MATRIX WHITEPAPER

EXECUTIVE SUMMARY

The use of matrix makes it possible for everyone to enjoy fast and secure transactions without experiencing the limitations associated with other cryptocurrencies. More so, the platform is open for everyone to be part of the mining process and having a PC and one or more graphics card makes the mining process a breeze.

EFFICIENT AND FAST
TRANSACTIONS USING
MATRIX COIN

TABLE OF CONTENTS

INTRODUCTION

The growth of cryptocurrency in the last decade is amazing, moving from obscurity to a place of dominance, and more changes are expected in the technological and financial landscape from the use of cryptocurrency. The use of cryptography by cryptocurrencies has made it possible to enhance the security of transactions with good regulation of the development of any additional currency unit.

The introduction of Matrix comes with additional benefit to the use of cryptocurrency, users will enjoy fast transaction process that is not obtainable with other cryptocurrencies.

The era of cyptocurrency has played an immense role in the digital currency landscape. The new technological innovation experienced with the use of cyptocurrency is great. Cryptocurrency is developed with the help of blockchain technology and it acts as a distributed ledger with several benefits that include; fast transaction timing, privacy, enhanced security and borderless transaction.

Bitcoin is the first cyptocurrency and it provides a good means of carrying out commerce effectively just like many other cryptocurrencies. The introduction of Bitcoin has led to the development of several other cryptocurrencies that provide their own unique services such as Matrix coin.

Impact of ledger technology

Ledger technology is responsible for the spreading of digital data across several countries and multiple sites. Blockchain is an early adopter of ledger technology, and there is an increasing level of awareness about the potential benefits of blockchain technology, because both governmental

and financial institutions have come to realize the importance of blockchain technology as a result of its high-level security.

NO MORE DARK AND SLOW TRANSACTION
PROCESSING MATRIX PROVIDES
AN ENLIGHTENED MEANS
OF ENJOYING SWIFT TRANSACTIONS

BLOCKCHAIN

Blockchain is best defined as a database that makes it possible to create digital ledgers and also send the available information of transactions to several computer networks. The means through which Blockchain functions is explained in its ability to develop a cryptograph of its algorithm and enable a user to customize the details in ledger form without asking for permission from any central registry.

The advantages of working with blockchain technology include the following;

Reliability

The intrusion of corrupt and foreign attacks can be stopped with the use of blockchain. Blockchain is secure because it is not prone to central point of failure. Blockchain technology is developed to prevent attacks that can affect an entire system.

Trustless exchange

A transaction can be executed on blockchain without the inclusion of a third party. The essence of its use as a trustless exchange enables users to carryout transactions without incorporating escrows or third party services that may be expensive to employ.

Empowered users

Blockchain has made it possible for users to be free from strict financial and governmental restrictions. Blockchain has a level of social freedom that is unmatched with fiat money. The use of blockchain enables users to have full control of their currency and utilize it for any purpose of their choice.

The transactions that are carried out on blockchain are immutable. When a change is made to transactions, the parties involved will all get a notification about changes in the transaction. The aim of sharing details about any change in a transaction is purely to make every transaction transparent. Ensuring that all parties involved in a transaction can perfectly boast of their knowledge of every process and every change in transaction details.

BITCOIN

Bitcoin has attracted a large number of users and that can be attributed to its position as the first cyptocurrency to be developed. The development of Bitcoin by Satoshi Nakamoto paved the way for the introduction of other cyptocurrency just as we presently have Matrix. Bitcoin adoption has grown in many areas since its inception in 2009, and since then, more innovations are introduced to handle the limitation faced with Bitcoin. A major challenge with Bitcoin is the wait time for network confirmation of all transactions carried at point-of-sale (POS). Payment processors try to remedy the situation by creating methods that allow vendors to receive zero-confirmation for transactions, but the process requires the use of a reliable counterparty to mediate transactions outside the protocol.

The pseudonymous transactions that Bitcoin is known for is provided in a pubic ledger and it has one-to-one relationship with the sender and receiver. This means there is a permanent record of every transaction performed on the network.

This paper proposes series of improvements to the limitations of Bitcoin thereby providing instant transactions that are anonymous with proof of work reward, masternodes and a secured mining process that prevents mining attacks.

MASTERNODE NETWORK

These are servers running on a peer to peer network that enables peers to utilize them in receiving updates about the changes taking place in a network. These nodes make use of a huge amount of traffic and other resources that are expensive to maintain. Which has led to a reduction in the number of these nodes on Bitcoin network. Thereby leading to an increase in block propagation times which has reached 40 seconds and above.

Since these nodes are vital to a healthy network and enable clients to facilitate and synchronize propagation of information throughout the network. The nodes will then provide availability and a specific level of work for it to be part of a reward program.

MASTERNODE PROTOCOL

Masternodes are propagated in the network with the use of protocol extensions that includes masternode announcement and masternode ping message. The two messages help to create an active node for the network, aside these, other messages needed to execute proof-of-work request include; InstantSend and PrivateSend.

The masternodes are created by forwarding 10,000 Matrix to a certain wallet address M (ex. B1VGAD6ASDA8A90), which will then activate the node that will enable it to be propagated throughout the network. The creation of a secondary private key is also carried out to sign all subsequent messages. When running on standalone mode, the use of a latter key enables the wallet to be fully locked.

The use of trustless quorums can also involve using masternode networks as decentralized oracle for a financial market and ensuring that secure decentralized contracts is a possibility.

PROPAGATION OF MASTERNODE LIST

For new clients on Matrix network, they must acquaint themselves with the current active masternodees available on the network, and once that is done, it becomes easy for them to utilize the services. Once new clients, join the network. A command will be sent to their peers requesting for a list of masternodes. The use of a cache object makes it possible to record details of masternodes and their present status, and as clients do a restart, they will load the file that contains the recent status of masternodes rather than getting a full list of all masternodes.

MATRIX REWARD PROGRAM, PAYMENTS AND COST

The lack of incentive to run a node is considered to be the reason behind the decrease of full nodes. As the cost of running a full node increases with time due to increased usage, more bandwidth will be created, which will cost more money. Once that happens, operators will be forced to run a light client or consolidate their services. Masternodes have several nodes and will provide an acceptable level of service for the network with a bond of collateral for participation. The collateral is safe as long as the masternode is operating. This enables masternode operators to give service to the network and earn payment for all the service rendered and also reduce the currency volatility.

A masternode is run when an operator demonstrates control over ten thousand Matrix. When masternodes are active, they give services to the client on the network and receive their payment from block reward. Masternodes get their payment from block reward, and they receive 100 % from block reward.

The formular for calculating the daily payment required in running a masternode is given below;

(n/b)*b*a*r

Where

n is the masternodes controlled by an operator

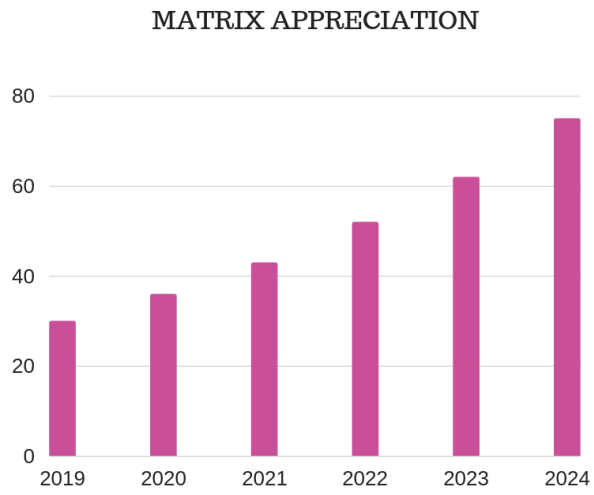
t is the complete number of masternodes

b is the blocks available on an average day

a is average masternode payment

A soft and hard limit of active nodes is created by running a masternode. The price it takes to get a node creates a soft limit.

The graph below shows the approximated level of appreciation for Matrix coin in hundreds of million.



DETERMINISTIC ORDERING

There is a special deterministic algorithm that helps to develop pseudo-random ordering for masternodes. The use of hash from proof-of-work associated with each block ensures high security via the mining network.

Selecting a masternode has a pseudocode as shown below;

```
For(mastenode in masternodes){
    current_score = masternode. CalculateScore();
    if(current_score > best_score){
        best_score = current_score;
        winning_node = masternode;
    }
}
CMasterNode::CalculateScore(){
   pow_hash = GetProofOfWorkHash(nBlockHeight); // get the hash of this block
   pow_hash_hash = Hash(pow_hash); //hash the POW hash to increase the entropy
   difference = abs(pow_hash_hash - masternode_vin);
   return difference;
}
```

Furthermore, same code can be extended to provide further rankings of the masternodes.

PAYMENTS THROUGH MINING

Blocks must pay the right masternode for work done and the payment will be a fair share of the accumulated block reward. To prevent any form of cheating, all miners must stick with the required mining regulation else their blocks will be rejected.

PRIVATE SEND

The reference client that ensures a high level of privacy should have a trustless implementation for enhancing user privacy. Clients such as Android, Electrum and iOS will have same anonymity layer handled directly and will make use of the protocol extensions. This will enable users to anonymize funds and secure their privacy.

PrivateSend comes with its unique benefit as it is considered to be an improvement of CoinJoin and other improvements for Matrix include the use of chaining approach, inactive ahead-of-time mixing and denominations alongside strong anonymity that protects user's details.

Though it is challenging to improve the privacy of cyptocurrency without obscuring the whole blockchain. The use of Bitcoin based currency makes it possible to know which outputs are not spent also known as unspent transactions.

This makes it possible for users to act as guarantors of the integrity of the system using a public ledger. Bitcoin protocol makes it possible for activities to be carried out without the involvement of trusted counterparties, and users can have access to auditing capabilities with the aid of public blockchain.

The use of a decentralized mixing service makes it possible to keep the currency perfectly fungible. Fungibility which is a characteristic of money, ensures that all units of a given currency remain equal. Also, by receiving money within a certain currency, there should be no trace of the history involved with the previous transactions performed with the currency or users should have an easy means of disassociating themselves from the transactions performed using the currency thereby

keeping the coin units equal. Also, a user should have the privilege of acting as an auditor and be able to guarantee the integrity of the involved public ledger without any compromise on privacy.

DENIAL-OF-SERVICE (DOS) RESISTANCE AND PRIVACY

The use of PrivateSend is based on the fact that transactions get developed by multiple parties that seek to merge their funds together and ensure it is not coupled together. The system is well secured because PrivateSend transactions are created to pay themselves, with high security for all coins. PrivateSend mixing presently requires a minimum of three participants.

PROOF OF WORK

Masternodes can give any number of services to the network. As proof-of-concept, the implementation includes InstantSend and PrivateSend. The use of proof of work makes it possible to keep nodes online and ensure that the blocks are positioned at the correct height

Nodes must also ping the network to remain active, which provides a means of having a secured system. To checkmate the rate at which people will attempt to use the system to their own advantage, the rest of the network will receive a ping from nodes to keep them active. This is achieved by the masternode network which selects 2 quorums for every block. Quorum B checks the activity of Quorum A for each block.

The masternode network ensures that all the required work necessary to ensure that all nodes are active is properly done. The entire network will be checked about 5 times each day to ensure that the entire system is trustless, and nodes are selected randomly with the aid of the Quorum system. If violations occur at six different times, the node involved will be deactivated.

SECURITY CONSIDERATIONS

Once transactions are merged, it is easy to have a clue of user's funds as they go through the system. Which is not a major security flaw as a result of the need for masternode's to have 10,000 Matrix and users can choose to work with random masternodes that they choose to join. Probability of going through a transaction process in a chaining event can also be calculated.

Attacker Controlled Masternodes / Total Masternodes	**Depth Of The Chain**	**Probability of success** $(n/t)^r$	**MATRIX Required**
10/1010	2	9.80e-05	10,000Matrix
10/1010	4	9.60e-09	10,000 Matrix
10/1010	8	9.51e-11	10,000 Matrix
100/1100	2	8.26e-03	100,000 Matrix
100/1100	4	6.83e-05	100,000 Matrix
100/1100	8	4.66e-09	100,000 Matrix
1000/2000	2	25%	1,000,000 Matrix
1000/2000	4	6.25%	1,000,000 Matrix
1000/2000	8	0.39%	1,000,000 Matrix
2000/3000	2	44.4%	2,000,000 Matrix
2000/3000	4	19.75%	2,000,000 Matrix
2000/3000	8	3.90%	2,000,000 Matrix

The table above shows the probability of following a PrivateSend transaction if the attacker controls N Nodes

When n is used as the number of nodes used by an attacker

And t is the number of masternodes present in the network

While r is the chain depth

By considering the number of Matrix supply which is 2,000,000,000 and low liquidity, it is obvious that it is impossible to have a huge number of masternodes to succeed with an attack. Also, if the system is extended by blinding masternodes to just the transactions taking place on assigned node, it becomes easy to enhance the overall security of the system.

USE OF RELAY SYSTEM TO BLIND MASTERNODE

A simple relay system can be used by users to safeguard their identity, to get this done, single transactions can be followed through PrivateSend mixing sessions. Which can be handled by blinding masternodes so they don't see the outputs/inputs that belong to others.

Users will need to pick a random masternode and request that it conveys the outputs/inputs signatures to target mastermode. Instead of users submitting their outputs and inputs straight into the pool. This makes it possible for the masternode to receive N sets of outputs/inputs and N signature sets. The set attained will be the possession of a user while the masternode will be unaware of who owns the set after it is allocated.

InstantSend Transactions

The use of masternode quorums ensures that users can receive and send instant irreversible transactions. By forming a quorum, the transaction inputs are locked and allowed to be spent in a specific transaction. Transaction lock can take about four seconds to be fixed on the network. A consensus on a lock by masternode network, will ensure that all conflicting transactions or blocks are rejected, except there is a match with the transaction ID of the actual lock in place. The use of InstantSend makes it possible for users to utilize mobile devices for commerce, and it can be done without having a central registry.

TOKEN SALE

The matrix token will be used as the payment instrument for the platform, and the token will be available at the pre-ICO stage. Thereafter, tokens will then be purchased with the help of an exchange because Matrix will be listed in an exchange. The use of electronic payment will also be made possible for token purchases.

TOKEN DISTRIBUTION

Matrix token release has both the hard cap and the soft cap. The soft cap has a total value of 2 billion while the hard cap has a total value of 10 billion.

The premise of Matrix currency is in the occurrence of a transaction mechanism between fund managers and investors through crypto exchanges. Matrix liquidity will rise with increased demand which will also lead to a rise in its value based on constant usage.

THE USE OF X11 ALGORITHM

X11 is a popular hashing algorithm that uses a different algorithm referred to as algorithm chaining. X11 comprises of 11 SHA3 contestants. Individual hash are calculated then replaced with the next algorithm present in the chain. The use of multiple algorithms leads to a reduced likelihood of creating an ASIC.

Bitcoin lifecycle began with mining by hobbyist who used their CPU to mine currency, before a switch to Graphics Processing Units (GPUs) that replaced CPUs. After the use of GPU's, Application Specific Integrated Circuits were developed and served as a replacement to GPUs.

Chaining hashing approach has an advantage for high end CPUs because it gives a result that is similar to what is obtained with the use of GPUs. GPUs are known to run cooler than CPUs and they consume less wattage. Which indicates the need for using GPUs for Matrix mining.

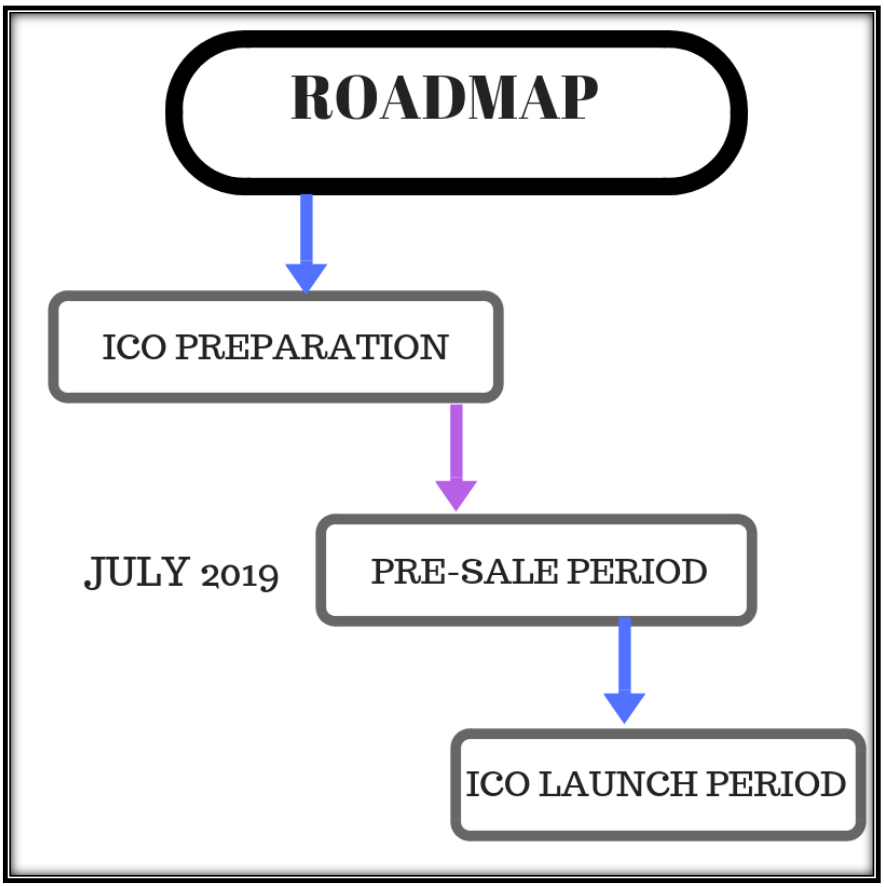
Mining Supply

The inflation of mining is curtailed by halving the supply after 150,000 blocks are mined. Matrix supply value is 10,000,000,000 while the premine value is 2,000,000,000. Production of Matrix will continue in this century and next without ceasing.

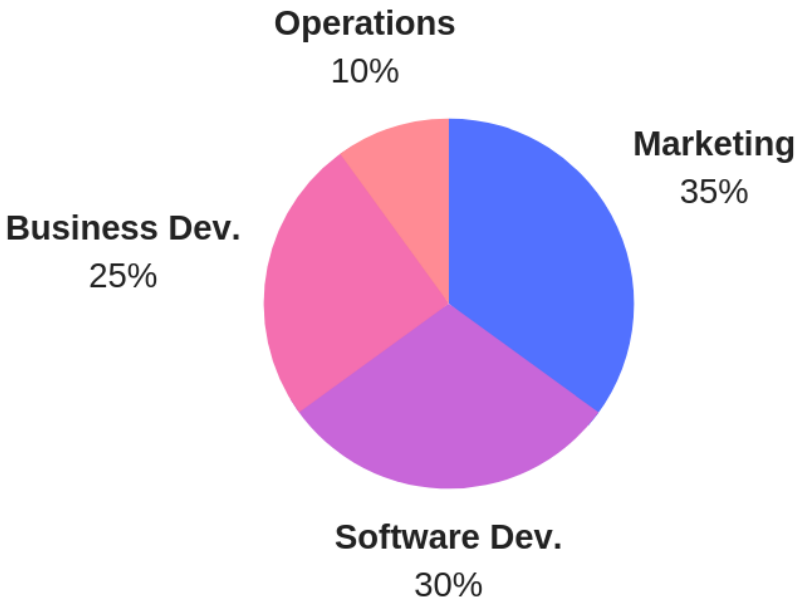
ROADMAP FOR MATRIX PRE-SALE

The pre-sale period will hold in the month of July 2019. Preparation for the pre-sale period will witness events and projects such as the development of PR articles, development of a multi-lingual response support (24x7).

The ICO launch proper timeline will witness the release of vital information on Matrix investment as well as updates on ICO.



FUNDS ALLOCATION



The right allocation of funds is important for the success of Matrix Coin, and that has led to the right allocation of funds as described below, which will ensure that the platform is able to handle all operational requirements.

Marketing 35%

An effective will go a long way in getting the needed attention for Matrix, which is the reason for the allocation of a huge amount of funds towards the marketing efforts of Matrix. The marketing will cover branding, public relations, ad campaigns, social media campaigns, newsletters and other marketing requirements.

Software development 30%

The development of Matrix is included in the software development budget. Software development covers CRM development, technical requirements, as well as API functionality.

Business development 25%

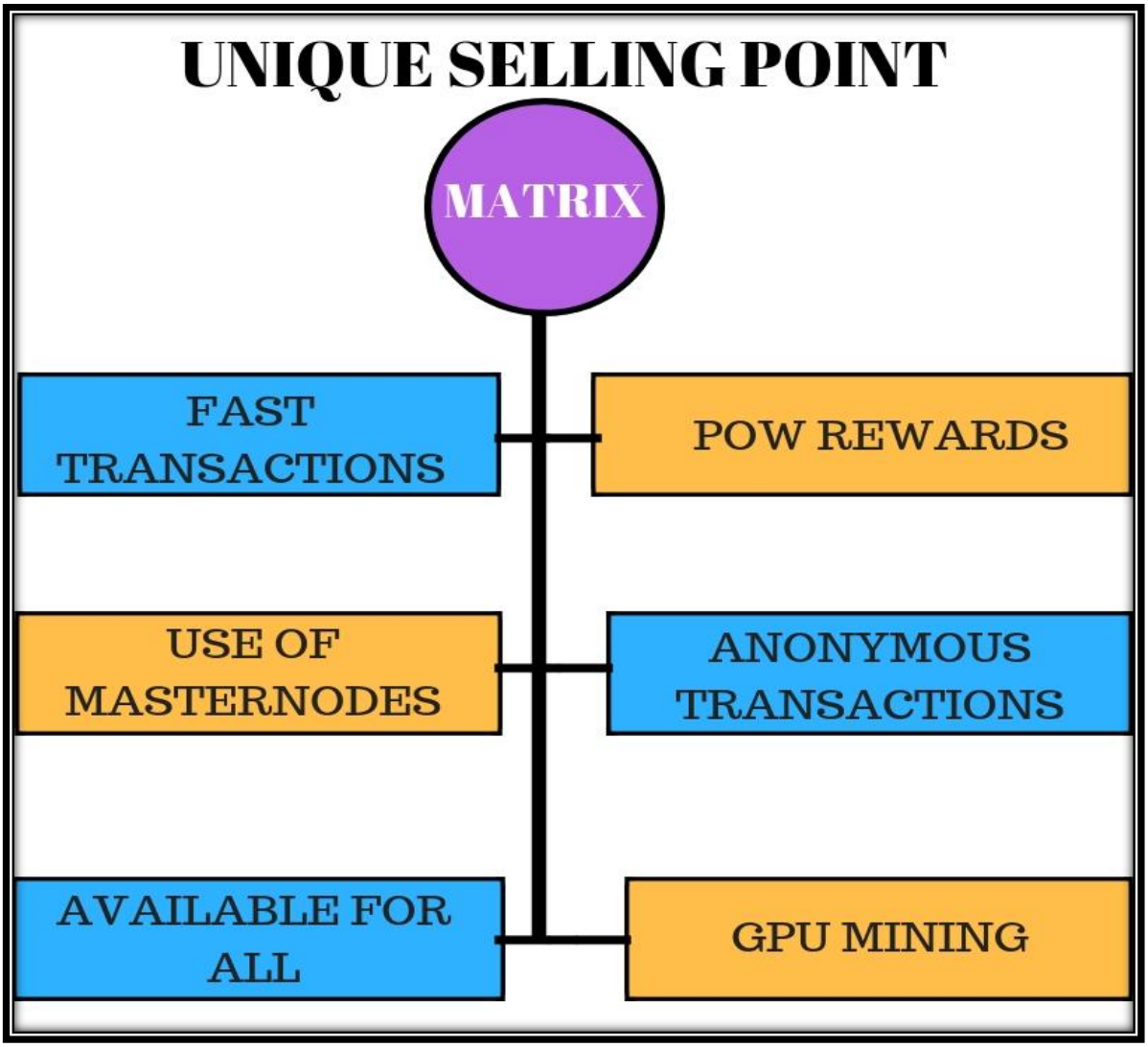
Business development allocation plays a major role in helping to improve and grow the working relationship with partners and industry leaders in order to enhance the client base of the platform. More so, expos, promotional events and conferences will be supported through the business development allocation.

Operational cost 10%

To sustain and keep the platform running, operational cost comes handy. Operational cost covers the day-to-day operations required to maintain Matrix platform. Operational cost covers expenses such as; recruitment process, office expenses and consultancy.

UNIQUE SELLING POINT OF MATRIX

The introduction of Matrix comes with several benefits that removes the limitations experienced with Bitcoin and several other cryptocurrencies. Some of the unique selling point of Matrix is shown in the image below;



TEAM MEMBERS

ALAA MEKKI : FOUNDER

Alaa Mekki is the founder of this overwhelming project which is bringing a new change in the finance and technology landscape. But he is unperturbed with the nature of the task involved because he has the right team that is willingly to assiduously work towards the success of the project.

ABRAHAM: CO – FOUNDER

Abraham is the co-founder of Matrix and provides immense support for the founder and all that is required to make Matrix a huge success.

ANIS ZENKRI : MARKETING ADVISOR

Anis Zenkri has an industry experience in marketing that is considered to be remarkable and his experience has played a great role in the publicity given to Matrix.

KARIM : DEVELOPER

Karim is a top-notch developer who played the major role in the development of Matrix as well as making sure that the technicalities involved for developing Matrix is perfectly handled.

MARLOSH : MARKETING , SOCIAL EXPERT

There is no better time than now in getting the services of a social expert to create buzz around Matrix, and Marlosh was just the right person to make it happen. Thanks to her ability to make public believe in the big idea of Matrix.

CONCULSION

Matrix is positioned to make its innovative project the right form of investment for everyone that desires a hassle-free means of carrying out financial transactions. Which means that individuals and businesses can now enjoy the immense benefit of using Matrix coin.