, you can transfer money from the wallet of the REVV coin to the wallet of the International Exchange, or you can cash it through the transaction between the REVV coin purse. In addition, you can purchase necessary products in the ON and OFF LINE stores. The donation group and individual contributes to the spread of awareness of the REVV coin and plays an important role in promoting the image of the REVV coin.



1. REVV Coin Integrated Platform

Conclusion and Vision

REVV Coin is a currency applied to real life by securing various uses and mining methods. - MULTI PAY COIN

- In this coin platform, some coins are acquired through lottery mining, jackpot mining, and event mining. Some of them are donated, where people will share and grow together with it. The REVV Coin Foundation will gather the profits related to mining and expand the usages of REVV coin in every corner of the world (in-store), and will expand and spread the full amount of the processes through reinvestment. This platform is made in the REVV E-wallet and communicates with reality due to the linkage of small functional applications.
- Among small applications, game applications are used for early mining but later will become independent game applications.
  This will be the coin usage of the existing REVV coin holders, and will play a role as an original hidden card for REVV coins in conjunction with other games.
- The merchant point application is an early stage for securing the common usage outside the use area established by the REVV coin foundation and plays a role of promoting the natural promotion and awareness of the REVV coin to both the merchant owner and the customer.
- Location-based augmented reality applications play an important role in the user's fun and spread of awareness of coins, and serve as applications to replace lottery mining in countries where lottery mining is not allowed.
- The Coin Exchange mining application replaces the function of the disappearing coin with the REVV coin, which makes it easier for anyone to access the REVV coin and also increases the awareness of the REVV coin one step further.
- ON · OFF LINE Alliance contents serve as a substitute for existing currency, points, tokens, coupons, vouchers, and other auxiliary goods.

The REVV coin is a differentiated coin even from the planning process.
The key role of coin is awareness, and mining, trading, and retention of many people are necessary, and it is essential to make them used as real money in various fields.
As stated above, if we provide various and interesting mining, securing the user with the profit, securing the more usages, then numerous transactions will be made via REVV coins. The value of the REVV coin It will be an automatic rise, voluntary not by manipulation. This will get more users and this will also form a loop of good circulation will be.
Coin's vision is not technology based on the development of coin, but rather the plan of marketing and expandability that is applied to coin so that reality spreads and settles as real coin.
The REVV coin is a coin with all of this and will be a coin that plays a pivotal role in opening the future of coin.

2. Technical Approach of REVV Coins

REVV Coin Account

The purpose of the REVV coin is to create an alternative protocol for creating distributed applications. It focuses especially on situations where it is important to provide other types of production techniques that might be useful for large-scale distributed applications, fast development times, security for small and rare applications, and efficient interaction with other applications. The REVV coin aims to achieve this goal by providing an essential and fundamental basis for building a block chain with Turing's complete language. Anyone can use this language to create smart contracts and distributed applications to create arbitrary rules for ownership, transaction formats, state transition functions, and so on. The basic form of a name coin can be written in two lines of code, and the protocol for a call or reputation system can be made up to about twenty lines of code. A smart contract, a kind of cipher box that allows you to store a value and get it only when certain conditions are met, can also be built on top of this platform. This is possible because Turing-completeness, value-awareness, block chain-awareness, and so on can be made possible because much more powerful functions are provided than those provided by bitcoin scripting.

REVV account

In the REVV coin, the state is made up of objects called accounts. Each account has a 20-byte address and a state transition between the account and the value directly. The REVV account has four fields:

* Nonce: a kind of counter that allows each transaction to be processed only once
* Current balance of the account balance
* The contract code of the account (if any)
* The storage space of the account (empty by default)

The balance is the default internal crypto-fuel of the REVV coin and is used to pay transaction fees. There are usually two types of accounts: external

There are Externally Owned Accounts and Contract Accounts controlled by Contract Code. An externally-owned account has no code.

To send a message from this account, you must create a new transaction and sign it. Each time a contract account receives a message, it activates its code, reading the message or writing it to internal storage, sending other messages, or creating contracts in turn.

In a REVV coin, a contract is not something that needs to be performed or compiled, but rather an autonomous agent alive in the execution environment of the REVV coin. When a message or transaction arrives, it always executes certain code, It directly controls its own key/value store to track persistent variables.

2. Technical Approach of REVV Coins

Message and Transaction

The term transaction, as used in the REVV coin, is a signed data package that contains messages. These messages are sent to the external owning account. This transaction includes:

* Message destination
* Signature to identify the sender
* The amount of balance the sender sends to the destination
* Optional data fields
* The value of STARTGAS, the maximum number of calculation steps allowed for the execution of the transaction
* GASPRICE value, commission paid by originator at each stage of calculation

The first three items are almost always used as standard in cryptography. The data field does not have a function set to its initial value, but the virtual machine has an opcode to use when the contract accesses this data. For example, if there is a contract functioning as a domain registration service on a block chain, the data sent to this contract can be interpreted as having two fields. The first field is the domain to be registered, and the second field is the IP address. The contract reads these values from the message data and stores them in the appropriate location in the repository.

The STARTGAS and GASPRICE fields play a very important role in the anti-denial of service model of the REVV coin.
Each transaction must be set to limit the number of calculation steps in the code execution that can be used to prevent accidental or malicious infinite loops in the code, or waste of computation. The basic unit of calculation is gas, and usually the calculation step costs 1 gas, but some calculations require more expensive calculation costs, or a larger amount of data to be stored as part of the state, . In addition, every byte in the transaction data charges a fee of 5 gas per byte. The intent of these commission systems is to force some attackers to pay a commission in proportion to all the resources they consume, including computation, bandwidth, and storage. Therefore, the transactions associated with a network that consumes a significant amount of any of these resources should have a roughly proportional gas fee.

2. Technical Approach of REVV Coins

Message

A contract can deliver a "message" to another contract. A message, which does not have to be stored physically, is a virtual object that exists only in the execution environment of an REVV coin.

The message includes the following.

* (Implicitly) the message originator
* Message destination
* Balance delivered with message
* Optional data fields
* STARTGAS value

Essentially, a message is similar to a transaction, except that it is generated by a contract, not by an external executor. A message is generated when a contract that is currently executing a code encounters a CALL opcode to generate and execute a message.
Like a transaction, a message arrives at the recipient account that executes the code. Thus, a contract can relate to another contract in exactly the same way that an external executor does.

The gas allowance assigned by a transaction or contract applies to the total gas consumed by that transaction and all sub-executions. For example, if an external executor A sends a transaction to B with 1000gas, B consumes 600 gas, then sends a message to C, then C will consumes 300 gas for internal execution, then B can use the remaining 100 gas before its exhaustion.

2. Technical Approach of REVV Coins

REVV Coin State Transformation Function

REVV Coin state transition function APPLY (S, TX) -> S 'can be defined as follows.

1. Check that the transaction is appropriate to the format (that is, has the correct number of values), and checks that the signature is valid, if the nonce matches the nonce of the originating account/ Otherwise, it returns the error.

2. Calculate the transaction fee with STARTGAS * GASPRICE, and determine the source address from the signature. It subtracts this fee from the source account balance and increases the sender nonce. Returns an error if there is not enough source balance.

3. After initializing with GAS = STARTGAS, subtract a specific amount of gas per byte to pay for the bytes used in the transaction.

4. Send the transaction value from the source account to the destination account. If the destination account does not exist, create it. If the destination account is a contract, code the contract to the end or until the gas is exhausted.

5. If the sender fails to send enough value because it does not have enough money, or when the code runs out of gas, return all state changes to their original state. However, commission payments are excluded and this fee will be added to the mining account.

6. Otherwise, return the fee for all remaining gas to the originator and send the fee paid to the consumed gas to the miner.

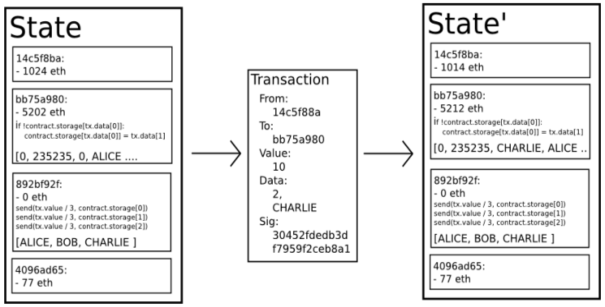
For example, consider the following contract code:

```
If !self.storage [calldataload (0)]:
    self.storage [calldataload (0)] = calldataload (32)
```

In practice, the contract code is written in low-level EVM code, but for simplicity, this example is written in Serpent , one of the high-level languages of REVV coin . This code can be compiled with EVM code.

Assuming the storage of the contract is empty, the transaction has 10 balances, 2000 gas, 0.001REVVC gas price. Let's assume that we send 64 bytes of data (the number 2 represent up to 0-31 bytes and the string CHARLIE represent up to 32-63 bytes)

In this case, the process of the state transformation function is as follows.



```
if !contract.storage[tx.data[0]]:
   contract.storage[tx.data[0]] = tx.data[1]
```

```
send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])
```

```
if !contract.storage[tx.data[0]]:
   contract.storage[tx.data[0]] = tx.data[1]
```

```
send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])
```

REVV Coin State Transformation Function

1. Ensure that the transaction is valid and properly formatted.

2. Verify that the transaction destination has a minimum balance of 2000 * 0.001 = 2, and subtract 2 balances from the shipping account.

3. After initializing to gas = 2000, assuming that the transaction has a length of 170 bytes and the commission per byte is 5, you must subtract 850. Eventually, the remaining will be 1150 gas.

4. Subtract additional 10 balances from the sender account and add this to the contract account.

5. Run the code. In this case, it is simple: make sure that the storage corresponding to the index 2 of the contract is used (in this case, not used) and set the storage value corresponding to index 2 to 'CHARLIE'. Assuming 187 gas is consumed in this operation, the amount of gas remaining is 1150 - 187 = 963.

6. Return 963 * 0.001 = 0.963 balance to the account of the sender and return the result status.

If there is no contract at the destination of the transaction, the total transaction fee will be equal to the GASPRICE supplied multiplied by the number of bytes in the transaction, and the data sent with the transaction will be irrelevant.

Note that a message returns its state to its original state in the same manner as a transaction. When a message runs out of gas, all other executions triggered by the message execution and its execution are returned to their original state, but their parent executions do not need to be returned. This means that it is safe for a contract to call another contract. When A invokes B with G gas, execution of A is guaranteed to lose only G gas. When you look at the opcode called CREATE, which creates a contract, the execution method is similar to CALL, but the execution result determines the code of the newly created contract.

Execution of the Code

The code that makes up the REVV coin contract is written in a low-level, stack-based bytecode language called "REVV virtual machine code" or "RVM code". The code consists of consecutive bytes, each byte representing an operation. Normally, code execution is an infinite loop that is designed to iterate repeatedly, incrementing the current program counter by zero, starting at zero, and stop execution when it reaches the end of the code or encounters an error, STOP, or RETURN command. To perform an operation, you must be able to access three types of space for storing data.

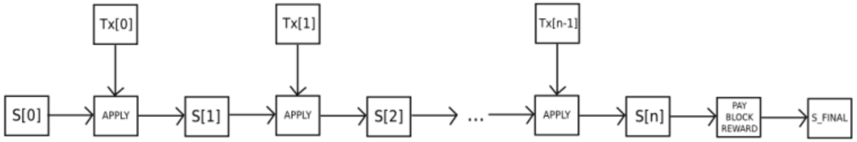
Stack: A last-in-first-out container allows you to push or pop values here.
* Memory: a byte array that can be extended infinitely
* Long-term storage of a contract: key / value store. At the end of the computation, the store is persistent, unlike the stack or memory being reset.

The code may also access block header data, as well as specific values, data in the sender and the received message, and may return a byte array of data as the result.

The official execution model of the EVM code is surprisingly simple. While the REVV virtual machine is running, all calculation states (block-state, transaction, message, code, memory, stack, pc, gas) can be defined as a tuple. The block-state is a global state that includes all accounts, including balances and storage. At the beginning of each iteration of the code, the current instruction of the pc (program counter) the byte of the code is executed, and if pc is greater than the length of the code (pc> = len The command knows its own definition of how to change the tuple. For example, ADD pops two items out of the stack, finds the sum, pushes it back into the stack, decrements gas by one, and increments pc by one. SSTORE retrieves two items from the stack and places the second item in the contract repository index pointed to by the first value of this item. There are many ways to optimize the REVV virtual machine environment through JIT compilation, but the basic REVV coin can be implemented with hundreds of lines of code.

Block Chain and Mining

REVV coin block chains are similar in many respects to bit coin block chains, but with some differences. The main difference between the REVV coin and each block chain structure in the bit coin is that the REVV coin block, unlike the bit coin, has the transaction list and the most recent state copy. In addition to that, two different value-block numbers and difficulty-are also stored within the block. The basic REVV coin block verification algorithm is as follows.



1. Make sure that the referenced previous block exists and is valid.
2. The timestamp of the current block is greater than that of the previous block referenced, At the same time, it is confirmed whether the value is smaller than 15 minutes after the present time.
3. Block number, difficulty, transaction root, uncle root, gas limit, etc. (Other various REVV coin low level concepts) are valid.
4. Verify that the proof of work contained in the block is valid.
5. Let S [0] be the last state of the previous block.
6. Let TX be the n transaction list of the current block. Set S [i + 1] = APPLY (S [i], TX [i]) for 0 to n-1. If the application returns an error or the total gas consumed in the block up to this point exceeds GASLIMIT, an error is returned.
7. Add the compensation block paid to the digger S [n] and call it S_FINAL.
8. Verify that the merge tree root of state S_FINAL is equal to the final state root of the block header. If these values are the same, the block is a valid block, otherwise it is judged to be invalid.

The approach may seem highly inefficient at first glance, because it needs to store the entire state with each block, but in reality efficiency should be comparable to that of Bitcoin. The reason is that the state is stored in the tree structure, and after every block only a small part of the tree needs to be changed. Thus, in general, between two adjacent blocks the vast majority of the tree should be the same, and therefore the data can be stored once and referenced twice using pointers (ie. hashes of subtrees). A special kind of tree known as a "Patricia tree" is used to accomplish this, including a modification to the Merkle tree concept that allows for nodes to be inserted and deleted, and not just changed, efficiently. Additionally, because all of the state information is part of the last block, there is no need to store the entire blockchain history - a strategy which, if it could be applied to Bitcoin, can be calculated to provide 5-20x savings in space.

From a physical hardware standpoint, it is easy to doubt whether the contract code is "where" it is executed. A simple solution is: The process of executing the contract code is part of the state transition function definition, Thus, if a transaction is included in block B, the execution of the code to be triggered by that transaction will be executed by all nodes currently downloading and verifying block B, either now or in the future.

3. Other Issues

Introduction of Modified GHOST

The Greedy Heaviest Observed Subtree (GHOST) protocol was first introduced in December 2013 by Yonatan Sompolinsky and Aviv Zohar. The problem raised by GHOST was that the block chains with the current fast confirmation times are experiencing poor security due to high stale ratios. This is because they take some time to propagate through the network. If the miner A mined one block and the miner B digs another block before it reaches the miner B, the coins that miner B mined will eventually be wasted.

Furthermore, there is a centralization issue: if miner A is a mining pool with 30% hashpower and B has 10% hashpower, A will have a risk of producing a stale block 70% of the time (since the other 30% of the time A produced the last block and so will get mining data immediately) whereas B will have a risk of producing a stale block 90% of the time. Thus, if the block interval is short enough for the stale rate to be high, A will be substantially more efficient simply by virtue of its size. With these two effects combined, blockchains which produce blocks quickly are very likely to lead to one mining pool having a large enough percentage of the network hashpower to have de facto control over the mining process.

As Sompolinsky and Zohar explained, GHOST solves the first issue raised above, namely network security loss, by including stale blocks when calculating which chain is "longest". In other words, in calculating which block has the greatest total work proof, not only the parent of the block and its ancestors, but also the stale descendants of that block (the term of the REVV coin is " Uncle "). To solve the second problem of centralization, we provide block compensation for stale blocks, beyond the protocols described by Sompolinsky and Zohar. The stale block receives 87.5% of the basic compensation, and the cousin that includes the stale block receives the remaining 12.5%. But fees are not given to uncles.

The REVV coin implements a simplified version of GHOST that includes only seven levels. It is specifically defined as follows.

* One block must specify one parent block and zero or more uncles must be specified.
* Uncle in Block B must have the following attributes:
  - It must be a direct descendant of the kth ancestor of B. Where 2 <= k <= 7 '.
  - It should not be the ancestor of B.
  - It must be a valid block header, but it MUST NOT be previously known or even a valid block.
  - Must be different from all uncles in previous blocks, and all other uncles in the same block (avoid duplication)
* For each Uncle U in Block B, B's digger receives an additional 3.125% plus coin-based compensation, while U's miners receive 93.75% of the base coin-based compensation.

There are two reasons for using the limited GHOST version, which can only include up to 7 generations of uncles.
First, unrestricted GHOST makes the computation of what uncle is valid for one block very complicated.
Second, if you apply the same unrestricted GHOST as the REVV coin, you will lose the motivation to dig in the "main-chain" rather than the chain of attackers.

3. Other Issues

Commission

Because each transaction put on the block chain imposes a cost on the network to download and verify it, any regulatory mechanism to prevent abuse, typically a transaction fee, is required. The default approach, used in Bitcoin, is to have purely voluntary fees, relying on miners to act as the gatekeepers and set dynamic minimums. This approach has been received very favorably in the Bitcoin community particularly because it is "market-based", allowing supply and demand between miners and transaction senders determine the price. The problem with this line of reasoning is, however, that transaction processing is not a market; although it is intuitively attractive to construe transaction processing as a service that the miner is offering to the sender, in reality every transaction that a miner includes will need to be processed by every node in the network, so the vast majority of the cost of transaction processing is borne by third parties and not the miner that is making the decision of whether or not to include it. Hence, tragedy-of-the-commons problems are very likely to occur.

However, the flaws in these market-based mechanisms offset the flaws themselves, such as magic, when certain inaccurate simplification premises are picked up. The argument is as follows.

Let's assume the following.

1. A transaction results in k operations, giving the miner who contains the transaction kR of compensation. Where R is set by the sender, k and R are (Roughly) pre-exposed to the miners.
2. A task has a processing cost of C for any node (ie, all nodes have the same efficiency).
3. There are N mining nodes, each with exactly the same processing power (ie 1 / N of the total).
4. There are no full nodes that are not mined.

The miner will try to deal with any transaction if its expected rewards are greater than its cost. Thus, the expected compensation is kR/N, because the miner has a 1 / N probability to process the next block, and the processing cost to this miner is simply kC. Therefore, miners will want to include transactions when kR/N> kC or when R> NC. Note that R is the per-operation fee provided by the sender, and is thus a lower bound on the benefit that the sender derives from the transaction, and NC is the cost to the entire network together of processing an operation. Hence, miners have the incentive to include only those transactions for which the total utilitarian benefit exceeds the cost.

3. Other Issues

Commission

However, there are several important differences when used in the reality:

1) The miner does pay a higher cost to process the transaction than the other verifying nodes, since the extra verification time delays block propagation and thus increases the chance the block will become a stale.
2) There do exist non-mining full nodes.
3) The mining power distribution may end up radically unequal in practice.
4) Speculators, political enemies and crazies whose utility function includes causing harm to the network do exist, and they can cleverly set up contracts where their cost is much lower than the cost paid by other verifying nodes.

(1) provides a tendency for the miner to contain fewer transactions, (2) increases NC, and therefore both of these effects partially offset each other. (3) and (4) are the main problems. In order to solve these problems, a floating cap is introduced. Any block can not have more operations than the BLK_LIMIT_FACTOR times the long-term exponential moving average. Specifically:
blk.oplimit = floor((blk.parent.oplimit * (EMAFACTOR - 1) + floor(parent.opcount * BLK_LIMIT_FACTOR)) / EMA_FACTOR)

BLK_LIMIT_FACTOR and EMA_FACTOR are constants and will be fixed to 65536 and 1.5, respectively, but are likely to change after further analysis.

There are also other factors that block large block sizes in bit coin. It is likely to be stale because it takes longer for large blocks to propagate. In Ethereum, highly gas-consuming blocks can also take longer to propagate both because they are physically larger and because they take longer to process the transaction state transitions to validate. This delay disincentive is a significant consideration in Bitcoin, but less so in Ethereum because of the GHOST protocol; hence, relying on regulated block limits provides a more stable baseline.

Computation and Turing Completeness

It is important to note that the virtual machine of REVV is Turing-complete. That is, RVM can encode any computation that can be conceivably carried out, including infinite loops. RVM codes can be conducted in two ways.
The first is to use the JUMP command to go back to the previous location of the code, in the code, and a JUMPI instruction to do conditional jumping, allowing for statements like while x < 27: x = x * 2. Second, contracts can call other contracts, potentially allowing for looping through recursion. This naturally causes some problems. Could a malicious user paralyze a miner and a pool node by causing the calculation to endlessly circulate? The famous problem known as the halting problem in computer science is similar here. In general, there is no way to determine in advance whether a given problem will ultimately stop. As described in the state transition section, our solution works by requiring a transaction to set a maximum number of computational steps that it is allowed to take, and if execution takes longer computation is reverted but fees are still paid. Messages work in the same way. To show the motivation behind our solution, consider the following examples:

An attacker creates a contract which runs an infinite loop, and then sends a transaction activating that loop to the miner. The miner will process the transaction, running the infinite loop, and wait for it to run out of gas. Even though the execution runs out of gas and stops halfway through, the transaction is still valid and the miner still claims the fee from the attacker for each computational step.

* Let 's say that a malicious attacker has created a very long infinite loop program with the purpose of letting the digger continue his calculations for a long time. At the end of the calculation, only a small number of blocks are created, making it impossible for the miner to include the transaction in order to claim a commission. However, the attacker must submit a value for the STARTGAS command that specifies the upper limit of the actual running step, so the digger will know in advance that the calculation requires an excessive number of steps.
* An attacker sees a contract with code of some form like send(A,contract.storage[A]); contract.storage[A] = 0, and sends a transaction with just enough gas to run the first step but not the second (ie. making a withdrawal but not letting the balance go down). Contract writers do not have to worry about defending against these attacks. This is because, if the calculation execution stops in the middle, the corresponding change is restored to the original state.

* Assume that a financial contract is operating to minimize risk by taking an average of nine financial instrument data values. Assume that a malicious attacker takes a single data value that is designed to be modified through a variable address request mechanism, as described in the DAOs section. By doing so, every attempt to find a fund from this financial contract will result in exhaustion of gas.
However, financial contracts can defend against attack by setting a gas limit on the message.

Computation and Turing Completeness

The alternative to Turing-completeness is Turing-incompleteness, where the commands for JUREVV and JUREVV1 do not exist and only one copy of each contract is allowed to exist in the call stack at any given time.

With this system, the fee system described and the uncertainties around the effectiveness of our solution might not be necessary. This is because the cost of executing a contract would be bounded above by its size.
Furthermore, Turing-incompleteness is not a big limitation either. Of the contracts that we have envisaged to date, there was only one that needed a circular order. On top of that, even the cycle command could be eliminated by repeating a sentence 26 times in program coding.
Given Turing - completeness implications and their limited advantages, why not use Turing - incomplete languages?
In reality, however, Turing-incompleteness is far from a neat solution to the problem. To see why, consider the following contracts:

```
C0: call(C1); call(C1);
C1: call(C2); call(C2);
C2: call(C3); call(C3);
...
C49: call(C50); call(C50);
C50: (run one step of a program and record the change in storage.)
```

Now let's send a deal to A. In 51 deals we send a contract to continue the calculation phase of 2 to 50 wins. The miners may be able to try to detect these logic bombs in advance by securing both the maximum number of calculation steps for each contract and the number of calculation steps for the contract recursively calling the other contract. This attempt, however, makes it impossible for the miners to deal with contracts that call other contracts. (Because the creation and execution of all 26 contracts above can easily be combined into a single contract).

Another problematic point is that the address field of a message is a variable, so in general it may not even be possible to tell which other contracts a given contract will call ahead of time.

Hence, we have a surprising conclusion: Turing-completeness is surprisingly easy to manage, and the lack of Turing-completeness is equally surprisingly difficult to manage unless the exact same controls are in place - but in that case why not just let the protocol be Turing-complete?

3. Other Issues

Currency and Issuance

The REVV coin network has its own built-in currency, 'REC' in it, which serves the purpose of efficient exchange between different virtual assets and providing mechanism for paying transaction fees. In order to prevent user discomfort and future disputes, the name of each unit of balance is predefined as follows. (See the controversy surrounding the bit coin name) *

* 1 : RES
* 10^{12} : REI
* 10^{15} : REF
* 10^{18} : REC

The basic unit of the REVV coin is REC, and when it expands to the decimal point, D -> E -> F ... .-> S, and if it is expanded beyond the decimal point, B -> A -> 1-> 2 ... Unit is formed.

This should be taken as an expanded version of the concept of "dollars" and "cents" or "BTC" and "satoshi". In the near future, "REC" is expected to be used for general transactions, "REF" for micropayments, and "REI" and "RES" for technical discussions involving commissions or protocol adoption. The remaining names are not included in the client right now.

The issuance model will be as follows:

* REC will be released in a currency sale at the price of 1000-2000 each BTC, a mechanism intended to fund REVV organization and pay for development that has been used with success by other platforms such as Mastercoin and NXT. At this time, buyers who purchase RECs earn inexpensive RECs with significant discounts.
* The BTC received from the sale will be used entirely to pay salaries and bounties to developers and invested into various for-profit and non-profit projects of REVV.

* As much as 0.142857 times (200,000,000) of the total RECs sold (1.4 billion RECs) of the REVV coin will be newly issued, and the initial contributors before the REVV coin launch will be distributed.
* From the time of mining to the end of the year, 5% of the remaining amount will be issued to the miners.

Classification		Notes
Amount of Public Mining	1 billion REC	Partial application of difficulty in private coin
For Presale	4 hundred million REC	Application of Price
For Lottery Sale	3 hundred sixty million REC	Application of Difficulty
For Affiliates' Points	1 hundred 20 million REC	Application of Difficulty
For Location Based AR	1 hundred 20 million REC	Application of Difficulty
For Game	2 hundred million REC	Application of Difficulty

3. Other Issues

Currency and Issuance

- Lottery Issuance Coin: It is formed with KRW 360 million REC, of which LOTTO worth KRW 180 million, and scratch worth KRW 180 million.
- The amount of the coin issued and the quota are applied to the month or the issuance period to determine the scale of the sales price and this does not exceed the specified sales amount.
- The price of a coin to be paid as lottery ticket is set at an initial price of 100 won. When a price exceeding 100 won occurs, it shall be calculated by applying the price.
- In the case of a lottery, 50% of the total sales amount will be issued by the amount of the coin to be paid in the calculation of the coin. If the winner does not appear, the amount will be accumulated in the winning coin for one month (4 weeks).
- If the remaining coins are less than the coins issued, 20% of the remaining coins will be used for the jackpot and 20% for the event. The remaining 60% is used for extended periods after the period.
- In the case of lotto, the number of coins to be issued will decrease when the market price is raised.
- The lottery winner applies the total sales amount to the coin price. The first place winner will get 23%, second place 4%, third place 4%, fourth place 7%, fifth place 12%, and the amount of prize will be distributed accordingly
- In the case of scratch, the market price is issued without prior notice. The number of lotteries to be issued is 10,000 per day, and the number of coins is reduced by the number of issuances per year.
- The amount of prize in case of scratch is 20% of the total issuance, the first prize winner will be five people, 20 people are distributed to 2nd prize, 49 people are distributed to 3rd prize, 493 people are distributed to 4th prize, and 2465 people will be distributed to 5th prize.
- 20% of the remaining coins will be used for the purpose of the event, among which 20% will be used for the event, 20% used as jackpot, and the remaining 60% will be used as lottery coins, used in places with prolonged period. However, it is applied only to the next month, and the remaining coins will be used for instruction and affiliates.
- The coin for the affiliates' POINT is attached to the affiliates' QR code so that the customer can easily installed and recognized by the user.
- The coin for the affiliates' POINT is formed with a total of 120 million RECs, and the coin applied at once is 0.1 REC (1RED). However, the quantity changes according to the coin's real-time price.
- Per consumer can only do it 2 times per day, and the franchisee's intentional and incomplete acts shall be terminated and withdrawn from the franchisees.

3. Other Issues

Currency and Issuance

- In the future, if the KRW 120 millions of REC is exhausted, the franchisees must pay for the purchase separately and there is no obligation. However, due to competition in the market, the effect on customers due to suspension is greatly affected. This makes it possible for a merchant to become a separate user and become a REC payment merchant.
- The coin for location-based AR is formed with a total of KRW 120 million, and it is distributed periodically to the franchisees, landmark areas, and tourist attractions.
- The mining time of is about 10 seconds and 0.01REC (REE) is mined. The quantity to be mined is reduced according to the real time quotes and the number of remaining coins.
- The game mining coin is 200 million REC.
- The cost of using one month of mining equipment is 30,000 won (Korean Won). There is no time limit.
- You will receive 1 point or more of points per victory of the game. You do not get if you lose.
- 100POINT can be switched to 1REC (exchange). However, a 1% fee applies when switching.
- If the coin's real-time price rises, the quantity of RECs converted per 100 points decreases.

3. Other Issues

Mining Centralization

The bit coin mining method is to repeat the 'SHA256 hashing' operation for a block header indefinitely until a value is lower than the target value, until eventually one node comes up with a version whose hash is less than the target (currently around 2^{192}). However, this mining algorithm is vulnerable to two forms of centralization.

The first is that the barriers to participation are now very high. Currently, the mining ecosystem has been completely eroded by ASICs (semiconductors designed specifically for special purposes, with better performance than general purpose semiconductors). These ASIC diggers have more than several thousand times more efficiency than general GPU diggers. This means that Bitcoin mining is no longer a highly decentralized and egalitarian pursuit, and the investment of billions of won would have to be transformed into a 'business' for the participating capitalists.

Second, most Bitcoin miners do not actually perform block validation locally; instead, they rely on a centralized mining pool to provide the block headers. As in the previous example, several participants participate in mining depending on the block header provided by the centralized mining pool rather than participating in the block creation. As a result, the three mining pools indirectly control about 50% of the hash, taking over the computing power of individuals. Of course, because individuals can move to other small pools before the pool's share exceeds 50%, pools will not be able to abuse resources at will, but this is still a big problem.

The mining method of the REVV coin is slightly different. Each explorer takes random data from the state, hashes the last few randomly selected blocks, and outputs the results. This has two advantages.

The first is that REVV coin contracts can cover all sorts of computer calculations. So, naturally, ASICs should be designed to fit all the calculation methods, and eventually it becomes a kind of high performance CPU rather than ASIC. In reality, ASICs (in-demand semiconductor) themselves become obsolete.

Secondly, miners must download the whole block chain at work and verify all transfers. This eliminates the need for a centralized large pool. Although the large pool itself has the effect of distributing the new block generation compensation evenly to the participants, the effect can be sufficiently realized through the pool of P2P format. There is no need to use a centralized pool approach.
Of course, the above mining model is not yet verified. There is also a doubt as to whether the work of increasing the resistance to ASIC equipment can be applied in reality as in theory. One thing is certain, however, that when a number of different contracts are applied, it is difficult to make ASICs that encompass all of these features stated above. Also, if there is an ASIC that is specific to any kind of work, anyone can introduce a large number of contracts into the block-chain specifically designed to stymie certain ASICs. In other words, miners who own ASICs specific to each part will attack each other by creating contracts that cause them to work against one another. This approach, of course, is more of an approach based on 'economic human behavior' rather than 'technological' approach.

3. Other Issues

Extendibility

One common question about REVV coins is about its extendibility. Like Bitcoin, REVV coin also has a weak point that all transfer operations must be verified and processed by all the nodes in the network. In the case of Bitcoin, the size of the whole block chain is about 15GB, and its size is steadily increasing by 1MB every hour. VISA handles more than 2,000 transfers per second, which translates to an increase of 1MB per 3 seconds (1GB per hour, 8TB per year).

REVV coins will suffer similar problems, and REVV coins covering all sorts of decentralized applications (Dapps), compared to Bitcoins that merely serve as currency, have much more problems in this area. It may be possible to suffer. However, the strength of REVV coin is that it uses full nodes to store just the state instead of the entire block-chain.

If all the individual nodes have to keep the whole block chain, the following problems can occur. Let's imagine that the size of the block chain is getting bigger and closer to 100TB. If the size of the block chain that needs to be kept at this level is large, only a small number of business or corporate type participants can afford it. Many end users will only use the "Lite SPV (SiREVVle Payment Verification)" node. In this case, there arises the potential concern that the full nodes could band together and all agree to cheat in some profitable fashion. Manipulation actions such as switching the block compensation amount may occur. Simple 'light node' will have no way to detect this operation. Of course, there may be a good participant among the 'full node' that owns the entire block chain. However, if a large number of 'full nodes' try to manipulate the block chain, it should be seen that it will be already late at the time of discovery. In fact, Bitcoin has been warned that there is a risk of similar problems at this time, and how to mitigate the problem has been discussed by Peter Todd.

In order to solve the above problem, we will introduce two additional strategies in the near future. First, because REVV coins are basically using a mining algorithm based on block-chain technology, at least every miner will be forced to be a full node, creating a lower bound on the number of full nodes. Second, it introduces an 'intermediate state tree root' into the block chain after the transfer history verification operation. In this way, even if the block creation task is concentrated on a small number of nodes, this problem can be solved through a verification protocol if there is at least one 'honest node'.

If a block propagated by a mining node is invalidated, the 'format' of the corresponding block is not correct or the 'state description S [n]' is incorrect. Since 'S [0]' is considered to be correct, if 'S [i-1]' is correct, there is an error in 'S [i]'. The verifying node would provide the index i, along with a "proof of invalidity" consisting of the subset of Patricia tree nodes needing to process APPLY(S[i-1],TX[i]) -> S[i]. The nodes perform their work using the above nodes and find that the generated 'S [i]' does not match the provided 'S [i]'.

A more sophisticated attack involving malicious mining nodes to propagate the incoREVVlete block can also be achieved. The information needed to verify the block may not be fully present. In this case, a 'challenge-response protocol' technique may be used. The verification node generates a 'challenge' with the 'target transaction indices', and the light node receiving the node treats the corresponding challenge as a verification error block. Upon receiving a node a light node treats the block as untrusted until another node, whether the miner or another verifier, provides a subset of Patricia nodes as a proof of validity.

Introduction and History of Bitcoin and Concepts

The concept of decentralized digital currencies and alternative applications such as property registration has been around us for decades.

In the 1980s and '90s, the anonymous e-cash protocol was based on' cryptographic primitive', commonly known as Chaumian Blinding. Chaumian Blinding provided new currencies that strongly protected personal information, but because it relied on a centralized intermediary, it failed.

In 1998, Wei Dai's [b-money] (http://www.weidai.com/bmoney.txt) originally proposed the idea of issuing money through a method of solving a distributed settlement and a calculation puzzle. However, it lacked the detailed instructions on how to implement the agreement in practice. In 2005, Hal Finney introduced the concept of "reusable proofs of work (http://www.finney.org/~hal/rpow/)".

The system combines b-money's idea with Adam Back's computationally difficult Hashcash puzzles. However, by putting trustworthy computing on the basis of external trust, it has again failed to implement the ideal. The deconcentrated currency, which was first implemented by Satoshi Nakamoto in 2009, combined the existing algorithms used for ownership management through public key cryptography with a consensus algorithm known as "proof of work" .

The mechanism behind proof of work was very innovative because it simultaneously solved two problems.
First, it provided a simple but moderately effective consensus algorithm. That is, all the "nodes" on the network have agreed collectively to a set of updates to the state of the Bitcoin ledger.

Second, allowing anyone to participate in the consensus process not only solves the political problem of consensus decision, but also provides a mechanism to defend from Sybil attacks. It does this by substituting a formal barrier to participation, such as the requirement to be registered as a unique entity on a particular list, with an economic barrier. Accordingly, the weight of a single node in the consensus voting process is directly proportional to the computing power that the node brings.

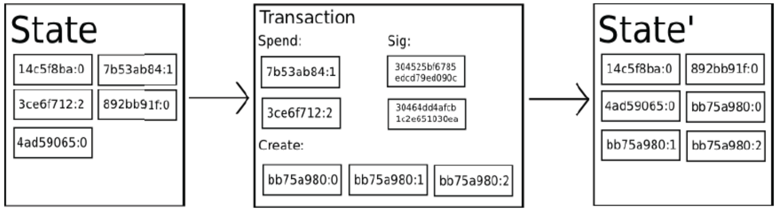
Since then, a new type of consensus algorithm called proof of stake has emerged, which means that each node needs to calculate the decision power of each node based on the amount of money held, rather than the computational ability of each node. The discussion of the relative merits of these two approaches is not covered in this white paper, but it should be pointed out that both methods can be used as the basis for encrypted currency.

4. Additional Data

Coin as the State Transition System

From a technical point of view, the ledger of cryptocurrency such as Bitcoin can be thought of as a state transition system. The system consists of a "state" of current bitcoin ownership status and a "state transition function" that receives the current state and transaction and outputs the new state. In a standard banking system, for example, the state is a balance sheet, a transaction is a request to move $X from A to B, and the state transition function reduces the value of A's account by $X and increases the value of B's account by $X. If A's account has less than $X in the first place, the state transition function returns an error. Accordingly, it can be defined as follows:

APPLY (S, TX) -> S 'or ERROR
In the conventional banking system defined above,
APPLY ({Alice: $ 50, Bob: $ 50}, "send $ 20 from Alice to Bob") = {Alice: $ 30, Bob: $ 70}
But:
APPLY ({Alice: $ 50, Bob: $ 50}, "send $ 70 from Alice to Bob") = ERROR



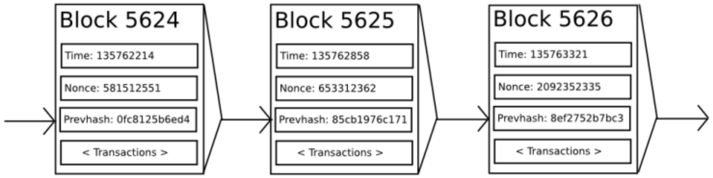
In Bitcoin, "state" is a set of all coins that have been created but not yet used (technically, 'unspent transaction output', or UTXO). Each UTXO has its own coin amount and an owner (defined by a 20-byte address which is essentially a cryptographic public key). Each entry contains reference information for an existing UTXO selected from the sender's purse address and an encrypted signature generated by a private key corresponding to the e-wallet address.

The state transition function APPLY(S,TX) -> S' can be defined as follows:
1. For each input of TX: * If the referenced UTXO is not in `S`, return an error. * If the signature does not match the owner of the UTXO, return an error.
2. If the sum of the denominations of all input UTXO is less than the sum of the denominations of all output UTXO, return an error.
3. The UTXO used in the input is deleted and the output UTXO is added and `S` is returned.

Here, the first half of the first step is to prevent nonexistent coins from being used in the transaction, and the second half is to prevent other coins from being used in the transaction. The above procedure is applied to the actual bit coin payment process as follows. Suppose Alice wants to send 11.7 BTC to Bob. First, we look for a set of UTXOs with a sum of the wallet address of at least 11.7 BTC or more. In most cases, you will not be able to choose exactly 11.7 BTC. Suppose you can refer to three UTXOs with 6, 4, and 2 BTCs in Alice's wallet address, respectively. Then, Alice creates a transaction with those three inputs and two outputs. The first output will be 11.7 BTC with Bob's address as its owner, and the second output will be the remaining 0.3 BTC "change". If Alice does not claim this change by sending it to an address owned by herself, the miner will be able to claim it.

4. Additional Data

Mining



It would be very simple if we could implement what we described above as a trustworthy centrally centralized service. This is because it could be coded exactly as described, using a centralized server's hard drive to keep track of the state. However, in Bitcoin, we want to build a decentralized currency system, which must combine a transaction ordering system that everyone can accept with a state change system. The distributed coalescing process of bit coins requires nodes that attempt to continuously create a transaction package called ‘blocks’ in the network. The network is planned to generate one block approximately every 10 minutes, and each block contains a list of all transactions that have occurred since the previous block, including a time stamp, a nonce, a reference to the previous block (hash of the previous block). This process creates a persistent, ever-growing, "block-chain" that continually updates to represent the latest state of the Bitcoin ledger as time passes.

To check whether the block is valid, the algorithm is as follows:

1. Check if the previous block referenced by the block exists and is valid.
2. Check that the timestamp of the block is greater than that of the previous block[Note 2] and less than 2 hours into the future
3. Check that the proof of work on the block is valid.
4. Let S[0] be the state at the end of the previous block.
5. Suppose TX is the block's transaction list with n transactions. For all i in 0...n-1, set S[i+1] = APPLY(S[i],TX[i]) If any application returns an error, exit and return false.
6. Return true, and register S[n] as the state at the end of this block.

Basically, each transaction in the block must cause a valid state transition. Note that the state is not recorded in any way in the block. The state is a fully abstract abstraction that must be computed and remembered by the validating node, which can be computed by sequentially applying all transactions from the original state to the corresponding block. Notice the order of the transactions that the miner will include in the block. Suppose there are two transactions in a block, A and B, and B consumes the output UTXO of A. If A is a transaction prior to B, then the block is valid, but not valid.
A characteristic part of the block validation algorithm is that it requires the condition of "proof of work". Specifically, he double-SHA256 hash of every block, treated as a 256-bit number, must be less than a dynamically adjusted target. The goal of proof-of-work is to make the creation of blocks computationally difficult, thus preventing Sybil attackers from arbitrarily manipulating the entire block chain.

4. Additional Data

Mining

Since SHA256 is designed as a pseudorandom function, completely unpredictable. The only way to create a valid block is to continue to increase the nonce of the block header and to see if the new hash matches and meets the above conditions.

In order to attain the valid block under the current target value of 2192, an average of 264 attempts must be made. In general, this target value is readjusted by the network every 2016 blocks so that the current nodes in the network can generate new blocks on average every 10 minutes. To compensate for these calculations, the miners of each block at the present time are entitled to 25 BTC. Additionally, if any transaction has a higher total denomination in its inputs than in its outputs, the difference also goes to the miner as a "transaction fee". Incidentally, this is also the only mechanism by which BTC are issued; the genesis state contained no coins at all.

To better understand the purpose of mining, let us examine what happens in the event of a malicious attacker. A Bitcoin based cryptosystem is known to be secure. Therefore, the attacker will target 'transaction sequence', which is not directly protected by the cryptographic scheme in the bit coin system. The attacker's strategy is very simple.

1. Pay 100 BTC to the seller to purchase a certain item (preferably a digital item delivered immediately).
2. Wait for the goods to be sent.
3. Create a transaction that sends the same 100 BTC to the attacker himself (double payout attempt).
4. The bit coin network should recognize that the transaction sent to the attacker itself is performed before the transaction to be paid to the seller.

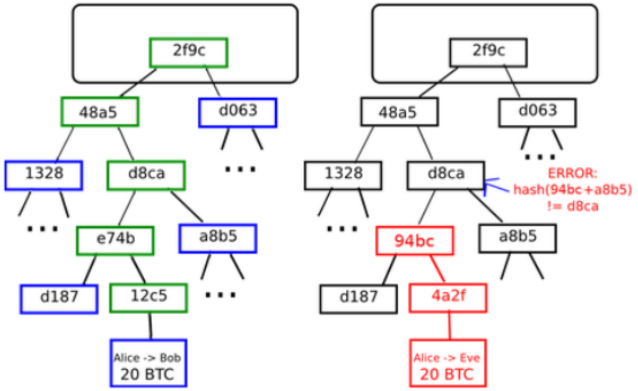
After step 1 has occurred, and a few minutes later, some diggers will include the transaction in the block. Let this block number be 270,000. After approximately one hour, five blocks will be added to the chain following this block. These five blocks are "confirming" by indirectly pointing to transaction # 1 above. At this point, the seller will determine that payment has been completed and send the goods.

Since we assumed it to be a digital product, the delivery takes place immediately. Now, the attacker creates another transaction sending the 100 BTC to himself. If the attacker simply attempted a transaction, the miner will run `APPLY (S, TX)` and notice that the `TX` tries to consume UTXO that no longer exists in the state. So instead, the attacker creates a "fork" of the bitcoin block-chain, starting by mining another version of block 270,000 pointing to the same block 269,999 as a parent but with the new transaction in place of the old one. Because the block data is different, this requires redoing the proof of work for the concerned block. Furthermore, since the attacker's new version block 270,000 has a different hash than the existing 270,000, the original blocks 270,001 through 270,005 do not point to the attacker's block. Therefore, the original chain and the new chain of attackers are completely separated. The rule of the bit coin network at such a branch point is to recognize the longest block chain as true. Since an attacker is working alone in his chain, legitimate miners will work on the original 270,005 chain, so to make the attacker's own chain the longest, the computational ability of the other nodes in the network must be greater than the computational ability. (This is called a 51% attack.)

4. Additional Data

Merkle Tree

An important extendibility of Bitcoin is that the blocks are stored in a multi-level data structure.
The "hash" of a block is actually only the hash of the block header, a roughly 200-byte piece of data that contains the timestamp, nonce, previous block hash and the root hash of a data structure, which is also known as the Merkle tree that stores all transactions in the block.
Merkle tree is a type of binary tree, composed of a set of nodes with a large number of leaf nodes at the bottom of the tree containing the underlying data, a set of intermediate nodes where each node is the hash of its two children, and finally a single root node, also formed from the hash of its two children, representing the "top" of the tree. The purpose of the Merkle tree is to allow data in any block to be separated and delivered. A node of the coin downloads only the block header from one source, and the transaction information associated with this block header is different. Downloading from the source ensures that the data is still accurate. This is possible because the hashes propagate upward: if a malicious user attempts to swap in a fake transaction into the bottom of a Merkle tree, this change will cause a change in the node above. Since the hash of this block changes as a result. This means that this block is a completely different block thanks to the proof of work.



Left: It is sufficient to verify the effectiveness of the branches only by looking at few nodes of Merkle tree.
Right : The attempts to alter Merkle tree somewhere eventually leads to inconsistency in the upper hash value.

The Merkle Tree protocol is the basis for long-term sustainability of Bitcoin networks. A "full node" that stores and processes all the information for each block in a bitcoin network requires nearly 15 GB of disk space as of April 2014 and is growing by over 1GB per month. At present, it can be accommodated on a desktop computer, but not on a smartphone. Later, it will be able to maintain a few businesses or pool nodes. A protocol known as "simplified payment verification (SPV)", on the other hand, enables another type of node called a "light node". It downloads the block headers, verifies the proof of work on the block headers, and then downloads only the "branches" associated with transactions that are relevant to them. This ensures that even though only a very small percentage of the entire block chain is downloaded, the state and balance state of any transaction can be determined, while ensuring strong safety.

Various Cases of Block-Chain and Scripting

◎ Various Cases of Block-Chain

The idea of expanding the basic idea of block chain and applying it to other concepts has a long history. In 2005, Nick Szabo stated his concept of secure property titles with owner authority "proprietary rights". He designed a sophisticated framework that included concepts such as homesteading, illegal occupation, and Georgism, and showed that the registration problem of who owns a land can be treated as a block-chain-based system. He said this was made possible by "a new evolution of database replication technology." Unfortunately, at the time, there was no effective file-duplication system available, rendering the protocol of Nick Szabo not realized. However, since 2009, as the Bitcoin decentralization consensus system has evolved, numerous alternative applications have begun to emerge rapidly.

* **Namecoin** - The Namecoin created in 2010 will be best referred to as a 'decentralized name registration database'. When using a decentralized autonomous organization protocol such as tor, bitcoin or bit message, the user has to distinguish his / her account in order to interact with others. However, the existing possible distinction method is to use a pseudo-random number hash such as 1LW79wp5ZBqaHW1jL5TCiBCrhQYtHagUWy. Ideally, it would be good for the user to have a common name like "george" as the account name. However, the problem is that if one person can create an account named "george" then someone else can use the same process to register "george" for themselves as well and impersonate them. The only answer is that the first person to register is successful and the second person to register fails. This is a problem that has already been fully applied to the bit coin agreement. Namecoin is the oldest and most successful name registration system applying this idea.

* **Colored Coin** - The purpose of Colored Coin is to serve as a protocol for anyone to publish his / her own unique digital currency on a Bitcoin block chain as a protocol for issuing its own digital token (which can be viewed as a simple case where the volume of digital money is only one unit). In the colored coins protocol, one "issues" a new currency by publicly assigning a color to a specific Bitcoin UTXO, and the protocol recursively defines the color of other UTXO to be the same as the color of the inputs that the transaction creating them spent (in the case of mixed color input, some special rules apply). This protocol traces back the block chains from beginning to end to determine the color of the UTXO they received so that the user can keep only the UTXO with a specific color in his wallet and send the coin up and down like a normal bit coin.

* **Metacoin** - The idea behind Metacoin is that it has a protocol running on the bit coin system, using the bit coin transaction for storing the Metacoin transaction, but having a different state transition function, APPLY'. Because the Metacoin protocol alone cannot prevent the occurrence of invalid Metacoin transactions in the bit coin block chain, one rule is added. That is, if APPLY'(S,TX) returns an error, the protocol defaults to APPLY'(S,TX) = S. Bitcoin itself is an easy mechanism to create a random cryptographic protocol with potentially more advanced properties that cannot be executed internally. On the other hand, the cost of developing this protocol is low because the problem of mining and networking complexity is already handled by the bit coin protocol.

Various Cases of Block-Chain and Scripting

In general, there are two approaches toward building a consensus protocol: building an independent network, and building a protocol on top of Bitcoin. The former approach has been quite successful in applications such as Namecoin, but it has difficulty in actual execution. Not only does each individual executor have to build and check all the necessary state transitions and networking code, but also run independent block chains. Furthermore, it is expected that the set of applications on the decentralization agreement technique will follow the inverse function distribution. That is, most applications will be too small to guarantee their own block chains. We also expect that there will be decentralized applications of large classes, that is, decentralized autonomous organizations (DAO) to interact with each other.

The Bitcoin-based approach, on the other hand, has the flaw that it does not utilize the simplified payment verification features of Bitcoin. Simple payment verification works on Bitcoin. Because Bitcoin can use the block chain depth as a verification means. If you look back enough to find the source of a transaction, you can say that there was a part that proved the coherence of the state. On the other hand, a meta-protocol based on a block chain does not have its own protocol itself to prevent invalid transactions from being included in a block chain. Therefore, fully secure SPV meta-protocol implementation would need to backward scan all the way to the beginning of the Bitcoin blockchain to determine whether or not certain transactions are valid. So far, all "light" block-chain users' implementations of a bit coin-based meta-protocol have depended on a reliable server to provide the data. If we especially recall that the most important purpose of creating a cryptogram was to eliminate the need for a third credit mechanism, this is, quite obviously, only a second-line outcome.

◎ Scripting

Without additional extensions, the Bitcoin protocol can enable the concept of a low-level "smart contract", though not full but weak. Bitcoin's UTXO can be obtained not only with public keys, but also with more complex scripts expressed in a simple stack-based programming language. In this case, the transaction that spends UTXO must provide data that satisfies the script. In fact, even the basic public key ownership mechanism is implemented via a script: the script takes an elliptic curve signature as input, verifies it against the transaction and the address that owns the UTXO, and returns 1 if the verification is successful and 0 otherwise. There exists more complicate forms of script language when used in the real practice.

For example, you can script to get validation only if you get a signature from two out of the three given private keys. These scripts can be useful for corporate accounts, security savings accounts, commercial depository situations, and so on. Scripts can also be used to pay rewards for answers to certain calculation problems. "If you provide an SPV proof that you sent me this pottery coin transaction, this bitcoin UTXO is yours". Indeed, the decentralized, inter-cipher currency exchange can be made fairly easily. However, the script language implemented in Bitcoin has some important, inherent limitations with it.

Various Cases of Block-Chain and Scripting

* Turing incompleteness: There are a lot of things that you can do with the script language, but it does not support all the programming. The main category that is missing is loops. This is done to avoid infinite loops during transaction verification. Theoretically, this is an obstacle that script programmers can overcome. This is because any cycle instruction can be implemented simply by repeating the underlying code multiple times with the if statement. However, this is a very space-inefficient program. For example, to execute an alternative elliptic curve signature algorithm, it would require 256 repeated multiplication rounds all individually included in the code.

* Value Blindness: There is no way to fine-tune the amount of withdrawal with UTXO script alone. For example, hedge contracts is a powerful example that illustrates the use of oracle contract. Let A and B deposit a $1000 BTC into a joint account. After 30 days the script sends $1,000 worth of BTC to A and the rest to B. This would require an oracle to determine the value of 1 BTC in Dollar. However, this contract requires a third party to determine how much 1BTC is in US dollars. If such a contract is feasible, it can be regarded as a highly developed contract type even under the present fully centralized financial system. On the contrary, UTXO is all-or-nothing in that the only way to achieve it is through the infefficient hack of having many UTXO, with the denominators varying (for example, to make 1 UTXO of 2^k, numbers ranging from k up to 30).

* Limitations in Representing State: The states that UTXO can represent are either used or not spent. Therefore, you cannot create a multilevel contract or script with any internal state other than spend or not spend. This makes it difficult for multi-stage option contract, or for istributed currency exchange transactions or two-stage cipher execution protocols (which are necessary to guarantee compensation for computation). That is, UTXO can only be used for simple, one-time contracts, but it cannot be used for more complex "stateful" contracts such as distributed organizations and makes meta-protocols difficult to apply.

* Blockchain-blindness: UTXO cannot decode block chain data such as nonce, timestamp, and previous block hash. This severely limits applications in gambling, and several other applications, because the script language for potentially valuable randomness is eliminated.

In summary, there are three approaches to creating developed applications. The first is to create an independent block chain, the second is to use a script already embedded in the Bitcoin, and the third is to build a meta-protocol that operates on a Bitcoin. Developing independent block chains allow you to create infinitely free programs, but you have to pay for the development, initial setup and care about its security. Scripts embedded in Bitcoin have the advantage of being simple and standardized, but their use is limited. Meta-protocols are easy to use, but it has flaws in extendibility. REVV coin is a system that shares block-chain security with an economic development environment, while having a stronger user interfaces and features that can overcome the aforementioned challenges.

5. References

References and Additional Information

1. Intrinsic value: http://bitcoinmagazine.com/8640/an-exploration-of-intrinsic-value-what-it-is-whybitcoin-doesnt-have-it-and-why-bitcoin-does-have-it/
2. Smart property: https://en.bitcoin.it/wiki/Smart_Property
3. Smart contracts: https://en.bitcoin.it/wiki/Contracts
4. B-money: http://www.weidai.com/bmoney.txt
5. Reusable proofs of work: http://www.finney.org/~hal/rpow/
6. Secure property titles with owner authority: http://szabo.best.vwh.net/securetitle.html
7. Bitcoin whitepaper: http://bitcoin.org/bitcoin.pdf
8. Namecoin: https://namecoin.org/
9. Zooko's triangle: http://en.wikipedia.org/wiki/Zooko's_triangle
10. Colored coins whitepaper:
https://docs.google.com/a/buterin.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit
11. Mastercoin whitepaper: https://github.com/mastercoin-MSC/spec
12. Decentralized autonomous corporations, Bitcoin Magazine:http://bitcoinmagazine.com/7050/bootstrappinga-decentralized-autonomous-corporation-part-i/
13. SiREVVlified payment verification:https://en.bitcoin.it/wiki/Scalability#SiREVVlifiedpaymentverification
14. Merkle trees: http://en.wikipedia.org/wiki/Merkle_tree
15. Patricia trees: http://en.wikipedia.org/wiki/Patricia_tree
16. GHOST: http://www.cs.huji.ac.il/~avivz/pubs/13/btc_scalability_full.pdf
17. StorJ and Autonomous Agents, Jeff Garzik: http://garzikrants.blogspot.ca/2013/01/storj-and-bitcoinautonomous-agents.html
18. Mike Hearn on Smart Property at Turing Festival: http://www.youtube.com/watch?v=Pu4PAMFPo5Y
19. Ethereum RLP: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-RLP
20. Ethereum Merkle Patricia trees:https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-Patricia-Tree
21. Peter Todd on Merkle sum trees:http://sourceforge.net/p/bitcoin/mailman/message/31709140/

REVV COIN

REVcoin2@gmail.com

http://www.rev-coin.biz

Meet-up