



Katerium - The first private
communication and payment
blockchain platform

Abstract: Katerium is an anonymous communication and payments platform which uses the blockchain technology having a network of about thousands of computers across the world. It runs on top of the internet and keeps the identity of the user anonymous and allows the user to communicate, make payments, have private groups, enable fund raising using a single application. Katerium is guaranteed to run with 100% uptime, ensures the identity of the users being kept anonymous, secure from Fraudsters on payment. It allows users to collaborate over for fund raising for a specific purpose. Katerium allows us to do the transaction through the Meta Mask browser plugin instead of downloading app and doing the transaction.

Introduction

Katerium uses blockchain technology and as with any other technology the blockchain is also going through a hype cycle – a term coined by Gartner to reflect the cycle of new technology from the technology trigger, inflated expectations, the slope of disappointment, the hope of raising again and going to a productivity plateau. However, unlike other technologies the blockchain is here to stay with us as it creates immutable transactions helping possible future landowner, future transactions on any commodity, impacting the complete cycle of supply chain for an industry. While Bitcoin or Ethereum are applications using blockchain the ability to innovate using blockchain will help to make business outcomes better. Block chain brings in a new trust factor in business. The business of trust had been so far outsourced to players like Banks, Financial Institutions, Private players and this technology has enabled complete decentralization of trust. Trust of data is the central to blockchain technology.

The problem Katerium is solving to keep the identity of the users anonymous while communicating or making payments or raising funds. It allows the decentralized applications to be built around the areas. To start with let us take the area of communication. Today's communication happens through multiple applications and majority of them happens through mobile using WhatsApp, Telegram and Messenger. Majority of the instant messaging traffic goes thru these messengers and the messages are crypted while getting transferred from the time they leave your mobile. However, the user identity is not kept anonymous. We cannot send anonymous messages to the users during the need and the reason being it is used from possibly a mobile where your location, identity is compromised at least with few players that includes application vendors and telecom operators.

Katerium enables you to communicate without registering a phone no or IP on your device. All your calls and messages will be untraceable through thousands of servers and encrypted all the way. The most secure bank today in the world is blockchain and Katerium enables you to make or receive payments anonymously. It enables you to be an anonymous account holder of a bank controlled by you and enabling you to make or receive payments. The entire set of transactions are enabled digitally using an android or IOS mobile applications. Let us say a fund raising needs to be done for a specific purpose and the fund raisers names must be kept anonymous. Payments into the bank controlled by you can be made anonymously and can be made from your bank anonymously as well. Katerium helps you to communicate using your existing apps like WhatsApp or Telegram. The anonymous payment capability or ability to receive payments through instant messaging application further empowers individuals to create new lines of business.

A private anonymous which was hitherto possible only when you deposit money into swiss banks is now made possible using the Katerium technology to all the users across the world and the payments made to a bank through Katerium will be completely protected.

1. Why Katerium Platform

- a) **Decentralized Approach:** Blockchain itself uses decentralized approach where a network of computers across the world stores all the messages using the Katerium messaging app. This avoids the messages being modified by an authority. The current messenger uses a platform-based approach and is centralized.
- b) **Immutability of Blockchain:** All blockchains are immutable in nature and therefore information once written cannot be changed. This helps in solving commercial disputes.
- c) **Anonymous:** The core value of the Katerium based instant messaging app is the anonymity of the users. Katerium signs off on keeping the location, IP address, other user attributes anonymous and ensures the same is not violated at any given time.
- d) **Privacy:** Katerium blockchain instant messaging is secure end to end through the right encryption algorithms and by the way of allowing the right authorization and authentication to access the messages.
- e) **Security:** Katerium avoids the MITM (Man in the Middle) attacks by the way of decentralization and automation of the entire chain of instant messaging from one person to another person.
- f) **Censorship Avoidance:** The content does not pose Censorship risks as it is decentralized, and the content cannot be removed without consensus. This avoids surveillance of the Government as well as any regulatory organizations.

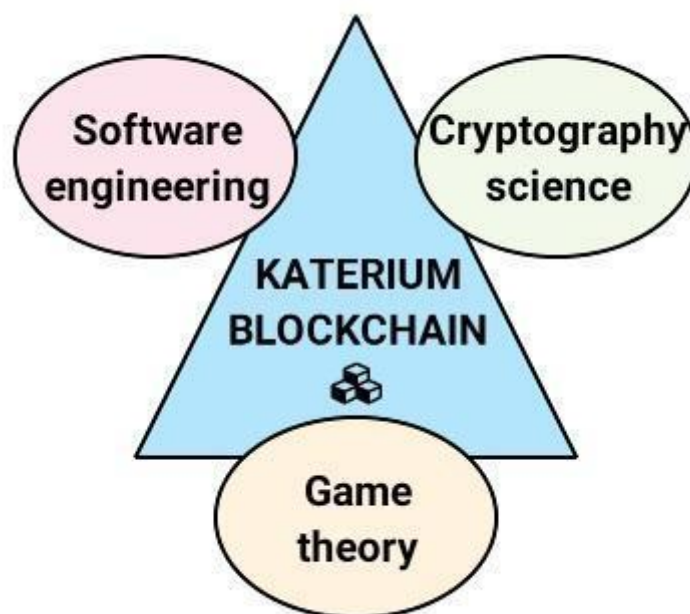
2. What is Katerium Platform

The basic philosophy behind Katerium is the value chain without intermediaries using the blockchain technology by the way of decentralization of trust. Katerium brings in the intersection of three different fields namely Software Engineering, Game Theory and Cryptographic Science. These three fields have existed together separately and with the introduction of blockchain they would tend to work harmoniously.

Game Theory involves the study of mathematical models that involves conflicts and cooperation between different parties involved in a transaction. The Blockchain technology when conceived uses the Byzantine general problem. In the Byzantine general problem there are multiple divisions of army outside a city and each division commanded by the general. All Generals can communicate using the messenger only and they must reach an agreement using the messenger. There could be traitor generals who will try and disrupt the plan. Therefore, the issue will be to ensure that the generals solve the problem of taking over the city by using the messenger. This solves the network security issue in the distributed network of nodes where data is stored. Katerium uses a proprietary protocol to solve this issue in the blockchain to come to a consensus.

Cryptographic Science enables the secure blockchain by usage of hashing, keys and digital signatures along the network to provide the security needed for an end to end transaction. Katerium uses encryption across the network to deliver the outcome

Software Engineering Constructs involving the cryptographic science and game theory uses applications to deliver secure use cases without dependency on a centralized trust engine. Katerium has built its application over a trusted game theory and cryptographic science to deliver its use cases.



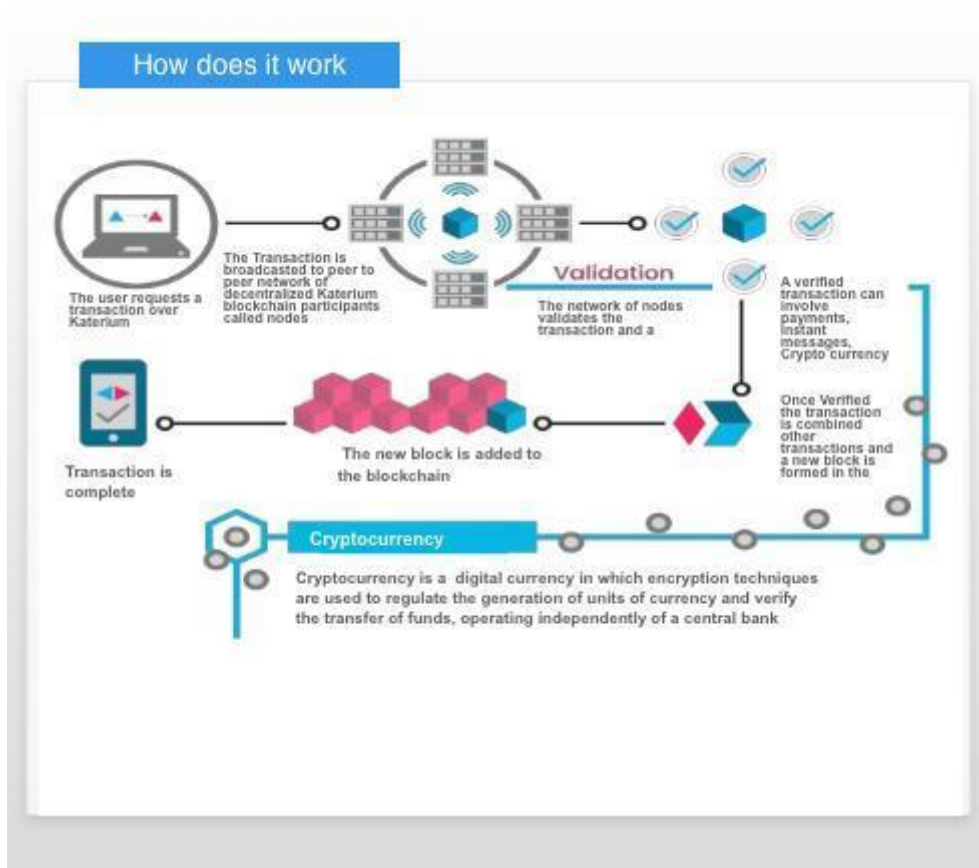
Like any other blockchain product Katerium has the blockchain properties of cryptocurrency, secure distributed ledgers, computing infrastructure, Transparent Transactions and Trust Services Layer. Katerium uses the cryptocurrency KTH based on ERC-20 standard as defined in <https://www.investinblockchain.com/what-are-ethereum-tokens/>

3. [How Katerium Platform works](#)

Katerium is a blockchain platform that enables the instant messaging, anonymous payments, anonymous fund raising etc. As in any other blockchain platform Katerium has nodes, miners, network consensus, proof of work, network consensus, double spending issues etc.

Let us see how Katerium works as a platform. Assume that someone wants to send a message to another person or a group. Katerium can be used from browser by downloading a meta mask plugin available in <http://katerium.com>. The plugin opens the application from the browser and the first step the user has to do is to buy some KTH token to complete the transactions.

Let us understand how Katerium as a platform works. Let us say how a user wants to create a transaction. The transaction could be as simple as sending an instant message, sending a payment anonymously to an individual or a fund raiser. The requested transaction will be sent to a network of computers using peer to peer network across the world. These computers are called nodes in a blockchain transaction. The network of computers validates the user's transaction using an algorithm. The verification can involve transaction regarding the cryptocurrency, the sender and the receiver information being validated. Once the transaction is verified a new block of transaction is created for the ledger. This new block is added to all the network nodes and a blockchain is formed. The transaction is then declared as completed.



4. Katerium Use cases:

To understand the blockchain transaction let us try and see how a simple transaction works in a bank and how a blockchain transaction will work. We will go thru three methodologies. A banking transaction that works currently, how a blockchain transaction usually works and how a Katerium transaction works. This will help us to differentiate between Katerium and other transaction.

4A. Normal banking Transaction

Let us say Jim wants to transfer money to John say \$5000. Jim logs into his banking apps (Bank of Mars) in the mobile and identifies John who is holding an account in another Bank (Bank of Venus). John transfers money from his checking account to Johns checking account after getting the account no from John. In the backend the following things happen. Jim initiates transaction. The banking software verifies Jim's account on the balance and updates the new money in a temporary database. The application sends a message to the Johns Bank about Jim's intention to transfer \$5000 and there is a handshake that happens between them. John's account gets added (credited) with \$5000 and Jim's account gets subtracted (debited) with \$5000. Transaction is complete. There are two ledgers that gets updated one in the Bank of Mars and Another in the Bank of Venus. There is a coordination that happens in the bank and the entire control is centralized with both the banks.

Current banking transaction methodology

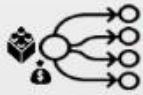


01

Jim logs into his banking apps (Bank of Mars) in the mobile and identifies John who is holding an account in another Bank (Bank of Venus)

John transfers money from his checking account to Johns checking account after getting the account no from John. In the backend the following things happen. Jim initiates transaction.

02



03

The banking software verifies Jim's account on the balance and updates the new money in a temporary database. The application sends a message to the Johns Bank about Jim's intention to transfer \$5000 and there is a handshake that happens between them

John's account gets added (credited) with \$5000 and Jim's account gets subtracted (debited) with \$5000. Transaction is complete.

04

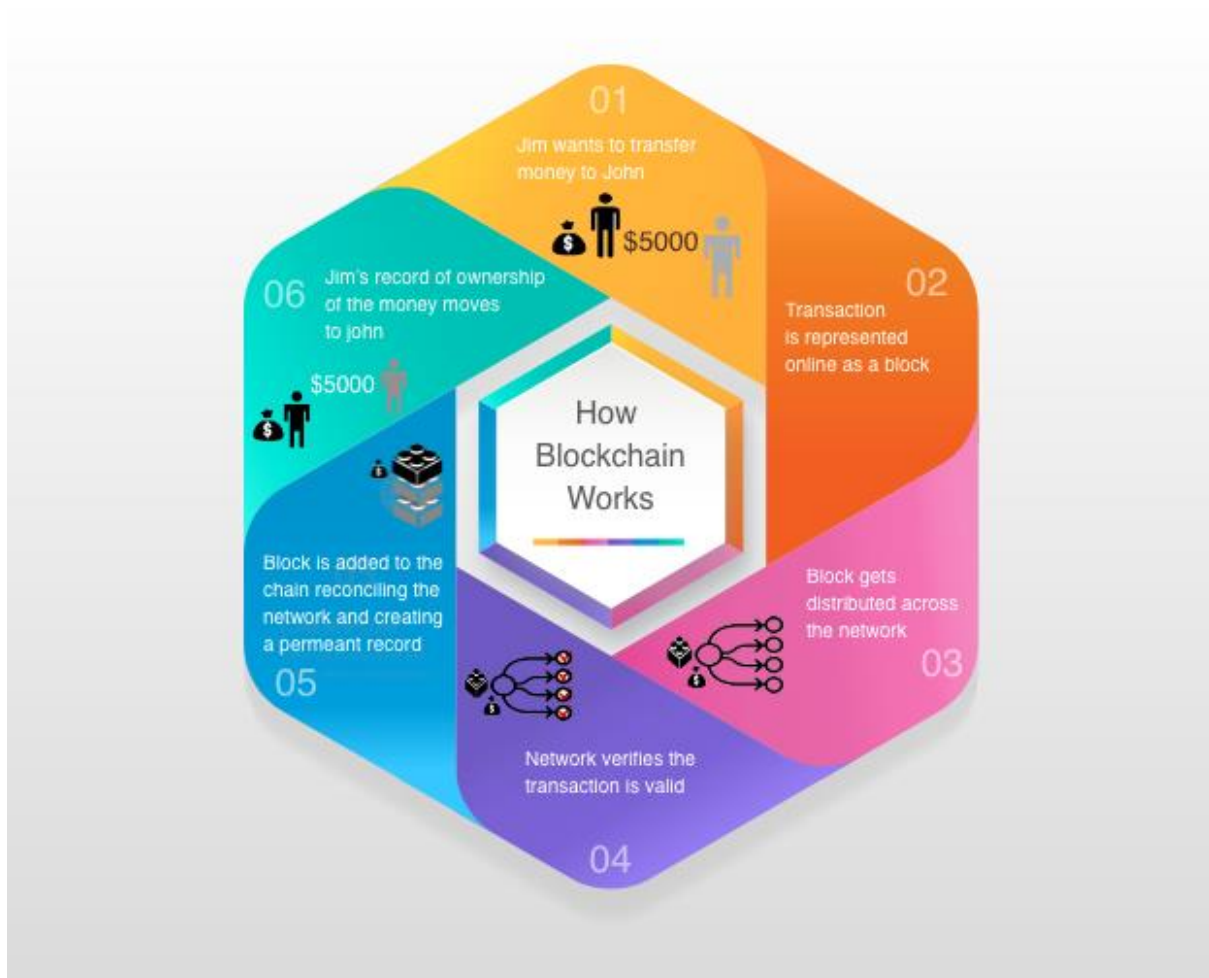


05

There are two ledgers that gets updated one in the Bank of Mars and Another in the Bank of Venus. There is a coordination that happens in the bank and the entire control is centralized with both the banks.

4B Normal Blockchain Transaction

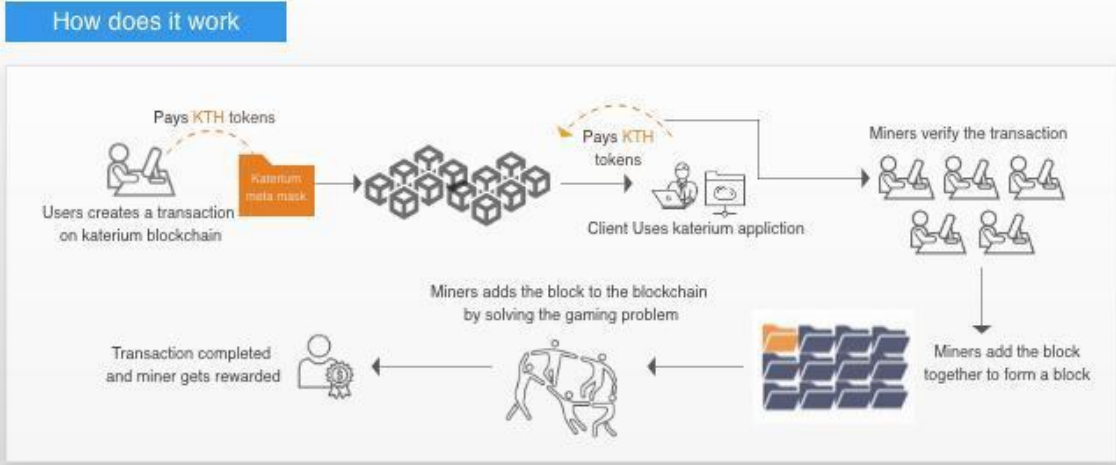
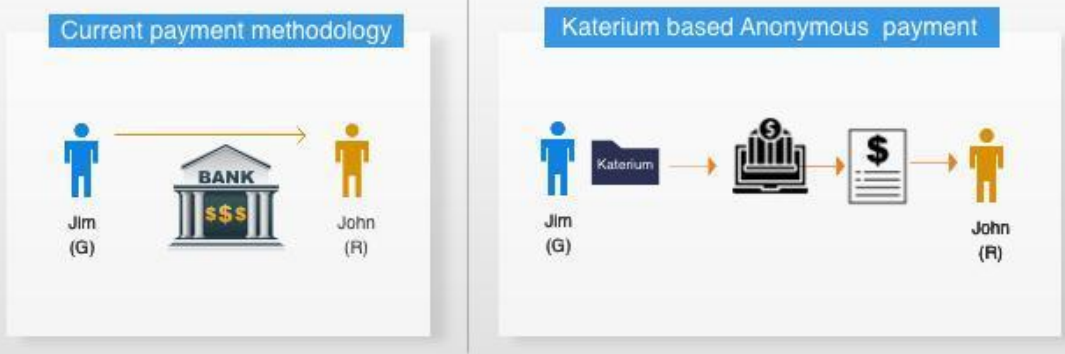
Let us look at the above transaction using Blockchain. Jim wants to transfer money to John say \$5000. This transaction is represented online as a block. The block gets distributed across the network. The network verifies that the transaction is valid. The block is added to the network reconciling across the network creating a permanent record. Jim's money moves to John as the permanent record of the transaction is created.



The transaction helps us to achieve the following

- Autonomy:** It does not have the interference from the third party as the entire transaction is carried out without the help from the banks. This leads to reduction in costs of transaction.
- Transparency:** The documents are encrypted, and it is available over the public ledger which can be seen by people who are authorized to see the transaction.

- c) **Backup:** The transaction is recorded on a network of computers and therefore a single point of failure is completely avoided. This entire transaction is very transparent.
- d) **Savings:** There is no transaction cost to the banks/any third party involved.
- e) **Reduction in Errors:** Chances of errors are minimum.



4C. Katerium based Anonymous Blockchain Transaction for a website

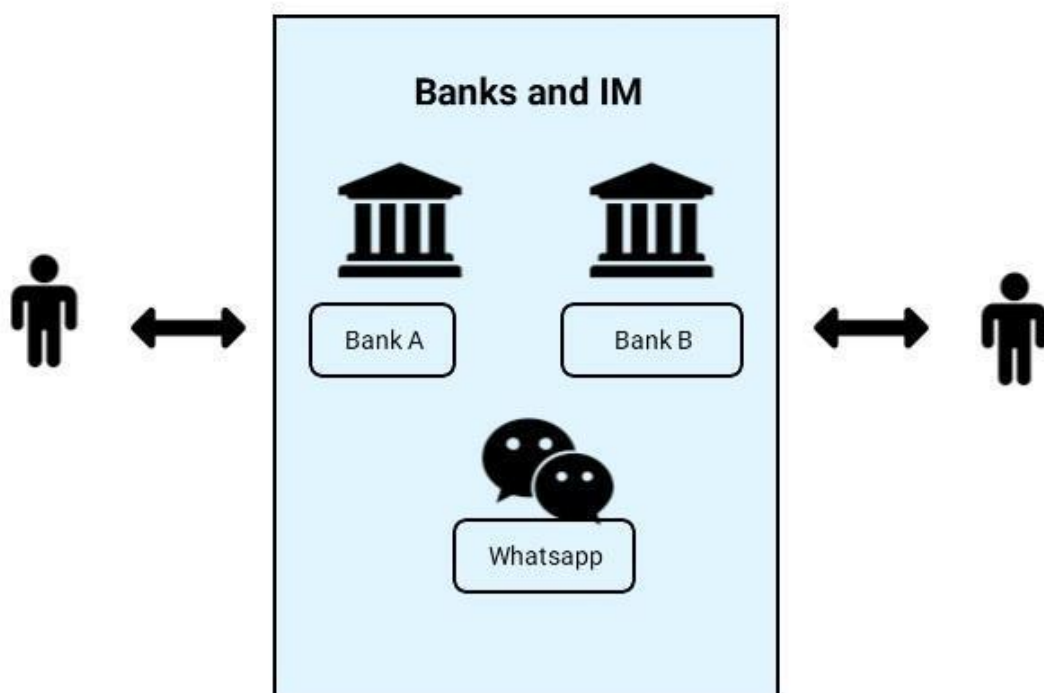
Mike wants to do some online shopping using the instant messenger. There are two examples that are explained below. One of them uses using the regular chat like WhatsApp or Telegram or any chat of the website and another uses Katerium based instant messaging system.

1. The buyer (Mike) and seller (John) agree on the terms and conditions of sale, return policy and on which account the payment is be made.

- Mike will chat with the seller through an Instant messaging platform such as WhatsApp. As third party apps are prone to advertising and manipulate personal data privacy and security become compromised. It introduces a dependency on the third-party app and the entire history of the chat is kept in the platform of the third party apart from the user systems.

Mike will make a payment to john through the bank as the mode of payment is online and most probably a credit card or a debit card will be used as part of the transaction.

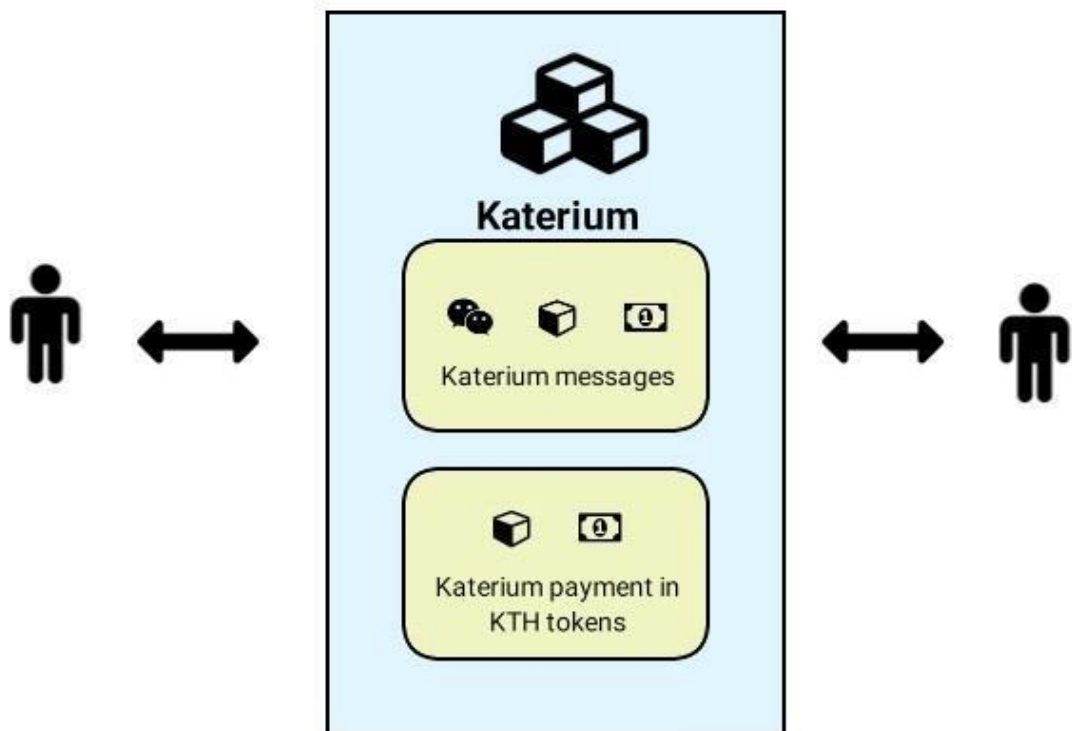
- This would involve maintaining accounts in bank and transferring it manually through the bank's website. The bank may charge a merchant fee and probably the seller could be charged the Merchant fee. This entire transaction is recorded in a platform where the buyer and seller are connected.



1. Katerium based transaction for an online website

In this transaction bank and the chat service provider are eliminated and are implemented through the blockchain system via the Katerium application.

- The transactions involved in the sale process agreement are made through the Katerium app. This involves spending KTH. This gives privacy and security as the blockchain is encrypted. The transaction is autonomous, and the entire transaction is immutable and will help at the time of any possible dispute.
- The payment is also done in the same manner using KTH through the Katerium app. This takes advantage of blockchain therefore no bank is involved. The transaction is anonymous, secure and decentralized.



Katerium Blockchain based instant messaging

One of the major concerns of people had been the safety of personal data with various social network platforms. This is specifically in the wake of Face – Cambridge Analytica scandal where there is an alleged personal data compromise had happened. This has led to the growth of more decentralized social network platforms. The decentralized chat uses Peer 2 Peer Protocol for instant messaging and transfer of photos. If we look at the current technologies being deployed it is a central platform and consumers and producers of data in social network communicate over the platform. The data is stored in a central platform leaving the platform vendor to possibly monopolize the data and earn money from the data by positioning right advertisements.

Katerium blockchain app comes with a KTH crypto currency wallet and has its own platform like Ethereum. It enables users to send text, videos and audios apart from making payments using the blockchain as explained the previous chapter. Most of the instant messaging apps in the website uses WhatsApp, Viber etc. The disadvantage of these apps is that the entire transaction is stored in the platform and most of the time the messages are deleted after the transaction is over. The Katerium based instant messaging app can be used so that the history of the transaction is completely stored. It uses the property of the blockchain where every transaction is immutable. These immutable transactions help to resolve the disputes involving commerce quickly.

Katerium instant messaging includes the following Features.

- a) Available in all the countries
- b) Voice call using internet
- c) Video calling
- d) Anonymous Fund Transfers
- e) Conference calling
- f) Group Messaging
- g) Make Payments and Trade Money

5. Conclusion

Katerium is a messaging app combined with cryptocurrency (KTH) wallet. Messaging apps with the blockchain infrastructure have taken few steps ahead of centralized apps like WhatsApp by allowing users trade money and make payments using the cryptocurrency. Hitherto Cash has been the only way of doing an anonymous transaction. Combination of Blockchain wallet with the messaging apps makes the anonymous payments a possibility. This has brought in the convenience of making anonymous payments using cryptocurrency wallets. This also takes away the surveillance imposed by the Governments and other organizations on any transaction involving money transfer. Many countries have political

sanctions where some of them cannot use credit cards like Mastercard and visa platforms and therefore these countries will take advantage of cryptocurrency transactions. The usage of Cryptocurrency may become a matter of acceptance by the Federal banks in the countries which controls the money supply in a country. In a blockchain the concept of double payment can be avoided. However, this becomes a possibility only with the crypto currencies. Usage of Conventional currency may still lead to double payment and therefore this can make the cryptocurrency more popular.

There are more uses for blockchain based messaging apps. In the current messaging apps says WhatsApp or Instagram there is no money paid for a valuable content. Chances of receiving payment for a valuable content is high using blockchain messaging apps. One of the use cases which the Katerium messaging app enables is the fundraising in an anonymous manner.

Fundraising requires a team and it could be an institutional fund raising or individual fund raising. This has been facilitated by the blockchain technique. One of the requirements of Fundraising is an outreach. The outreach can be made easier using an anonymous messaging app which uses blockchain infrastructure.