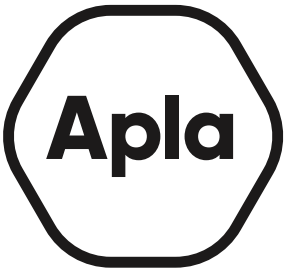


PUBLIC OFFER

E-VOTING SERVICES

ANNUAL SHAREHOLDER MEETINGS

Table of Contents

1. Apla E-Voting Technology

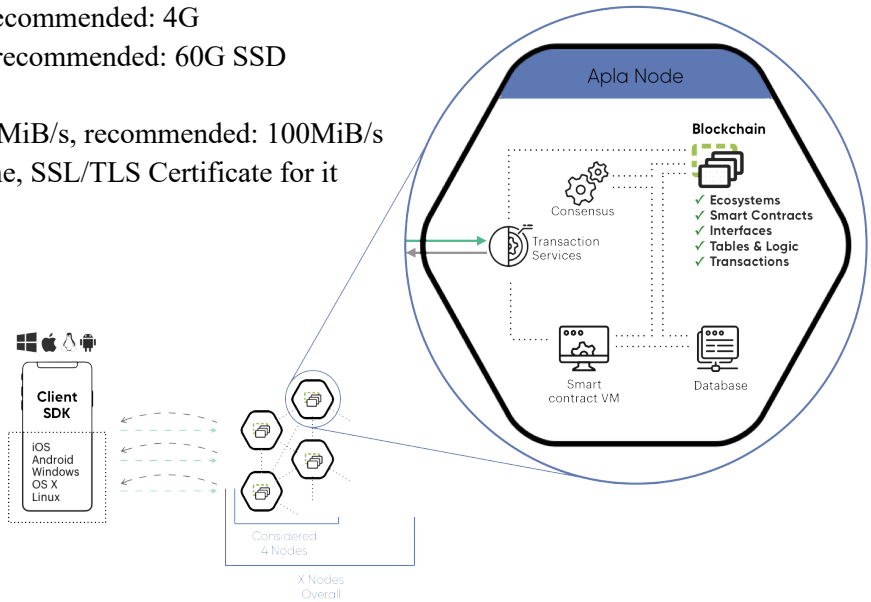
Apla (EGAAS S.A.) is a technology company based in Luxembourg. We are developing software solutions for our corporate clients to enable digitalization of their shareholder engagement practices. Apla E-voting is a blockchain-backed electronic voting software that is used by shareholders and board members to receive meetings notifications, documents and cast their votes electronically in a secure, transparent and legally sustainable manner.

For each client, we deploy a private e-voting digital platform to process all electronic transactions pretraining to our client's meetings. The platform is powered by our original blockchain technology in order to conform to the following requirements for electronic voting systems:

- Availability: the solution must always be available in the course of the voting process
- Traceability: the solution must store the history of all operations
- Data integrity and transparency: the solution must guarantee that it is always possible to check who modified the data in the data base
- Reliable: the solution must guarantee consistency of the data

The digital platform will operate on 3 nodes. The platform topology can be summarized as follows:

- full connected topology
- nodes are placed in a logically single-level p2p network
- all nodes maintain single source of truth and equal in functionality
- all nodes are connected to Cluster of NTP servers
- each period of time the right to generate a block passes to the next node
- block size is customizable
- Technical requirements for each node:
  RAM: minimal: 2G, recommended: 4G
  HDD: minimal: 30G, recommended: 60G SSD
  OS: Debian 9
  Network: minimal: 10MiB/s, recommended: 100MiB/s
  Static IP, Domain name, SSL/TLS Certificate for it



2. Digital signing operations

We've made our best efforts to ensure that our e-voting system will be legally sustainable in case of any potential litigation resulting from the use of our e-voting technology. This is achieved through the blockchain-backed traceability, transparency and integrity elements of the platform and digital signing architecture.

2.1.Signing by private keys

In the course of using the Apla e-voting software, all users' activities (eg., voting, etc) will be recorded in the system as electronic transactions **("electronic transactions").** Electronic transactions, which are called by shareholders and other users, will be signed by their private keys generated and stored on the users' devices at the time of the account's creation. We have integrated the Digital Signature Algorithm named ECDSA for generating private keys and authenticating their owners upon signing electronic transactions.

Upon singing-up for a new account, a user will be asked to acknowledge and confirm that:

- he/she will be solely responsible for a safe custody of the private key generated on her/his device;
- a signature by the private key shall be as legally valid and binding upon him/her as the original handwritten signature on a paper document;
- electronic transactions signed by the user's private key, including electronic documents, shall be deemed (i) to be "written" or "in writing," (ii) to have been signed and (iii) to constitute a record established and maintained in the ordinary course of business and an original written record when printed from electronic files;
- transaction reports, paper copies or "printouts," can be introduced as evidence in any judicial, arbitral, mediation or administrative proceeding, and you will agree to accept them as being admissible to the same extent and under the same conditions as other original business records created and maintained in documentary form;
- the user shall not contest the admissibility of true and accurate copies of documents signed by his/her private key on the basis of the best evidence rule or as not satisfying the business records exception to the hearsay rule.

2.2.Legal effects of electronic signatures

Signing electronic transactions by the user's private key is not treated as a qualified signature under EU law.

Nevertheless, according to Article 5 of the EU Directive 1999/93/EC on a Community framework for electronic signatures,

"*Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:*

— in electronic form, or

— not based upon a qualified certificate, or

— not based upon a qualified certificate issued by an accredited certification-service-provider, or

— not created by a secure signature-creation device."

You may want to seek a legal advice of your lawyers to verify the legally binding effect of signing by the private key under the law of your jurisdiction.

3. Apla services

We provide a wide range of services to facilitate the e-voting process for your general shareholder meeting (the **"Project"**) with the use of our e-voting technology. Specifically, our services include the following:

3.1 Platform set-up and maintenance

We will deploy a digital platform and install our e-voting applications on the top of it either on our servers, or your servers, or shared IT infrastructure to enable the following functionalities:

- setting up a company that conveys a shareholder meeting, including management of roles and access rights to data;
- creating a register of shareholders of your company, assigning voting rights to shares;
- registration of shareholders for participating in a general meeting: generating a pair of cryptographic keys by the shareholders in the mobile application, creating an account on the network using a public key, shareholders' identification by email;
- creating a vote with an arbitrary number of questions and setting up parameters for calculating the result, loading the necessary documents;
- notification of shareholders about a new vote;
- electronic voting functions;
- generating system reports for shareholders on the decisions made for each voting item;
- counting and displaying the result of voting;
- generating and storing of complete statistics on the voting procedure (approval of the agenda, notifications, confirmation of participation, voting).

The anticipated timing for the platform set-up services is one working day. We will also render the platform admin services throughout the whole period of the Project.

3.2. Customization services

Depending on the procedures that apply to your general shareholder meeting under the applicable law and internal by-laws of your company, we will create smart contracts and smart laws to digitalize the meeting assembly and voting process. This includes the following:

- voting majority rules applicable to each item of the meeting agenda (simple or qualified);
- voting eligibility rules attributable to the company's shares (eg., one share – one vote or different rules);
- quorum requirements for the meeting to be sustainable;
- shareholder notification requirements (by email or post)
- meeting notification content;

- requisites of the transaction report that will be issued to shareholders after each vote cast;
- requisites of the meeting minutes
- statistical information and data storage

Smart contracts are the basic elements in the implementation of algorithms in applications on the Apla platform. Contracts are final portions of code that perform the following functions: (1) receipt of information from the user interface or other contracts ("data" section), (2) analysis of data correctness ("conditions" section), and (3) execution of the required transactions – database records ("actions").

Smart laws can be qualified as governing smart contracts. They determine the access rights, signing authorities and other parameters demanded by the voting process.

We expect the timing for the services indicated in point 3.2 above to be from 2 weeks to one month, depending on the requested customization needs. This term includes the testing phase.

3.3. Corporate secretary services

There is a role of the "corporate secretary" on the platform that can be assigned by you to us. This role enables the following authorities:

- entering your company's details in the platform DB;
- creating an account for each shareholder of your company on the platform;
- filling out the shareholders' data in the platform DB;
- initiating the shareholder meeting;
- sending time-stamped meeting notifications by email through our platform resources;
- shareholders' help desk (by email).

We've got an integrated electronic sign off procedure on the platform. All data entries and electronic transactions with your shareholders initiated by the corporate secretary will need to be electronically validated in the system by a responsible person from your company before they can be processed.

The corporate secretary services will be rendered throughout the Project term.

3.4. Audit trail

Every electronic transaction on the platform leaves a time-stamped digital footprint that will allow you to identify the who did what and when during the meeting preparation and voting process. After the Project term has ended, we will create a back-up version of the platform on a hard disk and hand it over to you to make this data readily available for future audit.

In addition, we will prepare an audit trail report that will include the following data:

- algorithm for counting the voting results;
- time-stamped meeting notifications sent to shareholders;
- vote casting reports generated by the system of each shareholder;
- vote casting results for each item of the agenda indicating how many shares participated in the voting, total votes casted “For”, “Against” or “Abstained”.

4. Software license

In exchange for the fees indicated in section 6 hereof, we will grant you a non-exclusive right and license to use our e-voting software solution for the purposes and within the limits and duration of the Project.

Furthermore, at the time of setting up an account on the platform, your shareholders will need to acknowledge their consent with the end user license terms. It’s a free to use license.

5. Data privacy

We are committed to apply high standards to dealing with personal data and other sensitive information.

Specifically, the users’ personal data collected during the account registration process, meeting documents and other information will be directly sent to and stored on servers of your company; we shall get a remote access to this data for the purposes and within the limits required to fulfil our obligations under this agreement.

If the platform network is deployed fully or partially on our servers, after the completion of the Project, all the information on our servers we be deleted within 2 weeks. We will though retain an archived copy of the platform for the period of 3 years for future references as the case may be.

6. Fees

We charge royalties for the use of our platform resources for the purposes of the Project. The amount depends on a number of shareholders. The royalties include the price for services set forth in Article 3 hereof.

In addition, we will charge you out-of-pocket expenses related to the provision of the services such as rental of the servers, if needed, postal and other related expenses.

Before we proceed with the assignment, we’ll ask you to make the 50 % prepayment of the fees. The remaining 50 % is to be paid within 10 days after the completion of the Project.

7. Platform information

A more detailed information about the architecture of the platform, cybersecurity and other matters can be found in Annex 3 hereto.

If you agree with the terms of this commercial proposal, please countersign it along with the commercial license agreement and send us back the signed original copy by post to the address specified on the letterhead of the cover letter.

Kind regards,

Vitaly Bondar
Director

We hereby agree to and acknowledge our consent with the terms of the present commercial proposal.

Signatory

Name: _____

Represented company: _____

Date: _____

Annex 1

Apla Platform Overview

1. Apla Blockchain Protocol

The Apla team has developed an original blockchain protocol that will be used as a core technology to deploy the e-voting platform.

The source code of the Apla protocol, including the platform technical documentation, can be found in the repositories on GitHub: https://github.com/AplaProject/. It's open source and distributed under the GNU General Public License v.2

2. Network

The e-voting will be based on a peer-to-peer network. Full nodes of the network will store an up-to-date version of the blockchain and a database, in which the current state of the platform is recorded. After having been verified, transactions are to be recorded in a new block, and the data is to be simultaneously updated in the database.

3. Database

In order for contracts and interfaces to quickly search and obtain data, a common database will be used for the whole platform, copies of which will be stored on all full nodes of the network. Transactions that are broadcasted to the network by contracts, are in essence, table entries in the database. During the creation of a block and its subsequent addition to the blockchain, the database will simultaneously be updated on all full nodes of the platform. In this way, the database will hold the current (most up-to-date) state of the blockchain. The tables will not be linked to any specific contracts, and can be used by any and all applications.

4. Consensus mechanism

Full nodes of the network (i.e., validating nodes) will store the up-to-date version of the blockchain and the database, in which the current state of the platform is recorded. The network users will receive data by requesting it from databases of validating nodes using the software client (or REST AP commands). New data will be sent to the network in the form of transactions signed by the users. Such transactions are in essence commands for modification of information in the database.

Transactions are aggregated in blocks, which are then added to the blockchain on the network nodes. After a new block is added to the blockchain, each validating node will process the transactions in this block, thus making changes to data in its database accordingly.

Only validating nodes have the right to generate new blocks. Validating nodes will form and sign blocks subsequently one after another in accordance with a sequence list, in time intervals (one second, by default). If a validating node was not able to create a block in the allotted time, the right to sign a new block is passed to the next validating node in the list.

5. Cybersecurity

A blockchain is an informational system which by its own architecture is able to offer a high-level of security from falsification and loss of data. However, there are different ways in which hackers can launch attacks to crash nodes or the system as a whole. We have implemented solutions to protect the system against such attacks.

- *51% attack*

We deploy the original proof-of-elapsed activity consensus mechanism. The 51 % attack may theoretically work only in case of someone taking the full control over the 51 % of the validating nodes in the system.

- *Remote attack*

The building of an alternative chain is eliminated by introducing a parameter that determines the maximum depth of branching the blockchain. If a blockchain node breaks from the other nodes for over a specified number of blocks, it will not be accepted as valid.

- *DDoS attacks*

We place limits on a number of transactions per block signed by each user. Protection from DDoS attacks which execute data reading (interface calls) is facilitated by standard methods for servers. (Nodes which aren't able to withstand DDoS attacks will be excluded from the list of validating nodes where they are unable to process transactions within a set period of time.)

- *Sybil attacks*

The blocking of a separate node by connecting it only to the nodes of the hacker is practically impossible since the number of the platform nodes will be fixed and the full list of such nodes will be stored on each individual node.

- *Exploiting hash function crypto-algorithms*

Transactions are signed using ECDSA algorithm. ECDSA uses elliptic-curve cryptography (ECC), an approach to public key cryptography based on algebraic structure of elliptic curves over finite fields. It is currently considered as the most secure.

- *Wrongful use of contract code exploitation*

Where there is a wrongful use of contract code exploits which leads to a breach of the platform's data integrity, validating nodes retain the right to launch a preinstalled contract (smart law), which temporarily shuts down access to the contract and accounts which are affected during the attack. To remedy the situation, the validating nodes will execute a voting process to change to the source code in which the exploit was found and restore the blockchain platform to the state before the attack.

6. Specific Q&As

How consistency can be ensured?

The platform guarantees that if two nodes have the same state *state1* and both of them receive the same block *block1,* then after processing that block both nodes will have the same state (either *state1* or *state2* depending on whether block is accepted or no).

The only way to update state is by processing blocks. The Apla protocol guarantees that there is a chain of blocks, by executing which the platform will come up with the current state. Each validating node stores the chain of blocks that corresponds to its state.

What is a block?

A block is a set of verified transactions signed by one of the validating nodes. The block contains the entire body of transactions. For each block a hash is computed. Thus, the platform could guarantee integrity of all operations made inside the system. In particular, the platform guarantees the following properties:

- no transaction could be removed from the block after it was generated (block will become invalid)
- no transaction could be added to the block after it was generated (block will become invalid)

- no transaction could be modified after the block was generated (block will become invalid)

Block validation methods

For each block the following main properties are validated:

- block has the right format
- block was generated by one of the nodes (was signed by one of the nodes)
- block was generated during specified period of time
- block contains transactions

- each transaction is valid
- block has hash of the previous block
- block hash corresponds to the block content

Transaction verification methods

- Transaction has the right format
- Transaction is signed by one of the users of the network
- Transaction hash corresponds to the hash content
- Transaction wasn't processed before (wasn't included in any block accepted by the node)

Periodic / eventual cut-off

Any node could be turned off in any time. There is no danger for the network at all. Even more, no special activities are required in order to bring it back to the network. After turning on the node, it will automatically download the longest chain of blocks and updates its state.

How the fault tolerance has been ensured, system backup

It is provided by Apla out of the box. Basically, each node has all information that is needed for the network to work. The more nodes in the network, the more backups you will have