TERMS OF REFERENCE

CASE: VOTING PLATFORM.

BLOCK-CHAIN E-VOTING

Blockchain happened, a revolutionary technology that preaches decentralization in a world full of centralized authorities that are placed into authority in most cases, through electoral processes often carried out via offline voting system. In 2014 the topic of Block-chain technology as a stand-alone-tech and its applications separate from Bitcoin which was implemented earlier in 2008, were being addressed by concerned minds. What then is Block-chain and what is voting, in this case E-voting?

Blockchain technology is a method of data organization and decision-making that enables real time data synchronization and integrity by grouping all the data about existing transactions or other records into blocks, each of which is cryptographically linked to the previous one. *"Properties of Blockchain include; immutability, integrity, trustlessness, reliable reconciliation".*

"*In the simplest case, voting can be defined as a way of making a collective decision, which implies the formation of a common opinion based on the counting of votes of members of a particular group".* **E-voting (electronic voting)** is the implementation of the usual voting process via an online method by use of electronic devices, structures and applications that can access the internet.

OVERVIEW AND PURPOSE OF THE SYSTEM / PRODUCT

More often than none traditional offline voting systems and even the traditional online electronic voting (E-Voting) poses some basic challenges, advantages and disadvantages however , in this context ways will be considered on how to implement an E-voting platforms using blockchain technology (*using a common programming language)* as well as ways of mitigating the challenges facing traditional E-voting using blockchain technology.

SYSTEM CONTENT (SYSTEM BOUNDARIES).

A small scale election between trusted members of an organization can be pretty easy to handle and hardly will there be challenges. In a context of a larger scale election were there a large demographic and diversified population to cover in an enclosed time frame, traditional approaches that may be applicable to aforementioned small scale elections may not be feasible as such approaches will present the following disadvantages and limitations;

"

- *Non-transparency of vote counting*
- *Possibility of having fake voters*
- *Pseudo-anonymity of voters*
- *Possibility of vote forging* "

In this content possible solutions for the above mentioned will be considered as a fruition of the use of Blockchain technology to implement an electronic voting system in contrast to traditional electronic and paper and ballot voting system (offline voting).

INTERACTION (POTENTIAL) OF THE PRODUCT (WITH OTHER PRODUCTS AND COMPUTERS)

"*In order to apply decentralized (blockchain) E-voting to regular elections, we need a protocol that allows us to ensure the transparency of voting and the anonymity of users at the same time. Using blockchain as a technology on which a decentralized system can (not must) be based can provide the following features:*

- *A voter can verify at any time that his/her vote has been counted correctly*
- *Presence of the voting right proof and verification of the vote integrity due to using digital keys and signatures*
- *Vote forging is impossible because it will be immediately detected in the vote submission history*

"

The signatures to ensure the verification of authenticity and integrity of all sent transactions that are recorded in blocks. In regard to anonymity of voters, methods such as *ring signatures* can be used. *"Votes* above can be possible executing votes in form of transactions made by an eligible voter, which are signed using cryptographic

cannot be backdated, since such a change will be visible to all network participants who store the transaction history. Re-voting will only be possible by submitting a new transaction". Eligibility in this system may be based on rules of the voting system.

SECURITY REQUIREMENTS

Using cryptographic signatures and key pairs that are generated using specific hashing methods, provided a user doesn't expose these to others it will be quite impossible for a system hack or fraud of any form. Votes are cast in form of transactions that hashed and linked into blocks, as such a slight change in the system can be easily be noticed by the networks participants.

CHARACTERISTICS OF USERS (WHO IS THE END USER OF THE SYSTEM)

An eligible voter must present have following characteristics:

- Registered member of the local organization(as such application of centralized authority will be done here)
- Have an account or be a user of the voting platform (as such devices and software/applications that will be able to access the platform will be required)
- Generate key pairs and cryptographic signatures according to system rules/algorithm.

RESTRICTIONS

Basically, some of the restrictions that the system will have are; dependency on software and devices mistakes and lose of private key and other sensitive information may lead to disqualification of a voter and unlike the ballot and paper methods here a network participant will have to play a role of server in order to keep track of the history as such consuming a lot of storage space.