Technical paper regarding BitRich

Auto Exchange System

BitRich Total E-wallet Address

bitRich Global
The **Future** Of The **Global Financial** System

Technical paper regarding BitRich Auto Exchange System

1. Abstract

Experts have said that dispatcher, block-chain technology, virtual currency and smart contracts will create innovation in the foundations of existing industries. In other words, they think automated payments, transactions and contracts in the network will serve as a fundamental shift in the foundation of their existing industry. In fact, there are automated payments and transaction related platforms and services already in the market due to the growth of Bitcoin and Ethereum, in addition, it is viewed as dispersion application growing in the financial industry. As part of these new technologies, developers are building new tools, and they are finding mainstream, safe solutions that will be embraced by the general public and its organizations.

2. Background

As part of the block chain system, virtual currencies, such as, the Bitcoin (BTC), the NEO (formerly AntShares) and the ETH2XB (ETH2XB) have emerged as early leaders in digital asset distribution. Based on its block chain technology and distributed headquarters, SatoshI Nakamoto developed the first virtual currency, called the Bitcoin (BTC), in 2008. Since then, there have been many virtual currencies created, and market capitalization has never been higher. (Increase by 1000 % in 2017). Businessmen, venture capitalists, bankers, and other experts assume that virtual money will eventually become a new criterion and that businesses will eventually thrive. However, it was proven that recently created block chain knowledge and the technology of virtual currency background it more important.

3. Blockchain technologies

In a block chain, transaction information is contained in 'Block'.
When the block is full it closes and displays a number that summarizes the transaction information contained within it. The displayed number will be connected to the next block like chains of orgery/alteration can be verified easily by checking the last block. The individual will save the information on

their computer. In addition, no one can modify the information in "block chain". In this system data forgery/alternation will be prevented and reliability and transparency of the transaction will be secured because anyone can view the result on the changes. Block chains are considered to be the safest transaction method today. In order to try to forge them, one would have to change all the blocks in the ledger, However, that is an impossibility within the existing system.

The block chain aims to decentralize because it gives full control to individuals, not to central institutions, and it decides everything based on their agreement.

The reason why the term "currency " is used as virtual currency, digital currency, or encrypted currency is because it can be a " reliable " target. The source of trust is the block chain.
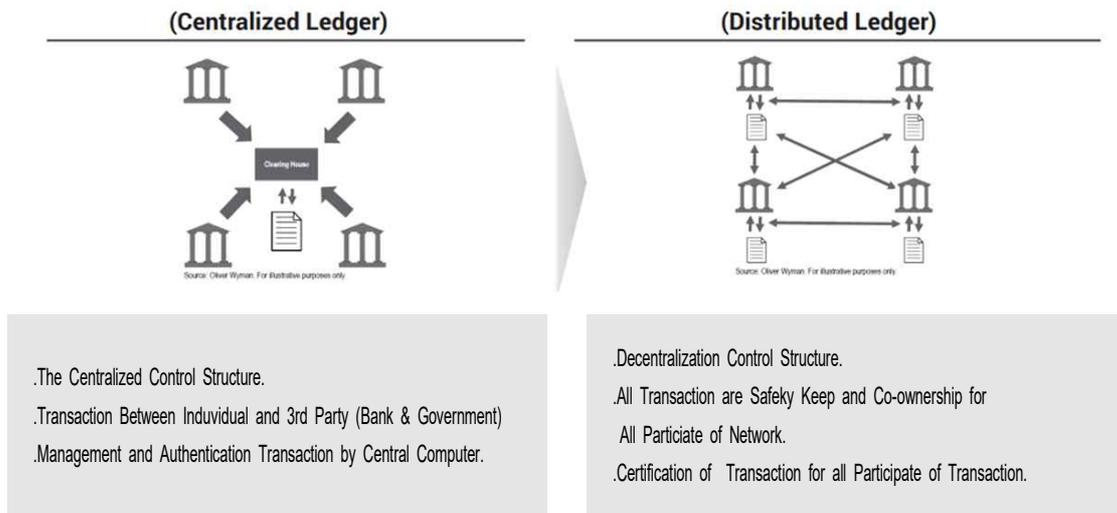

What a Block chain is,

A Block chain is a huge, distributed public account, and all of the individual transactions contained within it are digitally signed and can be guaranteed to be genuine without the need for bank or other third party intervention. It consists of thousands of nodes, so even with failure/attack the block chain network will run without problems. Through the correct mathematical calculation procedures, known as work validation and economic logic, it is impossible to perform forgery/alteration within the structure. It can be correctly concluded that recorded transactions are secured even without a centralized guarantee agency, such as a bank.

Divergence can occur as they propagate to distributed environments, but you select the longest block chain as a valid block chain. Only the main network remains as the original valid one.

---

3. 1 Distributed Public Register (Other Centralization)

Existing methods of storing data are vulnerable to hacking and relatively high maintenance costs as the transaction notarization and management of the central server of the individual's transaction has been conducted by a trusted agency. However, distributed disclosure books provide a way for transactions to be made to ensure transparency of information through shared and archived (P2P) transactions among all network participants, reducing the risk and maintenance costs of hacking.

<table>
<tr><td>.The Centralized Control Structure.

.Transaction Between Induvidual and 3rd Party (Bank & Government)

.Management and Authentication Transaction by Central Computer.</td><td>.Decentralization Control Structure.

.All Transaction are Safeky Keep and Co-ownership for
 All Particiate of Network.

.Certification of Transaction for all Participate of Transaction.</td></tr>
</table>

All of the transaction information in the block chain includes digital signatures so that you can trust that the transaction information is original.

3. 2 Digital Signature

Digital signature uses non-synchronizing keys and hash functions which help determine whether the data is true or not using following ways :
All of the transaction information in the block chain includes digital signature which makes the client rely on the transaction information.

3. 3 Node (HTTP Server)

Normal node (light node) is the node that participates in the block chain to perform the transaction which does not contain all block information. So SPV(Simple Payment Verify) will be performed in order to check individual transaction:
To validate the transaction, the normal node will request block information to full node and check whether it is validated transaction or not using Mockle-tree.
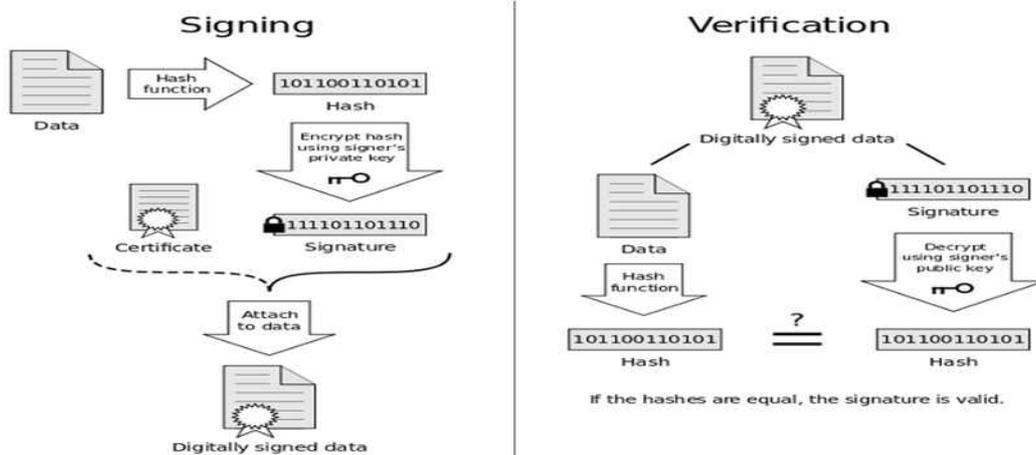
Full node is a node which gather and save all block chain information
perform block verification to add new block save and manage newly verfied block
or requested block information
All the message in block chain will be broadcasted.
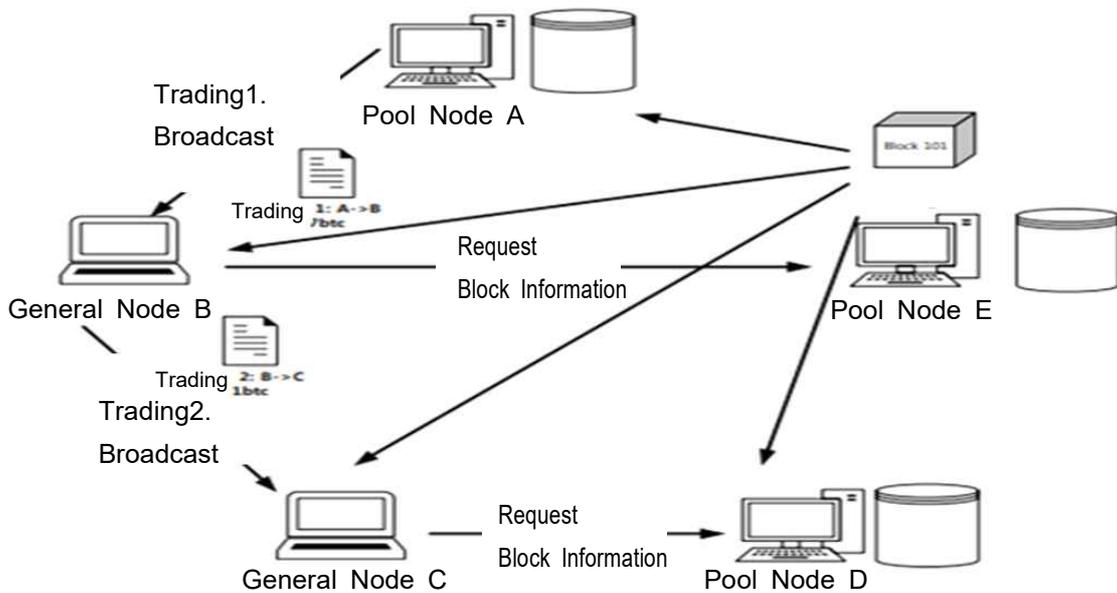
3. 4 Block Chain

A block chain is technically a collection of blocks that are made by blocks. A block is a bundle of valid transaction information and the block header consists of six types of information:

* version: Software/protocol version
* previousblockhash : Block hash of the block directly in front of
   the block chain
* merklehash : When configuring the transaction hash of the individual
   transaction information in binary tree form, the hash value in the tree root.
* time: Time in creating the block
* bits: Value used to adjust the level of difficulty
* nonce: The number of calculations that are incremented by one, starting at
   the first zero, until a hash value satisfying the condition is found.

The block chain is consist of 2 types of information : a block list (chain list) and a transaction list.

★ Confirm arrival block;

★ Confirm arrival transaction;

★ synchronization of transaction list.

★ synchronization of block list.

A block chain is a list of chains in which the hash of the following blocks is calculated based on the hash of the previous block and data from the block itself.

★ When the relevant block is the last block (Previous index + 1);

★ When previous block is correct (Previous hash == block.previousHash);

★ Hash is correct (Calculated block hash == block.hash).

★ The job proof task is at the right level of difficulty.
   (Level of difficulty block _n_ <Difficulty blocking);

★ All the transaction within the block is valid.

★ The sum of output transactions is the sum of
   input transactions + compensation for block miners.

3. 5 Transaction

The transaction contains an input and output list that indicates the transfer of coins between the coin owner and the address. The input list contains a list of existing unused output transactions and is signed by the address owner. The output list contains the amount for other addresses, including changes in owner's address. Are transactions within the block valid?

★ When transaction hash is accurate
   (Calculated transaction hash == transaction.hash);

★ If all input transactions are signed correctly
   (transaction data is signed with the public key of the address).

★ If the total number of input transactions is greater than the output
   transaction, you may need to obtain transaction fees.

★ If the transaction is not existing in block chain

★ If all input transactions are not used in the block chain

4. Overview of Auto Exchange System and Smart wallet

BitRich coin is a payment coin that can be used by the user on mobile devices, including merchant. BitRich coin customers use the allowance of an integrated compatible wallet to use their coins for Auto Exchange. BitRich Integrated Wallet allows you to manage multiple coins simultaneously by including various coins based on block chains. In addition, it is configured to be used in the exchange method se tby the merchant.

We offer protocols for payment across the transaction system. Anyone who has BitRich account can use Auto Exchange.

This is for consistency and continuity with the payment merchant.

Currently, there are too many kinds of coins and wallets, so the merchants must bear the burden of preparing different kinds of wallets for each coin. However, through BitRich Auto Exchange system, the coins can be used in by the

merchants after converting to BTR in addition to using this system conversion to KRW and other kinds of coin is also possible. Those bitcoins, dashes ,Ethereum held by the account can also covert to BTR and be saved or conveniently used in the BTR member stores.

4. 1 Design and Principles of Auto Exchange System and Integrated wallet

1. There is need to rely on connectors like Escrow.
2. A new type of trading platform that seeks security and efficiency based on the Stirling completeness
3. Modular consensus mechanisms to meet diverse demands.
4. Combinedataonablockchainwithdatathatisoffchain.
5. BlockchainAutoExchangedesignforvalueandinformationtransfers
6. Considersecurityandconveniencewithintegratedwallets

4. 2 Future Plan

We have big plan. By using mobile app cards it is enable to offer the customers many features that are not easily accessible by other digital calling and token wallet apps. Over time, we aim to create a world that is much easier and more intuitive regarding coin.

4. 3 New concept

Seven years after Bitcoin, one of the greatest experiments ever, we saw the emergence of a new industry. Ethereum have added Turing-complete mix and expanded.

This in turn led to the creation of a new synergy ecosystem that would reverse the status quo. There have been many attempts over the years to introduce encryption to the public, but adoption is still slow. Key issues include:

The security of storing assets is annoying and inevitably people choose to store them under third parties, such as exchanges. This destroys one of the biggest attributes of cryptocurrency and exposes it to risks that have been consistently proven fatal. Many people often put a lot of effort into seeing the actual use

of their digital assets. Users need wallets, exchanges, and accounts for various services.

5. Design of Auto Exchange System and smart integrated wallet

5. 1 Auto Exchange System Market

1. Sign up : Encrypt member information with SHA-3 hash algorithm

2. Transaction : Transaction through multi-sign

3. Data security : A multi-sigma contract suitable for use in wallets. It serves as a 2-3 multi-signing wallet for transferring some feature transactions in the contract. Support for synchronous (single transaction) approval with multiple signatures using ecrecover.

You can distribute a forwarder contract so that you can have multiple in coming addresses in a single wallet.

A bearer address contract has the ability to flush funds sent to the address before the contract is created.

The ERC 20 token can be flushed from the bearer wallet to the primary wallet with a single signature as the primary signatories.

The ERC 20 token and ether can be sent from the main wallet through the multi-sign process.

You can set 'Safe Mode' on a wallet contract to prevent the ETH2XB and ERC20 tokens from being transferred to other than the wallet signatories.

5. 2 Key Recovery Service

Main provisioning protocol (End point of bringing the key), provisioning key is from xPub. An email that is sent to the user when the key is provisioned to establish a relationship with the BitRich provider. Script for which the user configures and signs the recovery transaction for BitRich wallet.

Recovery request end points that use transactions to request signatures store the requested recovery and send an e-mail to BitRich owners and users. Offline signature tool (JSONformat) to sign a recovery request.

5. 3 JSON format onOffline Signing Tool

usage: signoffline.js [-h] [-v] [-f FILE] [-k KEY] [--confirm]

Tool to sign recovery JSON offline (for KRS owners recovery)

Optional arguments:
Offline Recovery Tool provides BitRich customers with a mechanism to search for BitRich stored with their BitRich wallets regardless of their BitRich status.

6. Auto Exchange and integrated wallets

6. 1 Hybrid App (iOS / Android)

The Wallet App (Android and iOS) is the primary interface that customers will use to interact with the platform. BitRich App is designed to deliver best-in-class functionality with top-level UI designs.
Set-up Wizard At first startup, the user is prompted to run the setup wizard and customize the settings to suit their preferences. The process includes the following steps
- Users download applications
- Users can create a new contractkey or import key.
- You will be prompted to enter a password and back up the key.
- Start of contract / load (BTR payment for gas)
- Select the Quick or Advanced Setup Wizard.
- Users select the default currency from the ranked list.
- World Wide Frame Walk, User Interface We have designed a diagram of more than 10 pages of Page State and with hundreds of transitions.

7. Design Logic and Algorithm

This development logic stores and automatically exchanges at least one or more of the encrypted currencies traded in an encrypted currency exchange and in an encrypted currency exchange to design and develop an encrypted currency exchange. Cryptocurrency trade for designing and developing cryptocurrency trade and

trading on an cryptocurrency exchange, Storage of at least one cryptocurrency, The cryptocurrency stored in the integrated electronic wallet system can be converted to another second cryptocurrency through the cryptocurrency of Exchange, cryptocurrency Conversion After switching to a standard cryptocurrency, The above standard cryptocurrency is characterized by conversion of the above standard cryptocurrency into the above secondary cryptocurrency, The above standard encryption currency is,It provides an automated, encrypted currency exchange system with an integrated electronic wallet featuring values linked to the value of real money.

7. 1 BitRich Network
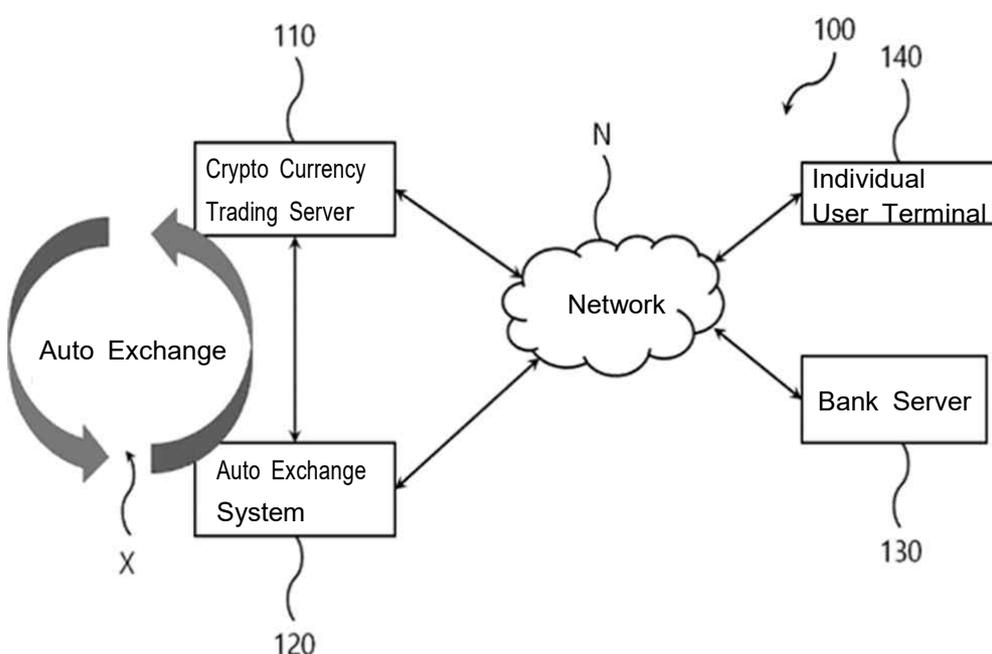
BitRich network is a multI-network using a block chain based base and its own intranet. For real-life storage, you will use a banking network, and payment will use a user-specific terminal.

7. 2 Member security system with multI-sign

The default signatories wallet is designed for use in a co-signature environment where two signatures are required for fund transfers. Typically used for 2/3 signature configuration. Use ecrecover to allow two signatures in a single transaction. The first signature is generated from the job hash (see Data format) and passed to sendMultiSig / sendMultsigToken. The signatories are determined

by verifi .ig (). The second signature is created by the transaction submitter (msg. signer).

```
contract WalletSimple {
  event Deposited(address from, uint value, bytes data);
  event SafeModeActivated(address msgSender);
  event Transacted(
      address msgSender, transaction
      address otherSigner,
      bytes32 operation,
      address toAddress,
      uint value,
      bytes data
  );

  address[] public signers;
  bool public safeMode = false;

  uint constant SEQUENCE_ID_WINDOW_SIZE = 10;
  uint[10] recentSequenceIds;

  function WalletSimple(address[] allowedSigners) public {
    if (allowedSigners.length != 3) {
      revert();
    }
    signers = allowedSigners;
  }

  function isSigner(address signer) public view returns (bool) {
    for (uint i = 0; i < signers.length; i++) {
      if (signers[i] == signer) {
        return true;
      }
    }
    return false;
  }
```

```
modifier onlySigner {
  if (!isSigner(msg.sender)) {
    revert();
  }
  _;
}
function() public payable {
  if (msg.value > 0) {
    Deposited(msg.sender, msg.value, msg.data);
  }
}
```
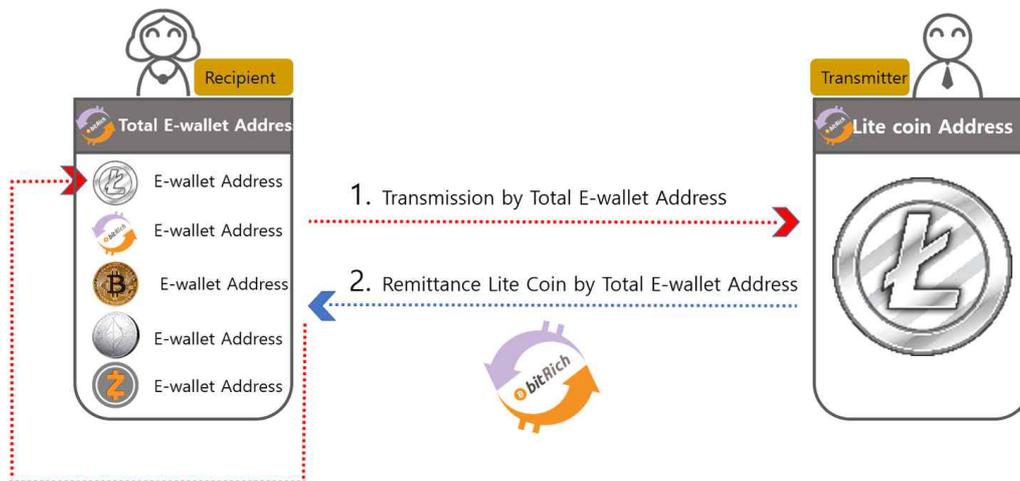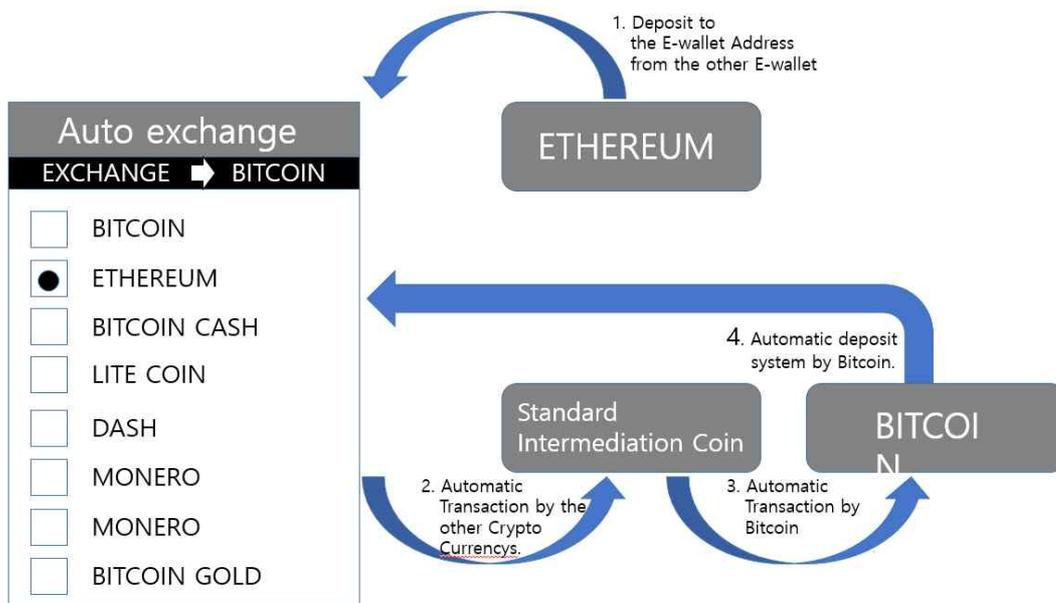
Skip…

The code above is a multI-signed base example, which is the basic code for controlling and securing users based on their own platform.

7. 3 Crypto currency Total E-wallet Address and auto exchange System

1. Transmission by Total E-wallet Address

2. Remittance Lite Coin by Total E-wallet Address
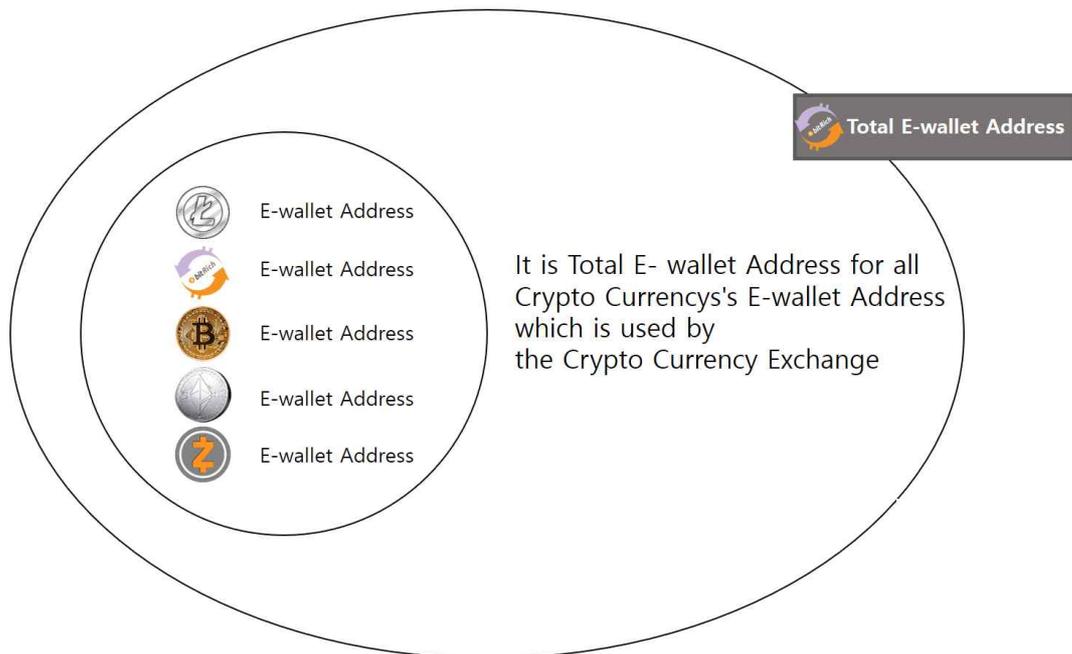
3. Identifying Lite Coin and deposit to the Lite Coin E-wallet address.

7. 4 coinList()- Obtain the current list of all cryptocurrencies and the following information for each token :

const cc = require('cryptocompare')

// Usage:
cc.coinList()

```
.then(coinList => {
  console.log(coinList)
  // ->
  // {
  //    BTC: {
  //       Id: "1182",
  //       Url: "/coins/btc/overview",
  //       ImageUrl: "/media/19633/btc.png",
  //       Name: "BTC",
  //       Symbol: "BTC",
  //       CoinName: "Bitcoin",
  //       FullName: "Bitcoin (BTC)",
  //       Algorithm: "SHA256",
  //       ProofType: "PoW",
  //       FullyPremined: "0",
  //       TotalCoinSupply: "21000000",
  //       PreMinedValue: "N/A",
  //       TotalCoinsFreeFloat: "N/A",
  //       SortOrder: "1",
  //       Sponsored: false
  //    },
  //    ETH: {...},
  // }
})
.catch(console.error)
```

7. 5 exchangeList() - Returns all exchanges that have been combined by CryptoCompare.

```
const cc = require('cryptocompare')

// Usage:
cc.exchangeList()
.then(exchangeList => {
  console.log(exchangeList)
  // {
  //    "Cryptsy":
```

```
//    {
//       "42":["BTC","BTR"],
//       "EMC2":["BTC","BTR"],
//       "POINTS":["BTC"],
//       "VTC":["BTC","LTC","BTR"]
//       ...
//    }
//    ...
// }
})
.catch(console.error)
```

7. 6 price() - Get the current price of cryptocurrency in another currency

```
const cc = require('cryptocompare')
// Basic Usage:
cc.price('BTC', ['USD', 'KRW'])
.then(prices => {
  console.log(prices)
  // -> { USD: 1100.24,KRW: 1039.63 }
})
.catch(console.error)
// Passing a single pair of currencies:
cc.price('BTC', 'USD')
.then(prices => {
  console.log(prices)
  // -> { USD: 1100.24 }
})
.catch(console.error)
```

7. 7 Other Functions

◆ priceMulti()

It works like price (). However, you can specify a matrix of From symbols.

◆ priceFull()

Get all current transaction information (price, volume, public price, transaction price, lowest price) in a list of cryptocurrencies in different currencies.

◆ priceHistorical()

Gets the cryptocurrency price of another currency from the given timestamp. The price is taken from daily information. Therefore, it will be the price at the end of GMT according to the requested timestamp.

◆ generateAvg()

The current transaction information (price, volume, open price, transaction price, volume weight, etc.) of the requested pair is taken as a weighted average based on the requested market.

◆ topPairs()

Gets the top pair by volume for the call.

◆ topExchanges()

This is the highest volume deal for currency pairs.

◆ histoDay ()

Import Open State, High, Low, Closed, Volume, and Volume from daily history data. Values ??are based on 00:00 GMT time.

◆ histoHour ()

Import the open state, high, low, close, volume, and volume from historical historical data.

◆ histoMinute ()

Import open state, high, low, closed, volume, and volume from historical data in minutes.

…. skip ….

8. Legal and Regulatory Compliance

Laws and regulations - 5% There is a legal cost to set up international financial services operations. Certain services planned for the BitRich platform, such as "token exchange", may require appropriate regulatory approvals and licenses in some jurisdictions. These licenses are generally not desirable to acquire, but costs, ie, bonding, capital, and operations. Email us at bitrich@slglobal.com.

- Disclaimer

Please read this disclaimer carefully. If you have no doubts about what you should do, you should consult with your legal, financial, tax law or other professional adviser (s).

The information provided below may not be exhaustive and does not imply an element of contractual relationship. While we strive to make sure that everything in this white paper is accurate and up-to-date, it does not provide professional advice. BitRich does not assume any liability with respect to the accuracy, reliability, currency or completeness of the materials contained in this white paper.

Investors and potential BitRich coin holders should consult appropriate independent experts before making any commitments or transactions based on the materials published in this white paper. This material is for reference only. BitRich does not constitute securities in any jurisdiction. This white paper does not constitute any kind of brochure or proposal and is not intended to constitute an offer to invest in any securities or securities of any jurisdiction. BitRich does not provide any feedback on the purchase, sale or other transaction advice of BitRich Coin,

Nor does it form the basis of an investment decision and does not depend on contracts.

No person is obligated to make any contract or binding legal commitment to the sale or purchase of BitRich Coin, and crypto currency or any other form of payment is not permitted on the basis of this white paper.

Thank you