ELECTRONIC VOTING

User Manual

Andreas du Preez	12207871
Azhar Mohungoo	12239799
Gift Sefako	12231097

STAKEHOLDERS

EPI-Use	Roelof Nuade

Contents

1 General Information

1.1 System Overview

Electronic Voting, or eVoting for short, is a system which does exactly what the name suggest. It allows members of a demographic country to vote for a political party during an election period. It does so that each vote is completely anonymous by using Blockchain technology.

The system is usable via an online web page and an Android(4.4+) application.

There are essentially 4 types of users: An Administrator, a Political Party, an Activator and a Voter. Each having their own dedicated functionality. An administrator user can add a political party user, add an activator user, and deactivate a voter account. A political party account can only check the number of votes they currently have. An activator can only activate a user. And a voter can cast votes.

In order to make Electronic Voting safe and trustworthy, the activator user is needed. Initially when a new user is registered, they will automatically be 'deactivated', which prevents them from casting any type of vote. This is to prevent a voter from creating a bunch of fake accounts and using those fake accounts to vote multiple times. An activator first need to verify the identity of a voter by providing proof of identity (a drivers license or ID document), after which a voter is then activated and will be granted 2 votes: one vote for a national party, and one vote for a provintial party.

If a user has not registered yet, they can do so on the web site or on the Android application. Apon registration, the user need to provide: a valid ID number, a password used to log into the system, a name, a surname, the location their registered in (pre defined list of values eg. Pretoria, Johannesburg etc), a mobile number and an email address. A voter is the only user type that can register itself, an activator, political party and administrator can only be added by an existing administrator.

The beautifull part of eVoting is that it uses Blockchain technology, the same technology used in the famous Bitcoin currency. A blockchain is a distributed database that maintains a continuously-growing list of records called blocks secured from tampering and revision. A more indepth description is beyond the scope of this document.

1.2 System Configuration

eVoting can be generaly simplified by Figure 1. When a client uses the system, they will communicate with eVoting through a RESTfull webservice, sending an receiving JSON objects. The webservice is connected to a backend, processing the requests which communicate with the database and blockchain. Since the system uses a webservice as a communication medium between the client and backend, it allows possible future expansion of eVoting for example integration of any third party company, or other mobile platforms.
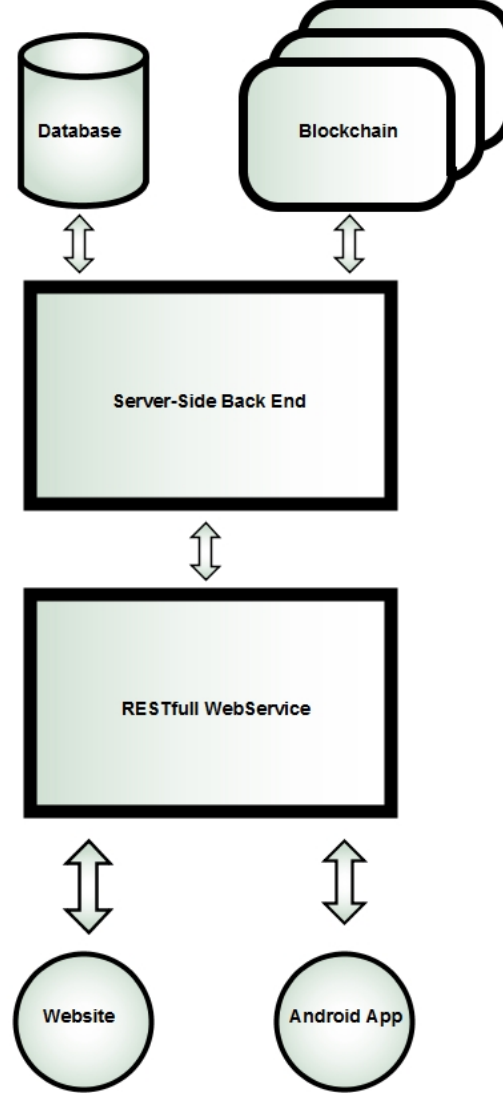
Figure 1: Overview of eVoting

The blockchain structure of eVoting is depicted by Figure 2. It consist of 3 types of nodes: a Root (admin) node, Political Party Node and a Voting Station node. Each of them have different permissions. The Root node has all of the permissions, a Political Party node only has connect and receive permissions and a Voting Station node has connect, send, receive and mine permissions. It is important to keep the eVoting blockchain private from public usage, so new nodes must be approved and added by the root node explicitly.
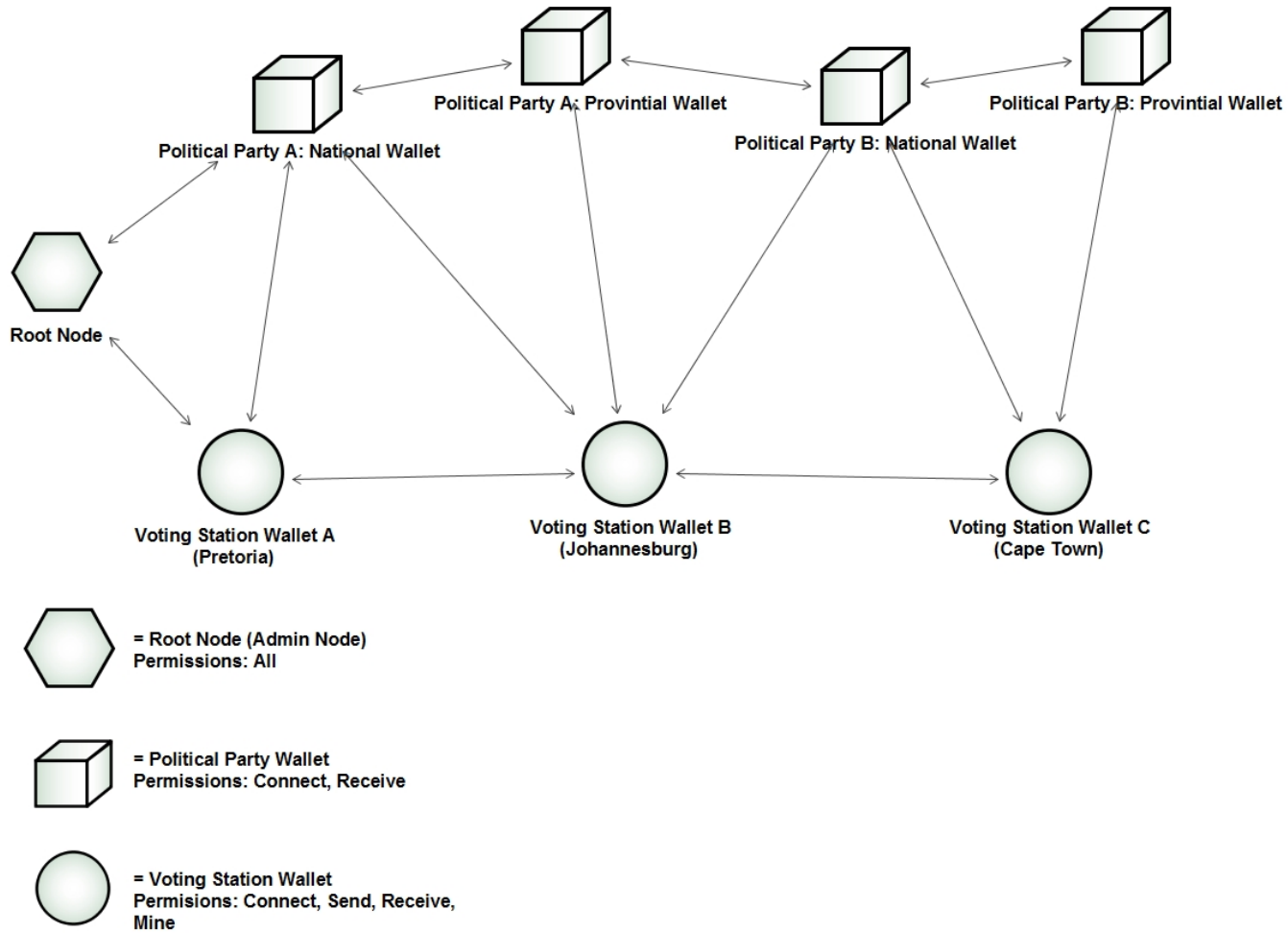
Figure 2: Blockchain Node Structure

TODO may need to elaborate here more

1.3 Installation

TODO: Webservice, database, android app etc

1.3.1 Blockchain

To set up the eVoting Blockchain, each node will need a static IP address.
Each node will also have a RPC username and RPC password automatically generated by multichain. If however you want to specify custom RPC usernames and RPC password, you may do so, but for the sake of eVoting, the generated RPC password is strong enough.

Each node will require the following setup:

Required Sofware:

- Linux distribution

- Multichain. Available at http://www.multichain.com

System requirements:

- Linux: 64-bit

- 512 MB of RAM

- 1 GB of disk space.

We chose Lubuntu because it is a minimalist lightweight Linux distribution. Lubuntu is available at http://lubuntu.net/
Installation instructions for Multichain can be found at http://www.multichain.com/download-install/

1.3.1.1 Setting up a blockchain the Root node   In the Linux terminal, issue the following commands:

su [Root-Password]
multichain-util create EVoting

You should see the text "Blockchain parameter set was successfully generated."
The blockchain has been created but isn't running yet, we first need to configure it.
Edit the "multichain.conf" file at the following default location:
/root/.multichain/EVoting/multichain.conf
Here we can specify this node's RPC username and RPC password, but for EVoting we leave it as it is. Then we need to add 2 extra lines to the file, one specifing that this is the Admin Node, the other specifying which network range is allowed to issue remote commands. The file should look something like this (the IP range might need to change in your case):
rpcuser=multichainrpc
rpcpassword=Gnb5RsXa783K9LbJGjtfZNpnJg8UbDu8bza8htd9DMPX
rpcallowip=192.168.43.0/255.255.255.0
server=1
rpcport=7419

Then we need to change the actual blockchain configuration. Edit the "params.dat" file and make sure the following values are as follows:

This part is to ensure the blockchain is private.

```
    anyone-can-connect = false
anyone-can-send = false
anyone-can-receive = false
anyone-can-issue = false
anyone-can-mine = false
anyone-can-activate = false
anyone-can-admin = false
allow-p2sh-outputs = true
allow-multisig-outputs = true
```

The following line is to give the admin an initial value of 10000000 which will be spread between all the Voting Nodes.
first-block-reward = 1000000

This line is to make a vote a multiple of 1 and not a decimal value:
native-currency-multiple = 100000000

The complete params.dat file that is used for eVoting can be found on our Github page at EVoting/Documentation/BlockchainConfigurationFiles/params.dat

To start the admin node and also the blockchain, issue the command:
multichaind EVoting
Now that the blockchain is running, other nodes can connect to it. In the terminal of the Voting Node, issue this command:
multichaind EVoting@192.168.1.20:4771
Where the IP is the IP address of the root node.