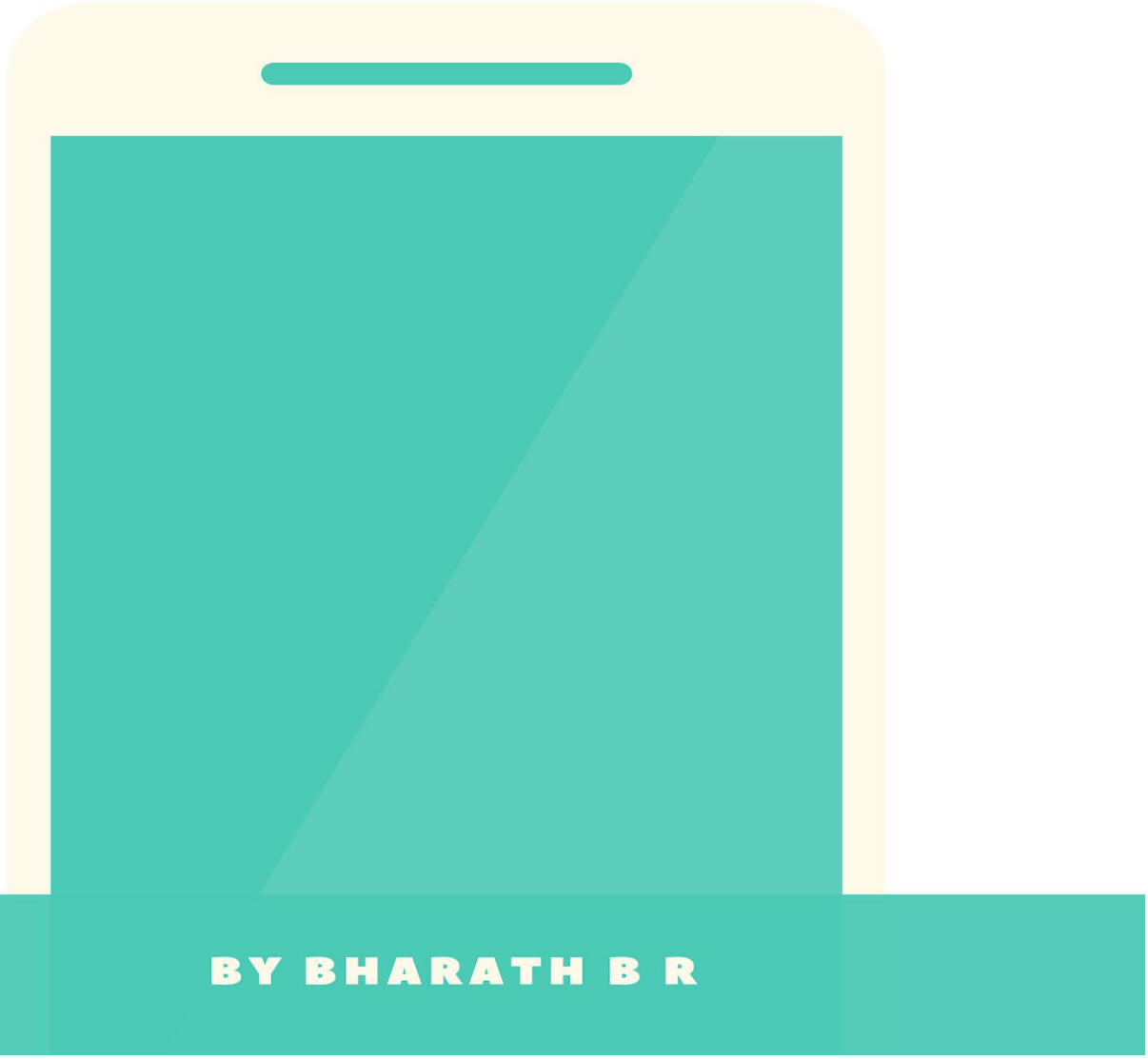
LIME WALLET

A user-friendly cryptocurrency wallet



BY BHARATH B R

Introduction

The average person will be able to remember his or her bank account number, but for a Bitcoin wallet address this is significantly harder to do.These addresses contain around 30 characters, which can be both (case sensitive) letters or numbers.

Satoshi Nakamoto did not conduct enough user experience testing prior to launching Bitcoin. He/she/they certainly didn't show up for all of the Drunk User Testing events. But the result from a lack of user experience highlights a major impediment in the form of one word when it comes to cryptocurrency adoption: Intimidation. There are solutions to these problems and more including things like the Ethereum Name Service but the process to getting a human-readable address can be quite daunting for the average user as well.EOS is the only crypto which offers easy address.

In this regards we started new initiative of to simplify and provide a single interface across all systems. Key drivers are:

- Simplicity - Paying and receiving payments should be as easy as swiping a phone book entry and making a call on mobile phone. Everyone who has wallet should be able to send and receive money with their virtual address . All they need to do is to "pay to" or "collect from" a "payment address" with a single click.

- Innovation - Solution should be minimal, functional, and layerable so that innovations on both payee and payer side can evolve without having to change the whole interface. This unified layer should allow application providers to take advantage of enhancements in mobile devices, provide integrated payments on new consumer devices, provide innovative user interface features, take advantage of newer authentication services, etc.

- Adoption - Solution should be scalable to a billion users and large scale adoption. This should allow gradual adoption across smartphone and PC users and provide full interoperability across all payment players, phones, and use cases.

- Security - Solution should provide end to end strong security and data protection. Considering self-service applications, data capture must be strongly encrypted at capture. Similarly, solution should allow a mechanism to pay and collect using true virtual addresses. While providing convenient, solution should offer 1-click 2-factor authentication, protection from phishing, risk scoring, etc.

Industry Trends

This section looks at some of the largest trends in the world particular that has impact in the way financial transactions are conducted. It is important to design new systems so that it is fully aligned to take advantage of these sweeping trends.Over the last few years, new companies and systems have emerged on the payments landscape, each of which has brought in newer technologies, and improvements on the payments experience, including easier access to the payments networks. In the below section, we highlight a few of them.

Square

Square introduced a simple piece of hardware that could turn a mobile phone into a payments device that can accept credit cards, thus allowing any one to accept card payments securely. This has now been replicated by many companies, and has expanded the number of people who can accept card payments. Square's innovation cantered around the use of a secure hardware, that could be use the compute and communication capabilities of a smartphone to enable anyone to accept a card payment.

Stripe

Stripe introduced simple APIs that allow any company with a web presence to securely accept electronic payments in as little as 10 lines of code, and a simple signup process. Stripe's innovation centres on the ease of use of acceptance of the payment information bypassing the merchant systems - thus improving security for the customer.

Apple Pay

Apple has recently launched an electronic wallet, which allows the user to make payments from existing cards, based on a 2 factor biometric

authentication. This is based on the biometric sensor installed in the phone, and a local secure element. The transaction is secure, and provides additional privacy to the user. Apple's innovation includes the use of local biometrics, built in security, the use of cryptography, and virtual card numbers to ensure that user data cannot be compromised, while ensuring that payment can be done with a remarkable ease of use.

Virtual Currencies

Over the past few years, bitcoin has created a system with a virtual currency that allows users to perform transactions, which cannot be repudiated, in the absence of a centralized trusted ledger. Based on this, and exchanges which allow the currency to be exchanged with real currencies, an entire bitcoin economy has taken off. In this economy, the cost of transactions is very low, while the amount of security is high. Bitcoin's innovation has cantered around the creation of a distributed ledger in the absence of a centralized trusted party, the use of proof-of-work as an incentive to maintain the ledger, and the use of a language to enable innovation in the use of payments, and the creation of smart contracts. Bitcoin has sparked off the creation of many virtual currencies, each with different characteristics. Other virtual currencies such as Litecoin and Dogecoin are also coming up in the worldwide market.

Ripple, Stellar and other Networks

The creation of virtual currencies, and exchanges has resulted in the creation of additional networks, which provide hooks into the existing financial system, allowing the exchange of currencies, and movement of money across financial institutions, thus further strengthening the use case for virtual currencies.Ripple, and Stellar enhance the usability of virtual currencies and real currencies, including the ability to connect institutions and exchange value.

Card Tokenization

The card number has not been a secret, and is visible to many entities in the payments chain, along with other payment credentials. The security for these systems has been controlled through audit and certification, along with instructions related to how various data has to be handled. In the event of a compromise, the institution have to replace the card - which is an expensive process. However, the use of a virtualized card number reduces the replacement cost to almost nothing. In fact, if the users

always use a virtualized card number, the system becomes that much more secure, because there is no value to stealing a number that is bound to change shortly.

Use of Smartphones as an authentication factor

Smartphones have become ubiquitous, more capable, and always stay with their owner. It is easy to see how they can be trusted by the relying party to become an authentication factor. For instance, the act of sending an OTP over the phone, and its use to access a secure system is an accepted form of security. The phone essentially becomes a 'what you have' credential. This is further extended through other mechanisms such as HOTP, and TOTP where the OTP does not have to be sent at all - but can be generated on the phone in a manner which the relying party can accept. This has been used in various systems - such as email systems, enterprise security systems, and payment systems.

Biometric Enabled Smartphones

Since smart phones have become an extension of the human identity, it has become important to secure them (and transactions) with an additional form of security. This has been achieved through the use of passwords, or biometrics to unlock the phone and its applications. Applications can use biometrics in the phone to capture credentials and use them in payment processes. While currently available popular phones use fingerprint technology, with the availability of cheaper Iris devices having much higher match accuracy, it is expected that Iris enabled smart phones will be available in near future.

The Opportunity

We are at the cusp of a revolution – technology is continuing to enter people's lives, making it easier. Users expect that their interactions with crypto will keep pace technology trends. With new players entering the payment landscape, it is to be expected that they will innovate to differentiate their services and to improve customer experience.

It is very important to take a role in ensuring that the participants continue to innovate while staying interoperable with existing systems. Interoperability allows the market to grow, provides customers with true any-to-any open payments, and helps to significantly reduce cash payments. Ecommerce, both on the web and the mobile, offers a potential

area for exponential growth in electronic payments. Payments is a large issue for the players in this segment and they will continue to look for technology that will improve the payments process.

LIME Wallet Interface

The LIME Cryptocurrency wallet offers architecture and a set of standard Application Programming Interface (API) specifications to facilitate online payments. It aims to simplify and provide a single interface across all cryptocurrencies besides creating interoperability and superior customer experience.

LIME Wallet Interface provide the following core features via a single payment API and a set of supporting APIs.

1. Ability to use wallet for all payments including person to person, person to entity, and entity to person.
2. Ability to use wallet to "pay" someone (push) as well as "collect" from someone (pull).
3. Ability to pay and collect using "virtual payment addresses" that are "aliases" to crypto address.
4. Ability for sending collect requests to others (person to person or entity to person)
5. Ability to pre-authorize multiple recurring payments(utilities, school fees, subscriptions, etc.) with a one-time secure authentication and rule based access.
6. Ability for all payment system players to use a standard set of APIs for any-to-any push and pull payments.
7. Ability to make payments using 1-click 2-factor authentication all using just a wallet on phone or PC without having any acquiring devices or having any physical tokens.

Payment Address

Every payment transaction must have source (payer) account details (for debit) and destination (payee) account details (for credit). At the end, before the transaction can be completed, these must be resolved to an actual crypto address. “Payment Address" is an abstract form to represent a handle that uniquely identify an account details in a “normalized" notation. In this architecture, all payment addresses are denoted as

“account@provider" form. Address translation may happen at provider/gateway level.

Examples of normalized payment addresses are:

Bitcoin : - bharath@bitcoin or bharath@btc

Tron :- bharath@tron or bharath@trx

Authentication

Authentication is typically done at the account provider domain. Authentication schemes separately evolved as new payment channels evolved. While numeric or alpha-numeric PIN/Passwords is the dominant authentication factor, different PINs were issued for different channels (Internet PIN, ATM PIN, Mobile PIN, etc.). In addition, OTP based authentication is used heavily these days to offer 2-FA authentication schemes.

LIME Wallet interface provides significant advantage from current systems to take crypto payments to next level. Its value lies in using customer’s mobile phone as the primary device for all authentication and authorization for both “Direct Pay” (push) and “Collect Pay” (pull) transactions.

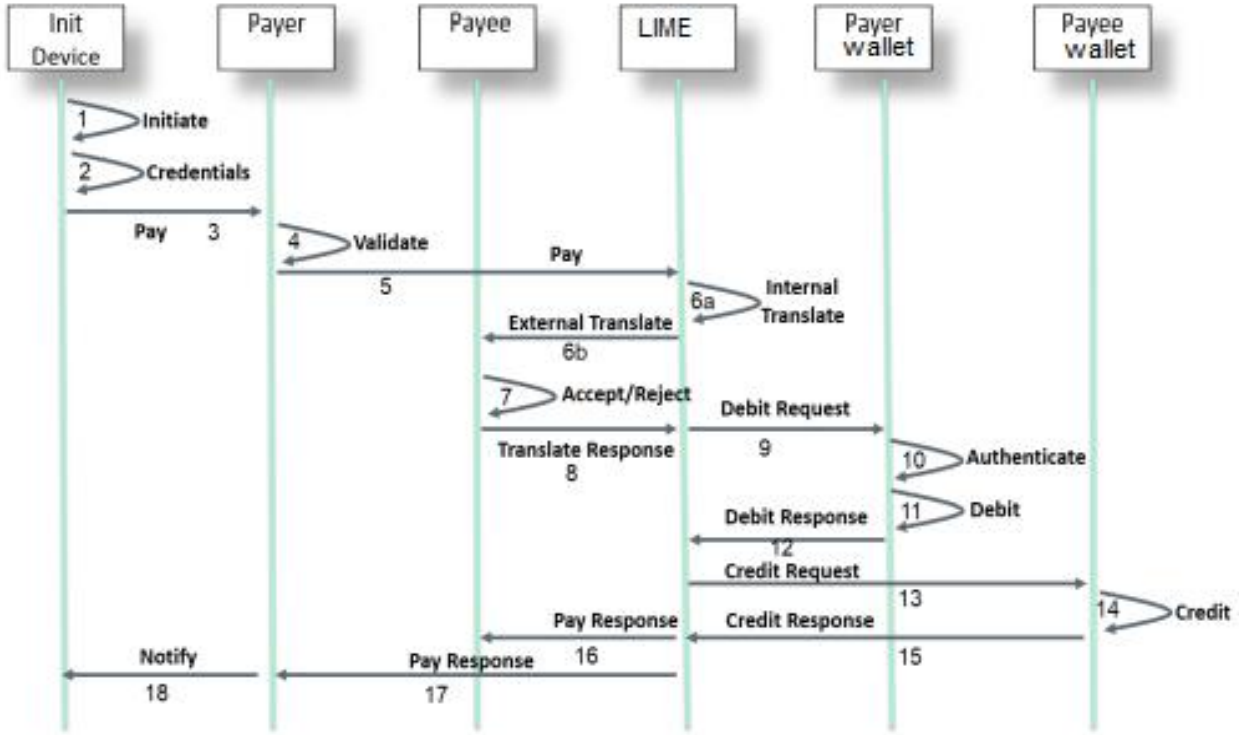
Direct Pay (Sender/Payer initiated)

- Person Initiated

Sender uses an application to send money to a receiver by providing sender credentials and receiver/beneficiary “address”.

- System Initiated

“Sender system” (a software application) is initiating payment a digitally signed request is used.



- Transaction Flow

1. Payer initiates transaction through application at his Device.
2. Payer provides authentication credentials at his Device.
3. The Payer Device initiates the Pay request to Payer system.
4. Payer validates the Payer details and validates the first factor authentication.
5. Payer PSP sends the pay request to LIME Mapper.
6. LIME Network resolves the Payee Address if the Address has global identifiers then the Payee Address is resolved by LIME central Mapper

   a. If the Address has global identifiers then the Payee Address is resolved by LIME central Mapper.
   b. If the Address has virtual address offered by Payee's wallet, then LIME Mapper will send the request to Payee's wallet for address translation.

7. In case of 6b, the Payee accepts or rejects the request based on the rules set at his end.
8. In case of 6b, on accepting the Pay request, Payee populates the Payee details and responds to LIME Mapper.
9. LIME Mapper sends the debit request to the debit account provider.
10. Account provider authenticates the Payer based on the credential provided.
11. Account provider debits the Payer account

12. Account provider sends Debit response to LIME Mapper.
13. LIME Mapper sends the Credit request to the credit account provider.
14. Wallet provider credits the account based on the Payee details.
15. Wallet provider sends Credit response to LIME Mapper.
16. LIME Mapper sends Pay response to Payee wallet.
17. LIME Mapper sends pay response to Payer wallet.
18. Payer wallet notifies payer.

Collect Pay (Receiver/Payee Initiated)

Local Collect

Paying a company using PoS/mobile application.

Payer's smartphone captures the payee payment address, transaction reference, from PoS (QRCode, etc.)

a. Allows payee to authorize and capture payee's payment information including credentials (eliminates any credential entry on external apps)
b. Payee's smartphone transfers the data securely to PoS which then carries out the transaction.

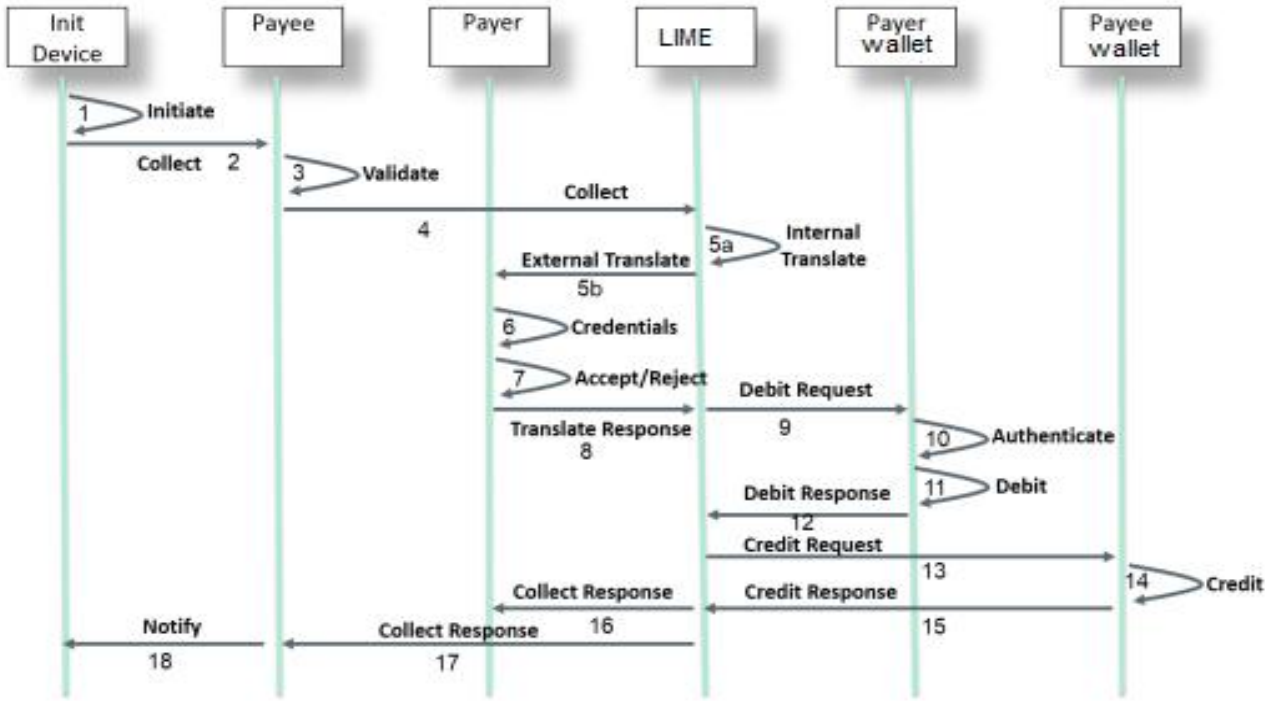
Remote Collect

Payee/Receiver (persons or entities) triggers the request without capturing sender credentials.

a. Uses a PC or Smartphone to do push authorization on sender.
b. Eliminates any credential entry on external apps
c. Allows single click one or two factor (mobile + PIN, mobile + biometrics, etc.) on a "trusted application"
d. Sender's phone becomes secure terminal for credential entry, wallet.

Examples

a. Store person uses his/her phone app to "collect" by entering customer virtual address.
b. Car service agency application "collecting" payment via virtual address without car owner having to go to collect car
c. Magazine subscription application requesting authorization for subscription renewal.



Transaction Flow

1. Payee initiates transaction through his application at his Device.
2. The Payee Device initiates the Collect request to Payee system.
3. Payee validates the Payee details and validates the first factor authentication.
4. Payee sends the Collect request to LIME Mapper.
5. LIME Mapper resolves the Payer Address in the following two ways

   If the Address has global identifiers then the PayerAddress is resolved by LIME Mapper.

   If the Address has virtual address offered by Payer, then LIME Mapperwill send the request to Payer's for address translation.

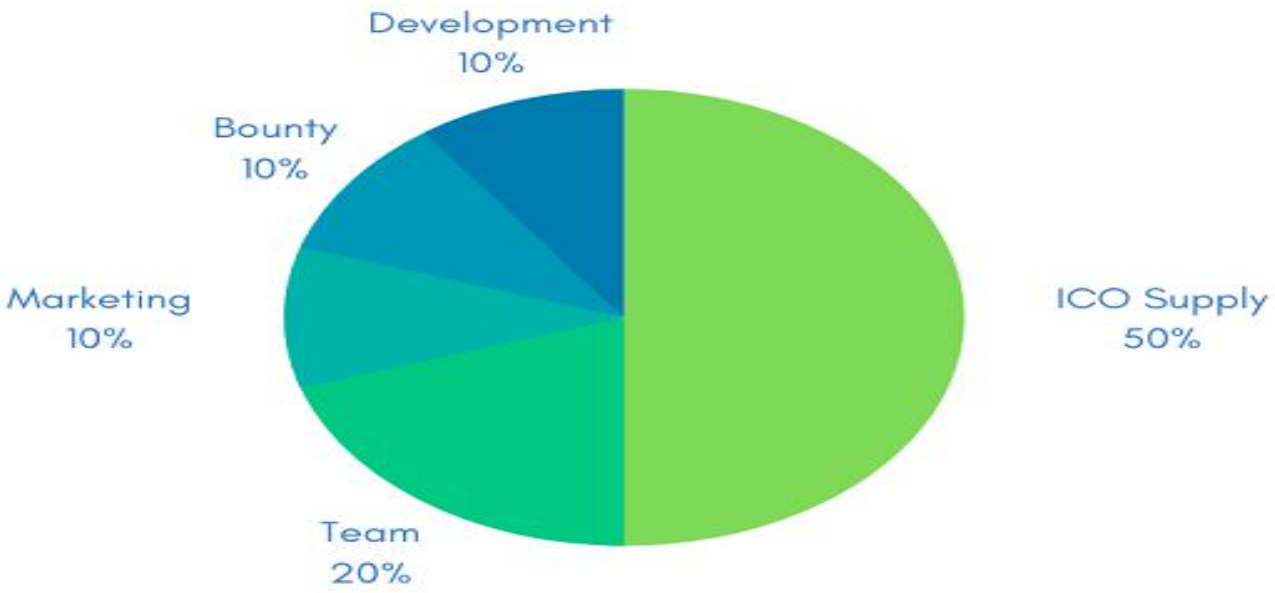
6. In case of 5b, The Payer accepts or rejects the request based on the rules set at his end.
7. In case of 5b, on accepting the Collect request, Payer initiates a request to Payer device to enter his authentication credentials. Payer provides authentication credentials at his Device.
8. In case of 5b, The Payer populates the Payer details and responds to LIME Mapper.
9. LIME Mapper sends the debit request to the debit account provider.

10. Account provider authenticates the Payer based on the credential provided.
11. Account provider debits the Payer account.
12. Account provider sends Debit response to LIME Mapper.
13. LIME Mapper sends the Credit request to the credit account provider.
14. Account provider credits the account based on the Payee details
15. Account provider sends Credit response to LIME Mapper.
16. LIME Mapper sends Pay response to Payer.
17. LIME Mapper sends pay response to Payee .
18. Payee Wallet notifies payer.

Token Information

- Name : LIME
- Type : Tron TRC20
- Price : 0.1 TRX
- Total Tokens : 1,000,000,000

Token Allocation



LIME Token Use Cases

- LIME token is required to create virtual address in LIME Wallet.For every virtual address created some amounts of LIME token will be burned.We are not extending supply of LIME.
- LIME Payment Gateway supports LIME Merchant Payment.
- LIME token is used to pay the fees in upcoming exchange project.
- LIME holders supports airdrop of partner projects.
