we.vote

Техническое описание Waves Enterprise Voting

Выпуск master

https://wavesenterprise.com

мая 03, 2023

О системе

Функционирование и развитие общества невозможно без механизма принятия коллективных решений. Таким механизмом являются выборы и голосования, считающиеся на сегодня наиболее справедливой и демократичной формой определения общественного консенсуса.

При интенсивных социальных взаимодействиях, характеризующих современное общество, практически каждый сталкивается с необходимостью участия в процедурах принятия решений. Однако, несмотря на невероятное развитие технологий, основными инструментами голосования попрежнему остаются ручка и бумага.

Тем не менее, информационные технологии позволяют выполнять огромное число задач в режиме «онлайн», но для процедуры голосования в большинстве случаев попрежнему необходимо либо личное присутствие, либо печать, распространение и обработка бумажных бюллетеней.

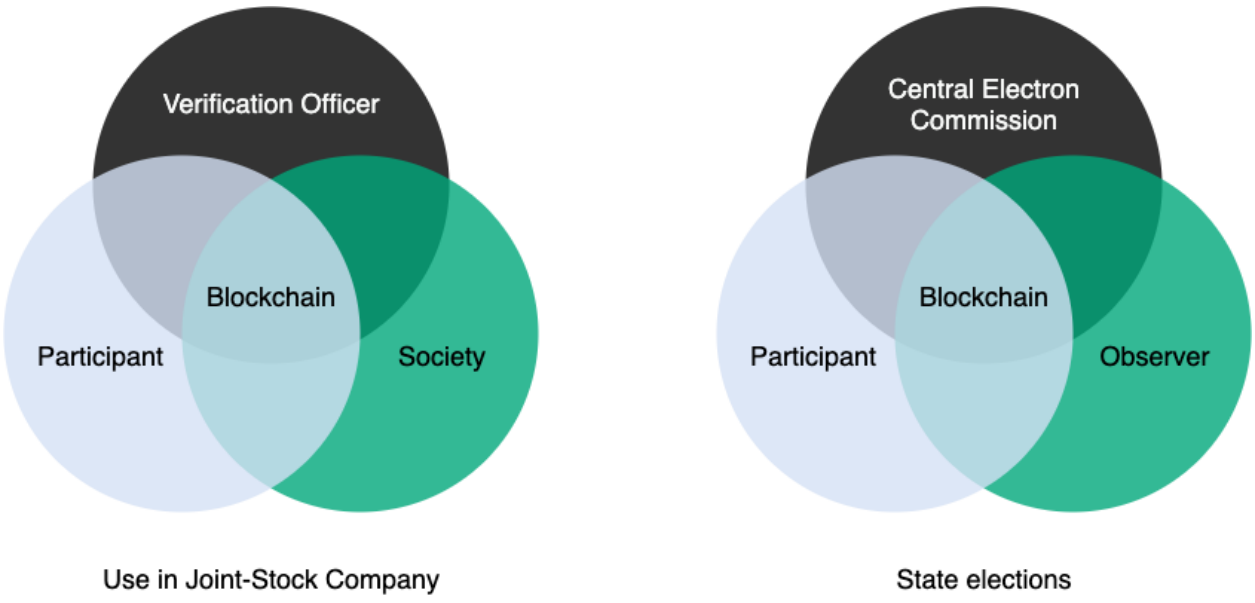
Развитие электронных систем голосования устраняет проблему личного присутствия, но их применение на практике все еще ограничено. Такое медленное внедрение технологии можно считать отчасти оправданным. Помимо общей инерционности крупных общественных структур, не позволяющей им пользоваться всеми преимуществами передовых технологий, существуют опасения по поводу возможных фальсификаций.

Стоит признать, что возможности для фальсификаций при электронном голосовании ненамного шире, чем при «бумажном» варианте. Слабым местом в обоих случаях является централизованный орган, осуществляющий хранение и подсчет голосов. Хотя этот орган и является доверенным для участников голосования, если есть возможность подменить бумажный бюллетень или запись в электронной базе данных, полностью исключить возможности манипуляций с результатами голосования нельзя.

Именно в сфере голосования технология распределенного реестра наиболее явно демонстрирует свои преимущества – прежде всего, прозрачность и защищенность.

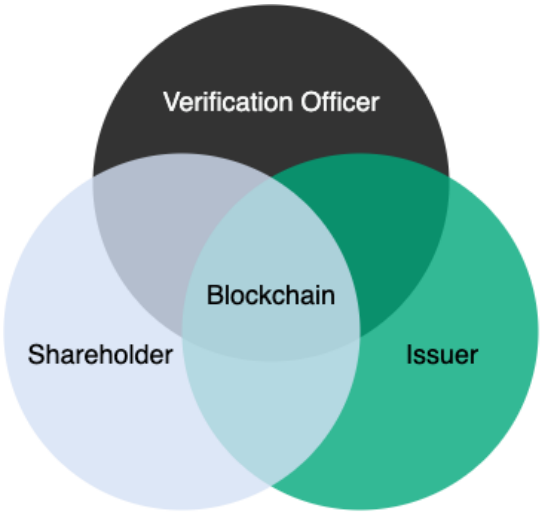
Используя свойства *блокчейна*, а также современные криптографические алгоритмы *криптографическую защиту целостности данных*, децентрализованный *консенсус*, невозможность манипуляций с информацией, *гомоморфное шифрование* и разделение ключей шифрования компания Waves Enterprise разработала систему WE.Vote, позволяющую любым организациям, в которых решения принимаются коллективно, организовать и провести доверенное голосование.

Пользователи системы

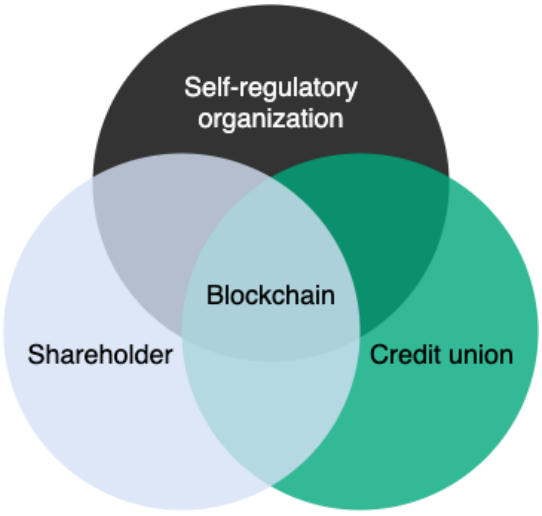


Любые организации, в которых решения принимаются на основе голосования. Прежде всего, это общества с ограниченной ответственностью, кредитные кооперативы и акционерные общества. Решение подойдет и для саморегулируемых организаций – товариществ собственников жилья и управляющих

компаний. Платформой можно воспользоваться и для организации государственных голосований муниципального и федерального уровня.



Use in Limited Liability Company



Application in credit cooperatives

ГЛАВА 1

Проблематика онлайнголосований

Несмотря на то, что онлайнголосования набирают все большую популярность, их применение сопряжено с новыми вызовами.

Вопервых, большинство сервисов онлайнголосований это централизованные решения, полностью управляемые компаниейоператором. Такие решения могут быть всесторонне защищены от внешних угроз, однако теоретически предоставляют своему разработчику доступ к организуемым голосованиям. Соответственно, компанияоператор может какимлибо образом вмешаться в ход голосования или получить информацию о его результатах. Это создает проблему доверия между организатором голосования, его участниками и компаниейоператором сервиса.

Проблема доверия решается путем создания децентрализованной системы, удовлетворяющей двум основным критериям:

- доступ к процессу голосования и его результатам имеют только его организатор и участники;
- доступ к собственному бюллетеню имеет только участник голосования.

Одним из технических решений, позволяющих реализовать такую систему, является **блокчейн** система хранения и передачи данных в виде последовательной цепочки взаимосвязанных блоков. Каждый блок содержит хэшсумму данных предыдущего блока. Это делает невозможным последующее изменение содержимого любого из блоков, поскольку для этого необходимо изменить содержимое блоков на протяжении всей цепочки на всех узлах.

Система на основе блокчейна не имеет единого центра управления, все данных одновременно хранятся на всех узлах сети в открытом или зашифрованном виде. Это позволяет обеспечить безопасность и целостность передаваемых данных, минимизируя возможность компрометации.

Применение современных алгоритмов шифрования и правил работы с конфиденциальными данными, наряду с технологией блокчейна, максимально защищает систему от возможных атак.

ГЛАВА 2

Концепция сервиса онлайнголосований на основе блокчейна

Применение технологии блокчейна позволяет создать безопасную систему голосования, подчиняющуюся следующим правилам:

- Организатор голосования полностью управляет правилами доступа к повестке голосования.
- Список участников голосования создается его организатором.
- В голосовании принимают участие лица, указанные в списке участников голосования.
- Правила проведения голосования задаются его организатором.
- Участнику гарантируется целостность его бюллетеня с повесткой голосования.
- Полностью соблюдается тайна голосования: доступ к содержимому своего бюллетеня имеет только сам участник.
- Доступ к результатам голосования имеют только его организатор и участники.
- Организатору и участникам гарантируется целостность результатов голосования.

В такой системе блокчейн выступает как универсальное решение для хранения и передачи информации. Данные, опубликованные в блокчейне посредством транзакций, невозможно изменить без изменения всей цепочки, что гарантирует их неизменность. Помимо этого, каждая транзакция подписывается публичным ключом отправителя. Поэтому данные блокчейна могут быть использованы для проверки целостности данных, передаваемых участникам голосования с бэкенда сервиса.

Поскольку все данные в блокчейне публичны, для конфиденциальных данных системы применяются алгоритмы шифрования, также гарантирующие их целостность.

ГЛАВА 3

Преимущества сервиса онлайнголосований WE.Vote

Сервис WE.Vote наиболее полно реализует концепцию безопасной системы онлайнголосования.

Сервис основан на блокчейнсети Waves Enterprise Mainnet, которая обеспечивает взаимодействие участников с системой:

- прием, хранение, передачу и сверку данных о голосовании и голосах участников;
- разграничение прав доступа при помощи ролевой модели блокчейна.

Данные в зашифрованном виде хранятся одновременно на всех нодах блокчейна, что гарантирует их целостность и невозможность утраты.

Учетная запись каждого участника снабжена ключевой парой для подписания голоса и идентификации в блокчейне. Ключевая пара, а также средства доступа к ней, могут храниться как у самого участника, так и в защищенном облачном хранилище сервиса. Это позволяет участнику самостоятельно определить степень защиты своих учетных данных, а также, при хранении ключевой пары в облачном хранилище, быстро восстановить доступ к учетной записи и голосованиям.

Данные каждого голосования защищены криптографическими алгоритмами, которые выполняют шифрование голосов участников и хэширование материалов голосования. Прииняемая схема шифрования ЭльГамаля позволяет подсчитать голоса, не расшифровывая их.

Для того, чтобы каждый участник мог убедиться в корректности учета своего голоса, используется система доказательств с нулевым разглашением. Эта система позволяет участнику факт записи и содержимое его бюллетеня, не раскрывая содержимое организатору голосования.

Для лёгкой организации и проведения онлайнголосования сервис снабжен вебклиентом интуитивно понятным вебинтерфейсом.

ГЛАВА 4

Создание и проведение вашего первого голосования

Сервис WE.Vote дает возможность ознакомиться с основными функциями голосования. Для этого на баланс каждого нового пользователя начисляется 20 бесплатных бюллетеней.

Чтобы создать ваше первое голосование с использованием демонстрационных бюллетеней, выполните следующие шаги:

1. Перейдите на вебсайт **we.vote** и нажмите кнопку **Log in**. Вы будете перенаправлены на страницу входа в клиентское приложение WE.Vote.
2. Выберите ссылку **Создать учетную запись**.
3. Введите ваш адрес электронной почты и пароль, затем подтвердите ваш электронный адрес по ссылке в присланном письме.
4. Войдите в клиентское приложение при помощи логина и пароля.
5. Введите ваше имя и название вашей организации.
6. Нажмите на кнопку **Создать** в сообщении, которое появится в правом верхнем углу экрана.
7. Выберите способ хранения seedфразы: в облаке или самостоятельно.
8. При выборе самостоятельного хранения, запишите вашу seedфразу и храните ее в надежном месте.
9. Пригласите участников: нажмите на кнопку **Участники** в правом верхнем углу экрана.
10. Нажмите на кнопку **Добавить участника**.
11. Введите электронные адреса участников голосования через запятую.
12. Нажмите на кнопку **Пригласить**. На электронные адреса приглашенных вами участников будут отправлены пригласительные письма с ссылкой на регистрацию в сервисе.
13. Нажмите кнопку **X** в правом верхнем углу экрана, чтобы вернуться в основное меню сервиса.
14. Нажмите на кнопку **Создать новое** для создания нового голосования.
15. Введите название вашего голосования.
16. Выберите дату и время проведения голосования, его тип, и кворум.

17. Введите вопросы, выносящиеся на повестку голосования. Для добавления нового вопроса, нажмите на кнопку **Добавить вопрос**.
18. Установите флажки напротив участников, выбранных вами для голосования.
19. При необходимости, приложите дополнительные материалы для ознакомления.
20. Нажмите на кнопку **Опубликовать**.

Вам не требуется выполнять какихлибо действий для начала голосования: оно начнется автоматически в выбранное вами время.

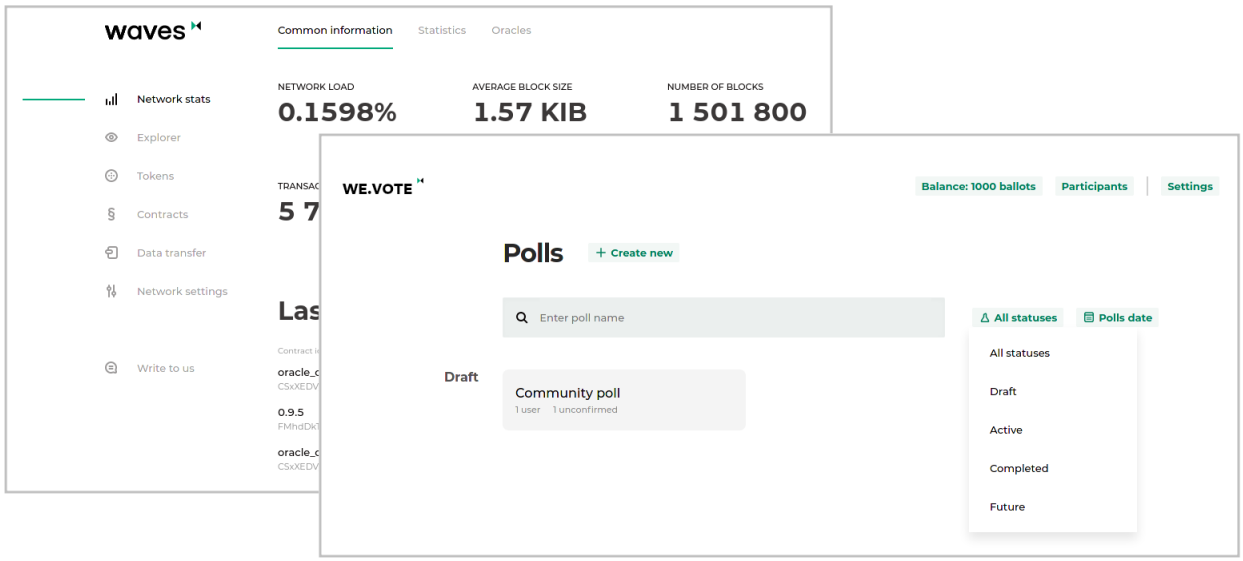
Чтобы принять участие в голосовании:

1. Выберите карточку вашего голосования в основном меню сервиса.
2. Ответьте на предложенные вопросы, нажав на радиокнопки или флажки напротив предпочтительных вариантов ответа.
3. Нажмите на кнопку **Проголосовать**.

Результаты голосования будут опубликованы автоматически по его завершении. Все участники получат уведомление об окончании голосования и смогут ознакомиться с результатами.

ГЛАВА 5

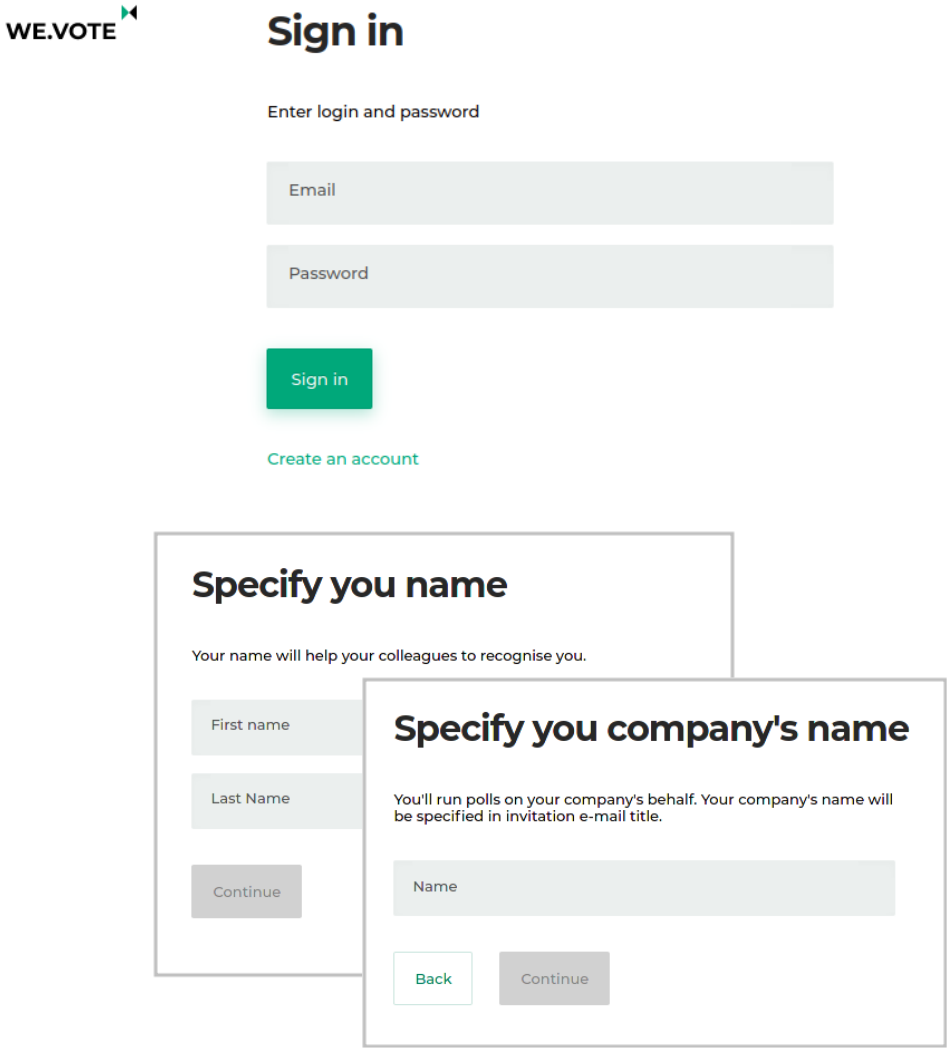
Регистрация учетной записи



Перед использованием WE.Vote создайте учетную запись в клиенте системы. Вы можете сделать это как самостоятельно, так и по приглашению от другого участника. Для работы на WE.Vote мы используем общую учетную запись для всей экосистемы сервисов Waves Enterprise. Если вы уже регистрировались на наших ресурсах, просто введите ваш логин и пароль на странице входа.

5.1 Самостоятельная регистрация

Для самостоятельной регистрации в клиенте нажмите кнопку **Создать аккаунт**. Укажите ваш адрес электронной почты, придумайте надежный пароль и нажмите кнопку **Зарегистрироваться**. Подтвердите введенный адрес электронной почты, перейдя по ссылке, которая придет в письме. После этого Вы можете зайти на портал и приступить к дальнейшей работе на сервисе.



При первом входе мы попросим вас:

- указать свое имя, чтобы ваши коллеги могли узнать вас в системе;
- указать название организации, от имени которой вы планируете проводить голосования.

Мы отправим письма с приглашениями вашим коллегам от имени указанной организации это позволит им обратить внимание на email и не отправить его в «Спам».

5.2 Регистрация по приглашению

Если вас пригласили зарегистрироваться на WE.Vote чтобы принять участие в голосованиях, вам придет приветственный email со ссылкой. Пройдите по этой ссылке, чтобы задать пароль для своей учетной записи и войти в личный кабинет WE.Vote.

При входе мы предложим вам присоединиться к пригласившей вас организации. Согласившись, вы получите доступ к ее голосованиям.

5.3 Смена и сброс пароля

В случае если вы забыли пароль от учетной записи, сбросьте его. После этого задайте новый пароль и восстановите доступ в свой личный кабинет. При этом стоит иметь в виду, что доступ к WE.Vote определяется не только знанием пароля от учетной записи, но и доступом к вашему секретному ключу.

Ключ используется для электронной подписи вашего голоса. Процедура смены/сброса пароля будет отличаться для пользователей хранящих свои ключи в облачном хранилище или самостоятельно. Подробнее об этом см. следующий раздел.

5.4 Создание и хранение ключей

WE.Vote создан с применением технологии блокчейна, что позволяет ему предоставлять беспрецедентный уровень защиты информации, недостижимый для обычных онлайнсервисов. Это достигается в том числе за счет того, что любое взаимодействие участников процесса голосования с системой представляет собой транзакцию, подписанную уникальным секретным ключом.

Каждый пользователь имеет два ключа открытый и закрытый. Открытый ключ служит идентификатором пользователя в блокчейне, а закрытый для подписания его голоса. Если вы являетесь участником определенного голосования, ваш ключ будет зарегистрирован в смартконтракте. Сервис примет и посчитает только те голоса, которые были отправлены и подписаны одним из зарегистрированных ключей.

Такие строгие правила работы с данными налагают повышенную ответственность за надежность хранения ключа утратив его, вы не сможете принять участие в уже опубликованных голосованиях.

Для облегчения работы с ключами, на WE.Vote они трансформируются из длинного случайного набора букв и чисел в мнемонический вид набор из 15 слов, называемый **seedфразой**. Сохранив seedфразу, вы сохраните доступ к своему закрытому ключу и, соответственно, возможность участвовать в голосованиях.

WE.Vote предоставляет два варианта хранения seedфразы: самостоятельное хранение на устройстве пользователя, или в защищенном облачное хранилище сервиса.

Самостоятельное хранение более предпочтительно для пользователей, которые готовы самостоятельно определить необходимый уровень защиты своей seedфразы и обеспечить ее собственными средствами: записать на листке бумаги и положить в сейф, сохранить в менеджере паролей, сохранить в текстовом файле с заметками, сделать скриншот и т.п. В этом случае безопасность seedфразы целиком и полностью сосредоточена в руках пользователя: ваша seedфраза не передается и не хранится на WE.Vote, мы не сможем восстановить ее в случае утери.

При работе с сервисом закрытый ключ хранится локально, на устройстве пользователя в защищенном хранилище браузера. Ключ зашифрован паролем пользователя. После того, как вы вводите логин и пароль и входите на WE.Vote, ключ расшифровывается и может быть использован для подписания вашего голоса. Чтобы получить возможность голосовать на другом устройстве или в другом браузере,

Greetings,

You've been invited to participate in e-voting at WE.VOTE.

User group: [redacted]
Group administrator: [redacted]

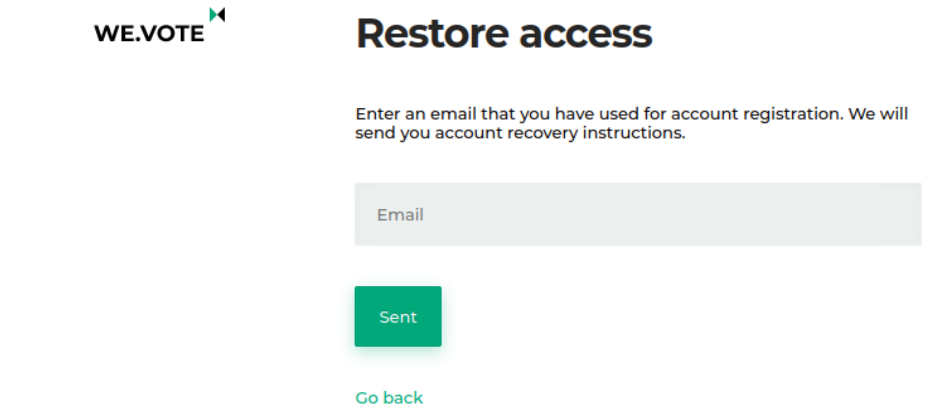
WE have built WE.VOTE using modern cryptography and blockchain technology in a way that gives our users an opportunity to vote, with no one (us included) able to forge your vote or corrupt the decision being made.

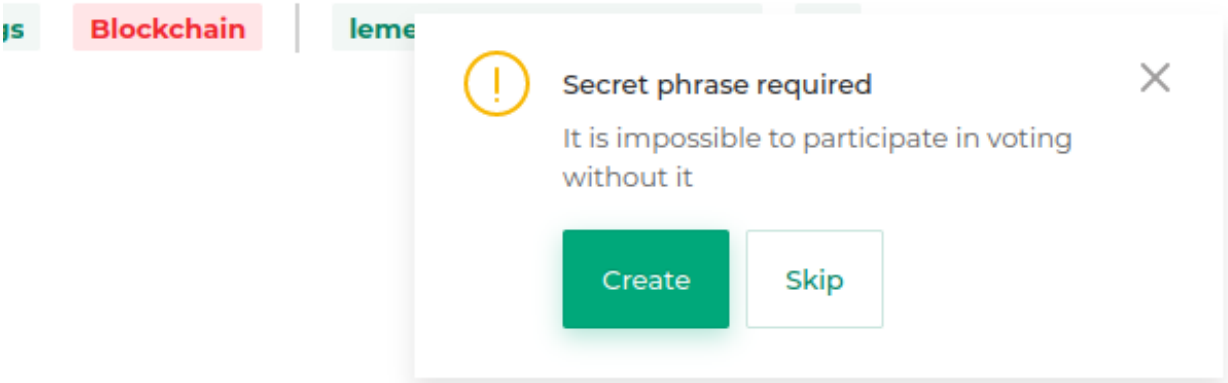
Sign-up or sign-in using your Waves Enterprise account credentials to participate in e-voting.

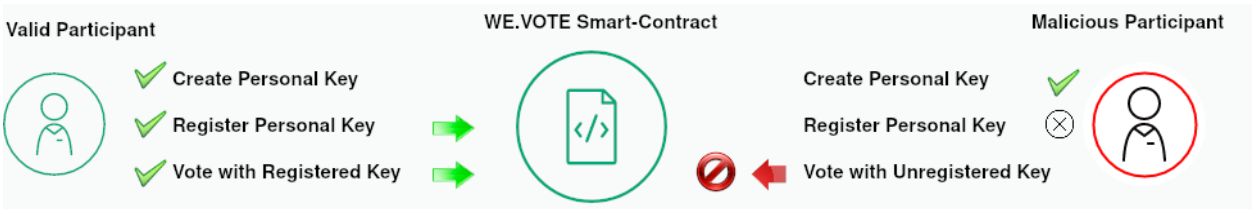
Please note, that beside account registration it is required to create and store secret seed-phrase. At poll start your unique key will be saved at poll's smart-contract. If you'd require seed-phrase reset, your key will be updated as well and your vote, signed with this new key will be rejected.

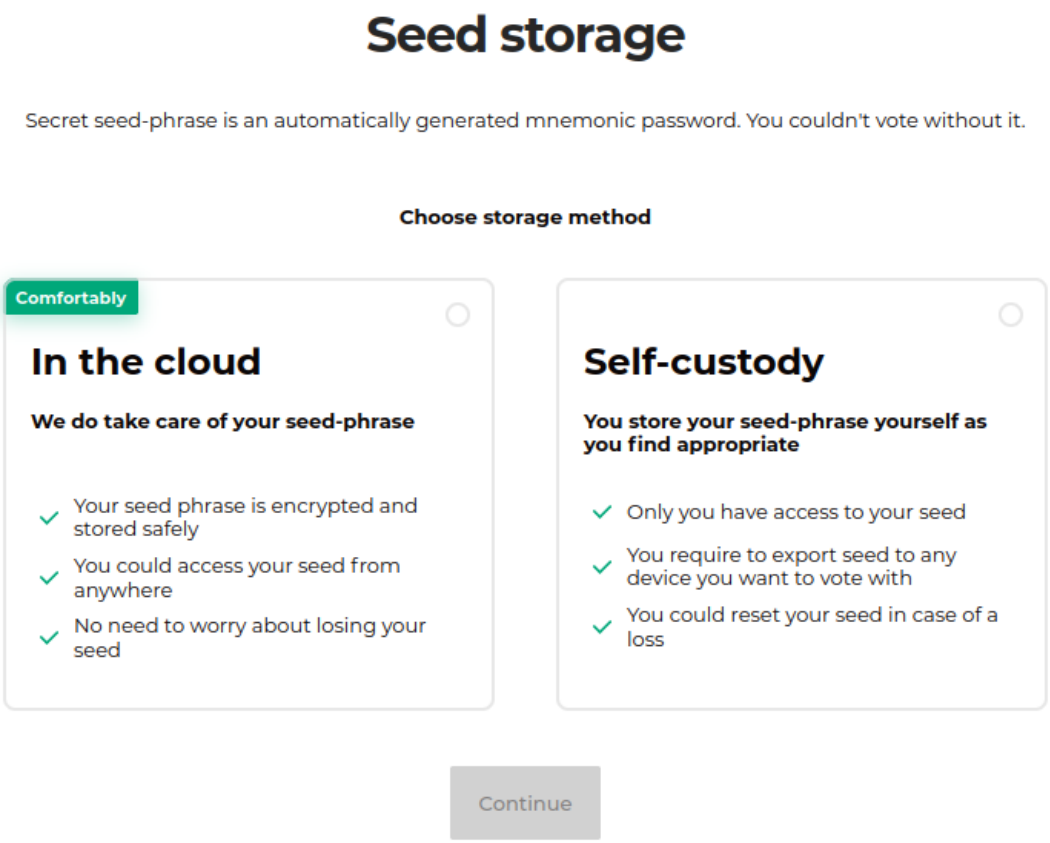
Best regards,
team Waves Enterprise.

Follow the news on social networks:


WE.VOTE
Restore access
Enter an email that you have used for account registration. We will send you account recovery instructions.
Email
Sent
Go back


Blockchain
Secret phrase required
It is impossible to participate in voting without it
Create
Skip


Valid Participant
WE.VOTE Smart-Contract
Malicious Participant
Create Personal Key
Register Personal Key
Vote with Registered Key
Create Personal Key
Register Personal Key
Vote with Unregistered Key


Seed storage
Secret seed-phrase is an automatically generated mnemonic password. You couldn't vote without it.
Choose storage method
Comfortably
In the cloud
We do take care of your seed-phrase
Your seed phrase is encrypted and stored safely
You could access your seed from anywhere
No need to worry about losing your seed
Self-custody
You store your seed-phrase yourself as you find appropriate
Only you have access to your seed
You require to export seed to any device you want to vote with
You could reset your seed in case of a loss
Continue

необходимо самостоятельно перенести закрытый ключ на новое устройство. Для этого и предназначена seedфраза, которая вводится при входе в аккаунт пользователя на другом устройстве и генерирует закрытый ключ.

Смена и сброс пароля при самостоятельном хранении seedфразы также имеют свои особенности. При штатной смене пароля, когда мы попросим ввести старый и новый пароль, приложение локально перешифрует ключ новым паролем и вы сможете продолжить работу. При этом, на других устройствах, куда вы уже перенесли ваш ключ, перешифрования не произойдет: перенести ключ на это устройство при помощи seedфразы потребуется повторно.

Если вы забыли пароль и вам необходимо сбросить его, мы поможем это сделать, и вы восстановите доступ к своему личному кабинету. Но при этом ключ на вашем устройстве будет зашифрован старым утерянным паролем, и использовать его будет нельзя: WE.Vote попросит ввести секретную фразу, чтобы получить из нее ключ заново, зашифровать новым паролем и сохранить.

Поскольку самостоятельное хранение имеет много осложняющих факторов, WE.Vote предоставляет альтернативный, не менее безопасный и надежный способ **хранение seedфразы в облачном хранилище сервиса**. При выборе этого варианта ваш ключ создается выделенным сервисом хранения ключей.

Созданная seedфраза привязывается к вашей учетной записи и хранится в облачном сервисе в зашифрованном виде. При отправке голоса, ключ будет шифроваться локально на вашем устройстве, а затем подписываться на сервисе хранения ключей. Таким образом, ваш ключ не будет передаваться по сети в открытом виде и, соответственно, не может быть похищен в ходе передачи.

Создание ключа происходит моментально после выбора метода хранения ключа в облачном хранилище. У вас не возникнет никаких сложностей с хранением ключа или его переносом на другие устройства: он будет доступен из любого браузера с любого устройства, его невозможно забыть или потерять. Сброс или смена пароля так же никоим образом не затрагивают доступность ключа: все это WE.Vote берет на себя.

После создания вашей учетной записи и секретного ключа вы можете начать пользоваться сервисом.

ГЛАВА 6

Роли пользователей сервиса

Пользователи WE.Vote могут иметь две роли: **Администратор** или **Участник**.

Администраторы имеют следующие полномочия:

- редактировать название и описание группы;
- добавлять и удалять участников;
- создавать и запускать голосования;
- назначать Администраторами других участников;
- пополнять баланс группы (подробнее см. раздел «Оплата голосований и баланс»).

Администратор может просматривать все голосования организации, даже если он не участвует в них.

Первый пользователь, создавший учетную запись в системе WE.Vote и добавивший организацию, автоматически назначается **Администратором** в рабочем пространстве организации. В дальнейшем он может назначить других пользователей администраторами в окне Участники для более эффективного управления голосованиями.

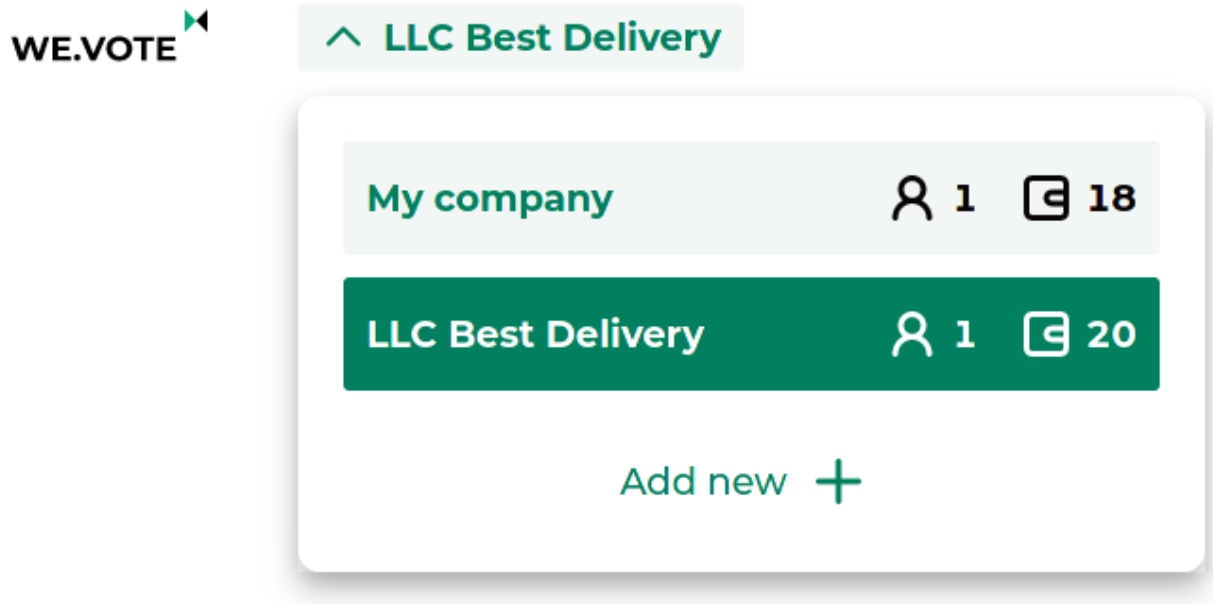
Участники имеют право участвовать в голосованиях при условии подтверждения учетной записи (подробнее см. раздел *Неподтвержденные участники*). **Участники** не могут просматривать или пополнять баланс организации или голосования, в которых они не участвуют.

ГЛАВА 7

Администратору

7.1 Подготовка голосования

7.1.1 Организации



Для организации, от имени которой вы планируете проводить голосования на WE.Vote, мы создаем выделенное рабочее пространство. В его пределах вы сможете управлять учетными записями своих коллег, настраивать группы участников и запускать голосования.

Если вы одновременно организуете голосования в нескольких компаниях, вы можете добавить на сервис новую организацию. Мы также создадим для нее полностью изолированное пространство со своими

пользователями, голосованиями и балансом.

Чтобы пользоваться сервисом WE.Vote, пополните баланс бюллетеней. Бюллетени расходуются при проведении голосований: к примеру, чтобы запустить голосование на 10 участников, баланс должен составлять не менее 10 бюллетеней. При старте голосования необходимая сумма бюллетеней на Вашем балансе замораживается. Она будет списана, если голосование завершится без какихлибо сбоев со стороны сервиса. Каждый новый пользователь имеет возможность опробовать функциональность сервиса, для чего мы начисляем 20 бесплатных бюллетеней.

Для пополнения баланса нажмите на ссылку Пополнить баланс, которая находится в разделе меню **Баланс**. В открывшемся окне выберите подходящий вам тариф и способ оплаты. Каждый пакет бюллетеней имеет установленный срок действия после покупки. Запускаемые вами голосования должны полностью уложиться в срок действия приобретенного пакета. Помимо фиксированных пакетов, вы можете обговорить индивидуальные условия использования сервиса вашей организацией. Для этого поставьте флажок **Корпоративный**: при нажатии кнопки Отправить запрос вы будете перенаправлены на форму обратной связи с Waves Enterprise.

Пополнять баланс могут только **Администраторы** организации. После выбора тарифа и доступного способа оплаты вы будете перенаправлены на страницу оплаты, где вам будет необходимо выбрать предпочтительный источник оплаты в левой части окна и ввести необходимые данные. Голоса будут начислены на счет вашей учетной записи после проведения оплаты. История ваших платежей и их статус, а также факты списания голосов с баланса доступны в разделе меню **Баланс** / **Посмотреть всю историю**.

7.1.2 Приглашение участников

Для приглашения выбранных вами участников голосования загрузите их email в систему. Мы отправим им приглашения к регистрации в сервисе WE.Vote. Ваши коллеги должны будут создать и подтвердить учетную запись, выбрать метод хранения своего секретного ключа и создать ключ.

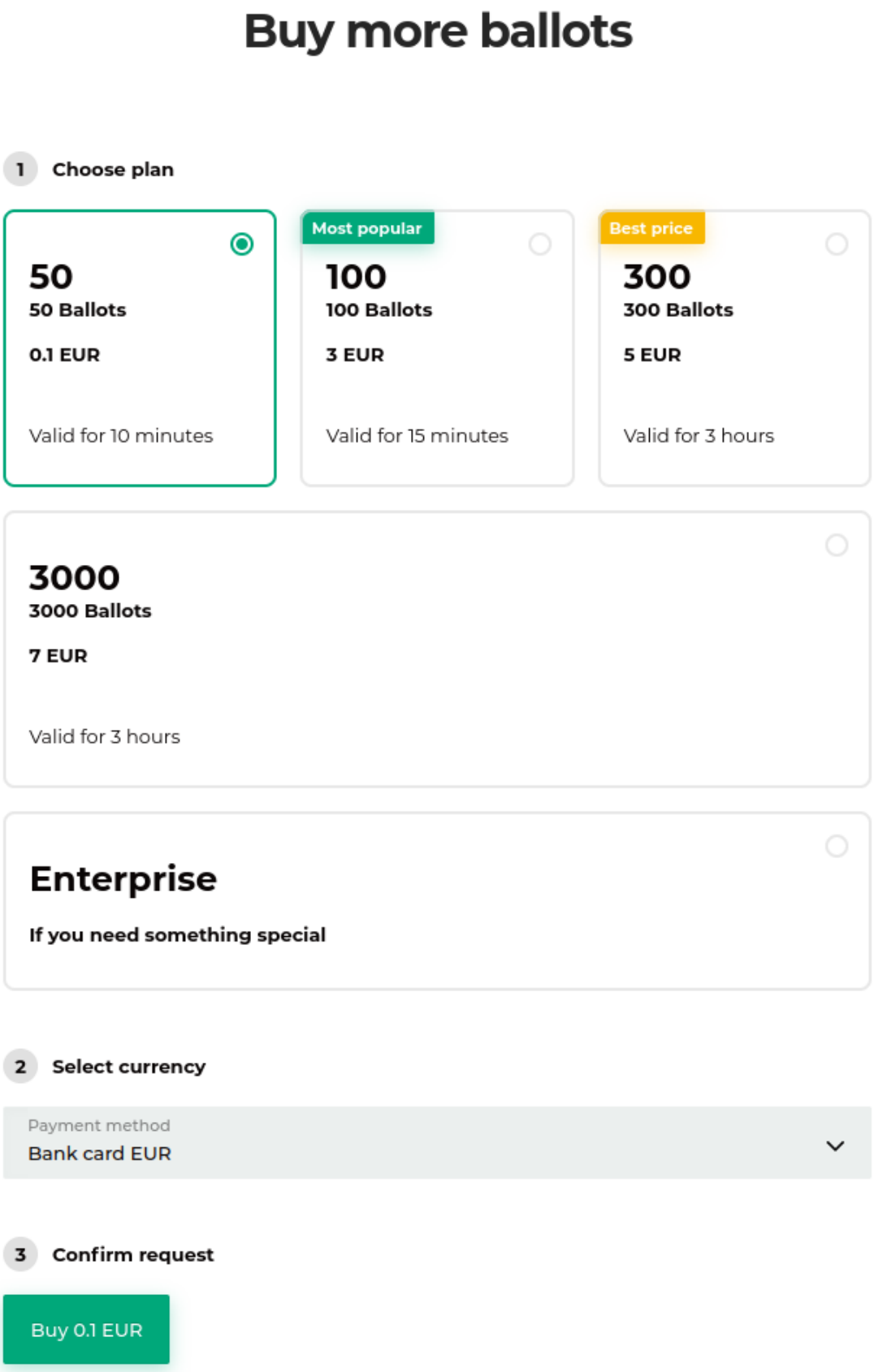
Как Администратор голосования, вы можете видеть кто из приглашенных участников успешно зарегистрировался и может принять участие в голосовании. Если у когото из участников возникли сложности с регистрацией, вы можете отправить ему приглашение повторно, нажав кнопку **Пригласить повторно** на вкладке **Участники**. Также вы можете повторно отправить приглашения участникам при создании голосования, нажав на кнопку **Пригласить всех повторно**.

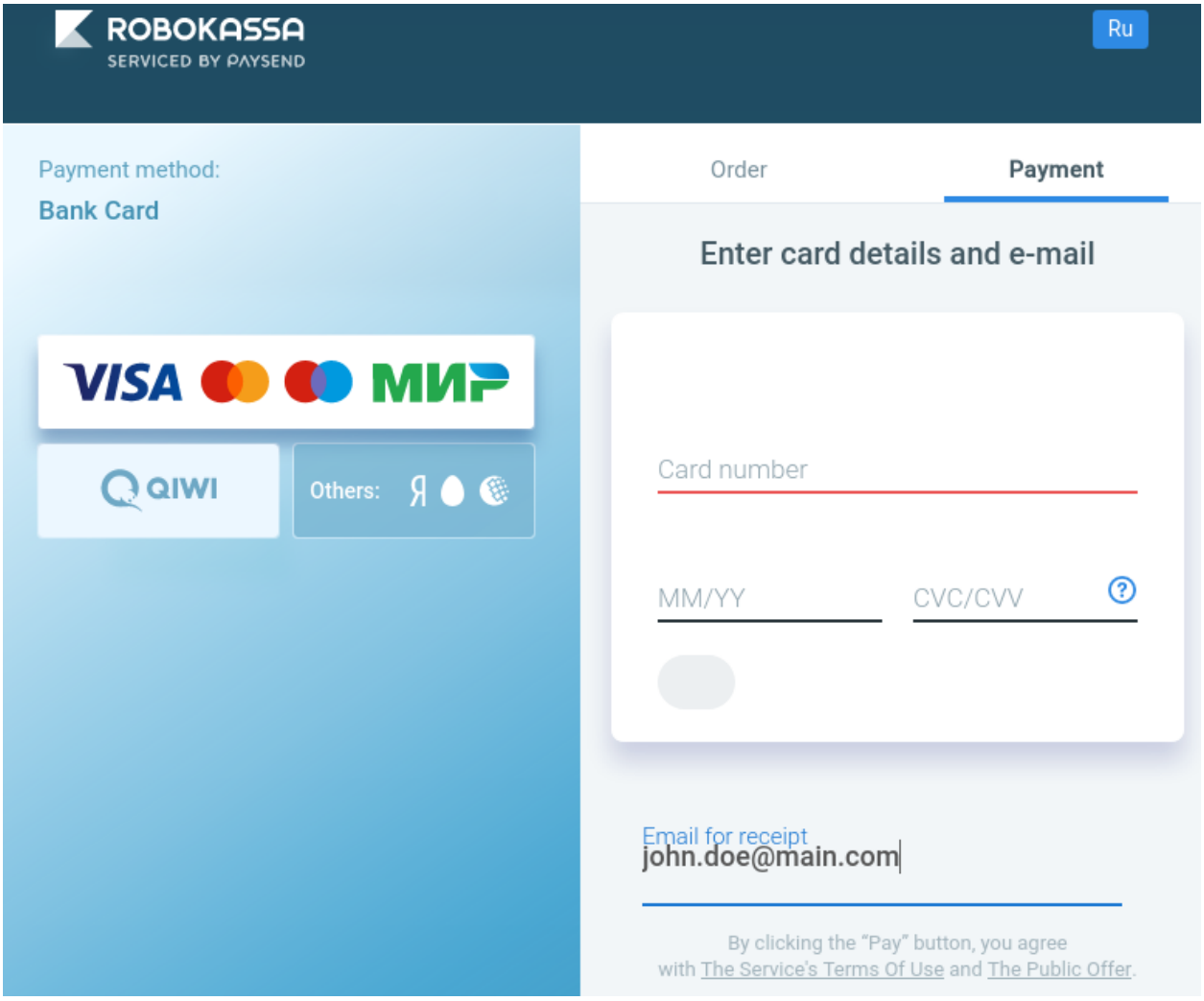
Вы можете добавлять пользователей, указывая из их email через запятую в форме добавления пользователей. Но более удобной является возможность загрузить пользователей в виде таблицы формата Microsoft Excel или файла CSV. Шаблон для создания файла доступен в форме добавления пользователей.

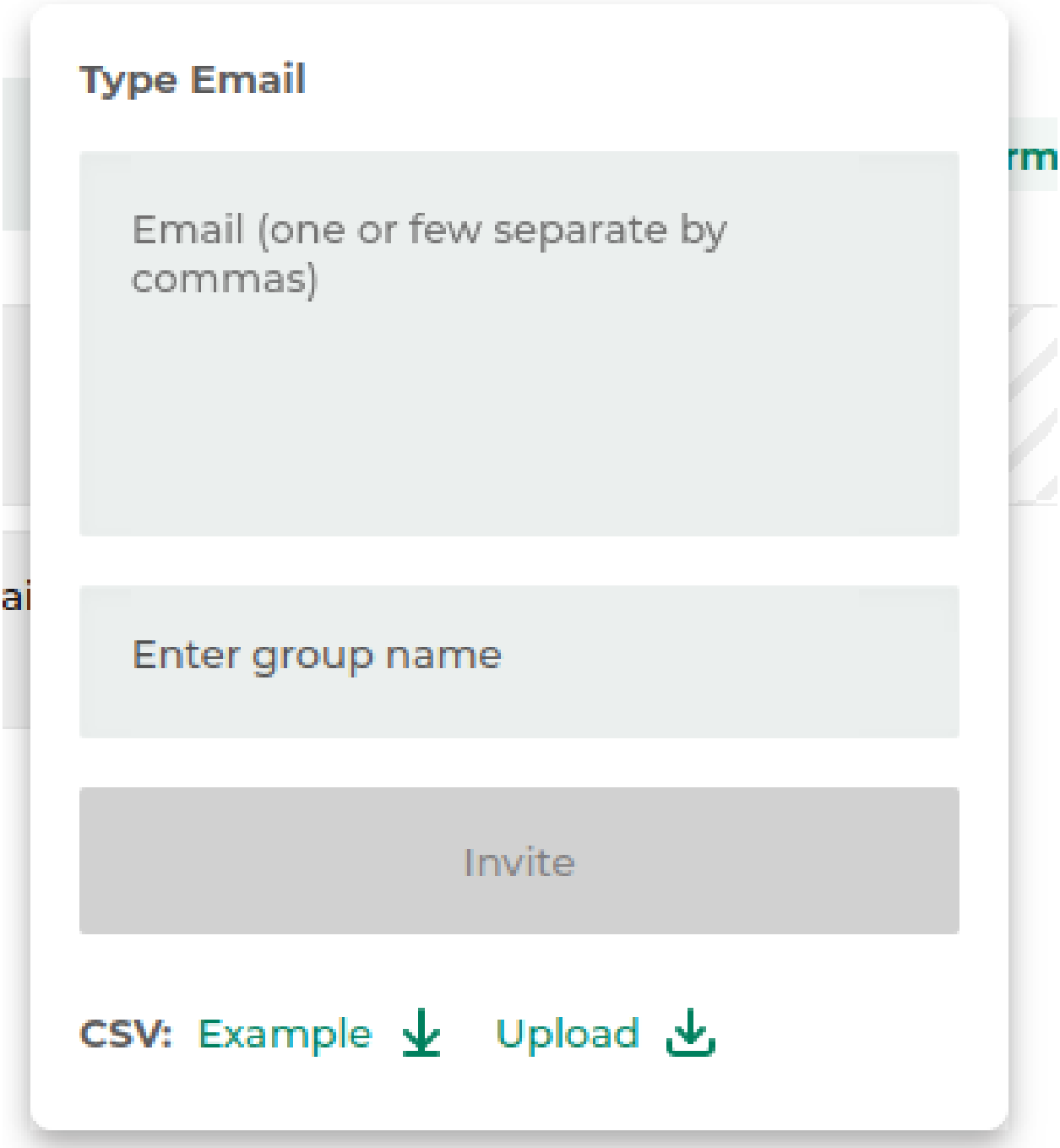
После загрузки вашего списка участников вы увидите сообщение о результатах загрузки. Если вы неправильно заполнили список, в сообщении будет указана причина. В этом случае исправьте ошибочные записи и повторите загрузку.

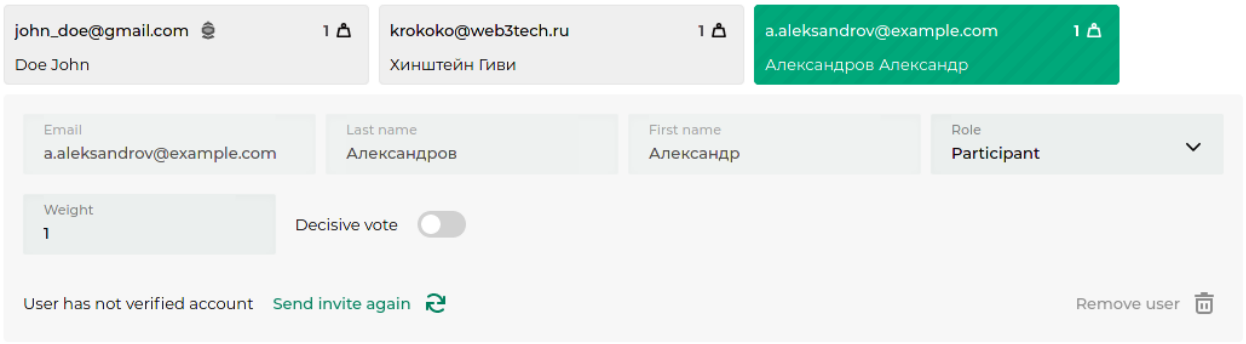
На карточках добавленных пользователей вы можете назначить дополнительных Администраторов для помощи в организации голосований или самостоятельно настроить параметры пользователей право решающего голоса и вес. Эти параметры будут использованы в соответствующих видах голосований.

Если ктото из ваших коллег не заметил приглашение и не зарегистрировался на сервисе, это будет заметно в списке участников организации: карточка неподтвержденного пользователя заштрихована. В этом случае вы можете отправить пользователю повторное приглашение.


Buy more ballots
1 Choose plan
50
50 Ballots
0.1 EUR
Valid for 10 minutes
Most popular
100
100 Ballots
3 EUR
Valid for 15 minutes
Best price
300
300 Ballots
5 EUR
Valid for 3 hours
3000
3000 Ballots
7 EUR
Valid for 3 hours
Enterprise
If you need something special
2 Select currency
Payment method
Bank card EUR
3 Confirm request
Buy 0.1 EUR


ROBOKASSA
SERVICED BY PAYSEND
Ru
Payment method:
Bank Card
VISA
МИР
QIWI
Others:
Order
Payment
Enter card details and e-mail
Card number
MM/YY
CVC/CVV
Email for receipt
john.doe@main.com
By clicking the "Pay" button, you agree
with The Service's Terms Of Use and The Public Offer.


Type Email
Email (one or few separate by commas)
Enter group name
Invite
CSV: Example
Upload



7.1.3 Неподтвержденные участники

Не все приглашенные пройдут регистрацию сразу после приглашения. Ктото может принять приглашение за спам и не на него внимания, поэтому рекомендуем проинформировать ваших коллег о планируемом голосовании на WE.Vote. Пока голосование находится в статусе черновика и не опубликовано в блокчейне, все приглашенные в него пользователи могут успеть пройти регистрацию. Их статус автоматически изменится на **Активирован**, и при публикации голосования они смогут участвовать в нем. Однако те, кто не пройдет регистрации до этого момента, не смогут отправить свой голос, поскольку их публичные ключи не будут зарегистрированы в смартконтракте сервиса голосования.

Пользователи WE.Vote, хранящие свои ключи в облачном хранилище, не могут их потерять. При самостоятельном хранении, пользователь может по той или иной причине утратить доступ к своему ключу. В этом случае, даже пользователю, прошедшему регистрацию, придется воспользоваться функцией сброса секретной фразы, и он не сможет принять участия в уже запущеных или опубликованных голосованиях. После обновления секретного ключа пользователь вновь получит возможность участвовать в будущих голосованиях, но текущие активные голосования будут для него недоступны.

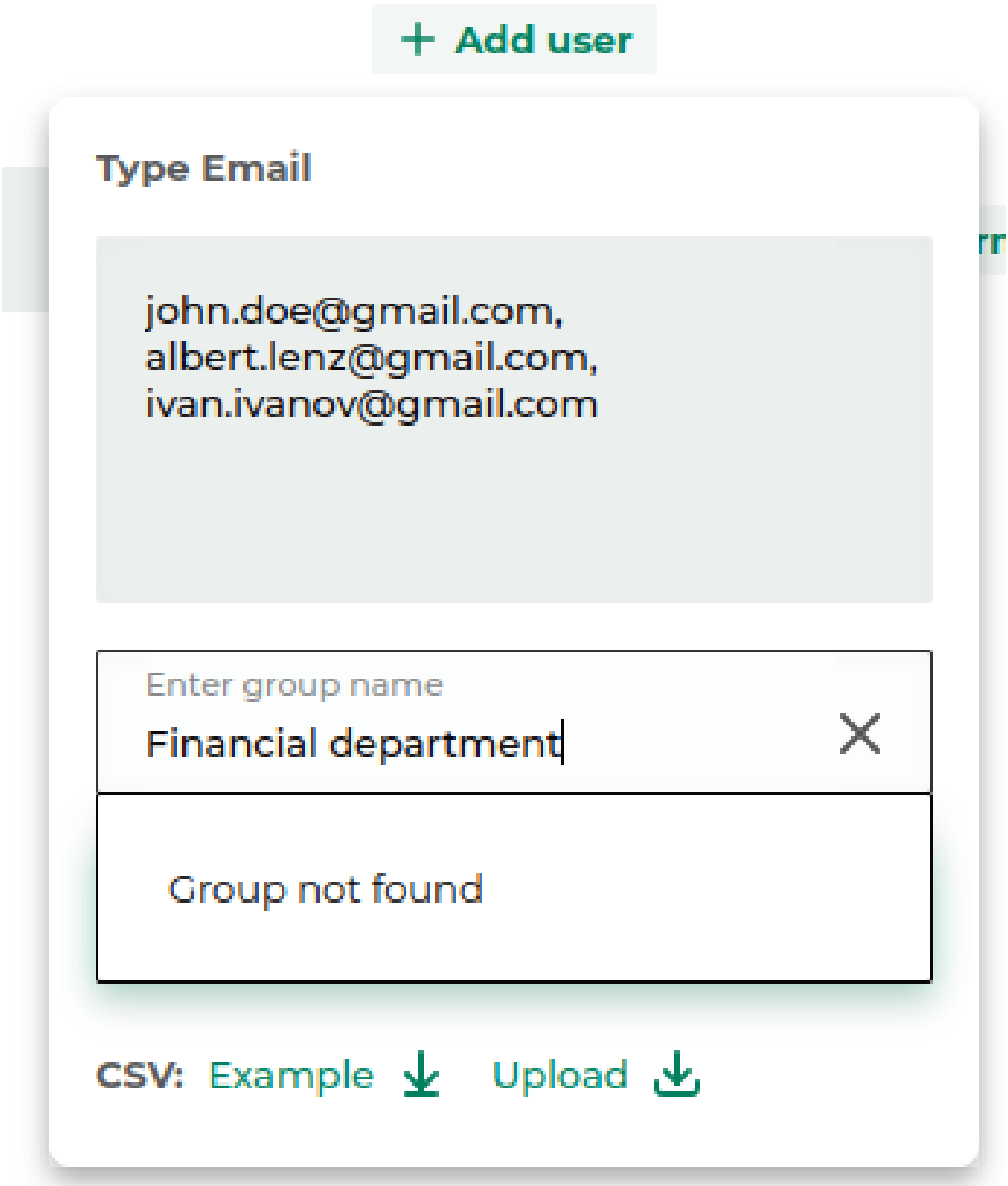
7.1.4 Управление группами участников

Если вы планируете организовывать голосования среди небольшого числа людей, достаточно пригласить участников голосования на сервис (подробнее см. в разделе «Приглашение участников»). Однако при работе с большим количеством пользователей вы можете более эффективно управлять процессом голосования, разделив их на группы. Это позволит вам структурировать список участников в зависимости от ваших потребностей: распределить участников по отделам или подразделениям организации, их местонахождению, и т.д. В дальнейшем вы сможете более оперативно создавать разные голосования для различных групп пользователей и управлять составом групп.

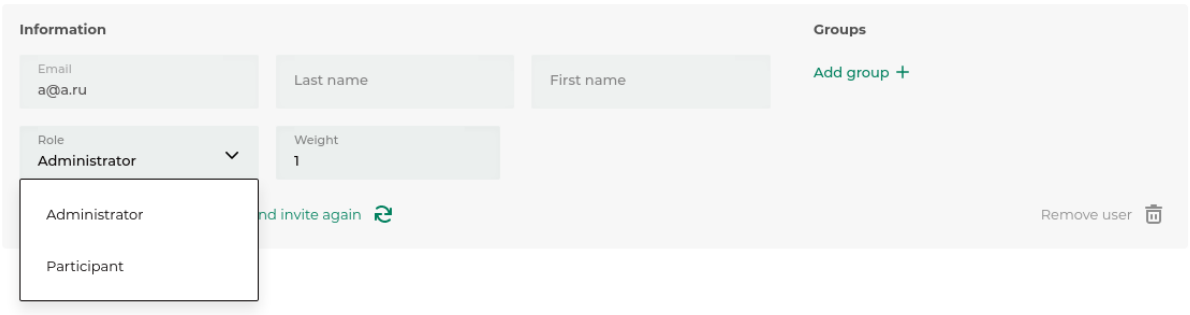
Группа создается при приглашении участников. Введите список email участников создаваемой группы через запятую или загрузите CSV/Excelфайл с этим списком, а затем впишите название группы в соответствующем поле.

Чтобы добавить участников к уже существующей группе, выберите необходимую группу из выпадающего списка.

При создании голосования, вы можете выбрать группы участников, для которых оно предназначено.


+ Add user
Type Email
john.doe@gmail.com,
albert.lenz@gmail.com,
ivan.ivanov@gmail.com
Enter group name
Financial department
Group not found
CSV: Example
Upload

7.1.5 Распределение ролей



Как администратор, вы можете назначить любого участника из вашей организации Администратором для помощи в организации голосования. Для этого перейдите в раздел Участники, нажмите на карточку участника и выберите пункт **Администратор** в выпадающем меню **Роль**. Сразу после этого участник получит права администратора.

Чтобы вернуть администратору роль участника нажмите на его карточку и выберите пункт **Участник** в выпадающем меню **Роль**.

7.2 Создание голосования

Чтобы создать голосование, нажмите на кнопку **Создать новое** в основном окне клиента. Обратите внимание, что создание голосования не поддерживается при использовании клиента на устройстве с маленькой диагональю экрана. В таком случае, кнопка будет погашена.

7.2.1 Общие настройки

1. В открывшемся окне введите предпочтительное название голосования.

2. Затем установите даты и время начала и окончания голосования.

Важно: Обратите внимание, что время начала голосования должно быть больше текущего времени, поскольку сервису требуется создать смартконтракт вашего голосования, а затем произвести распределенную генерацию ключа для шифрования бюллетеней (*Криптографические алгоритмы*).

---

3. Выберите тип голосования в выпадающем списке:

Обычное (мажоритарное)

Базовый вариант голосования. У каждого участника один голос, он может отдать его за один из предложенных вариантов по каждому из рассматриваемых вопросов повестки голосования. Итоги определяются путем подсчета суммы отданых голосов за каждый вариант, побеждает тот, который набрал большинство голосов.

Весовое (взвешенное)

Вариант голосования, который подходит для принятия решений в организации, где сила голоса ее членов определяется долей участия/владения например, общества с ограниченной ответственностью или товарищества собственников жилья. Сила голоса (его вес) задается до начала голосования. Побеждает вариант, за который проголосовали участники с наибольшим суммарным весом.

С правом решающего голоса

Голосование с решающим голосом необходимо для принятия решений небольшим числом участников, когда высок шанс равного разделения голосов между вариантами, что приводит к блокированию решения. В этом случае одному из участников голосования, например председателю совета директоров компании передается право решающего голоса. Это право реализуется только в случае «ничьей» побеждает вариант за который проголосовал председатель. В остальных случаях его голос имеет такую же силу как и голоса остальных членов совета директоров.

Множественный выбор

При этом варианте голосования каждый участник может выбрать несколько вариантов ответа на каждый вопрос.

4. Настройте конфиденциальность голосования. Для этого нажмите на тумблер **Открытое голосование**, если планируется голосование с предоставлением информации о голосах всех участников. В этом случае, голоса участников не шифруются, и по окончании голосования WE.Vote предоставляет подробный отчет о выборе каждого участника.

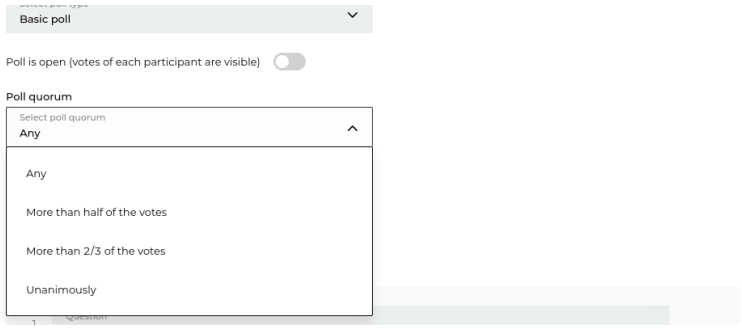
Примечание: При выборе опции Открытое голосование, ваше голосование проводится в соответствии со ст. 37 п. 10 Федерального закона от 08.02.1998 N 14ФЗ «Об обществах с ограниченной ответственностью».

---

5. Настройте кворум голосования:

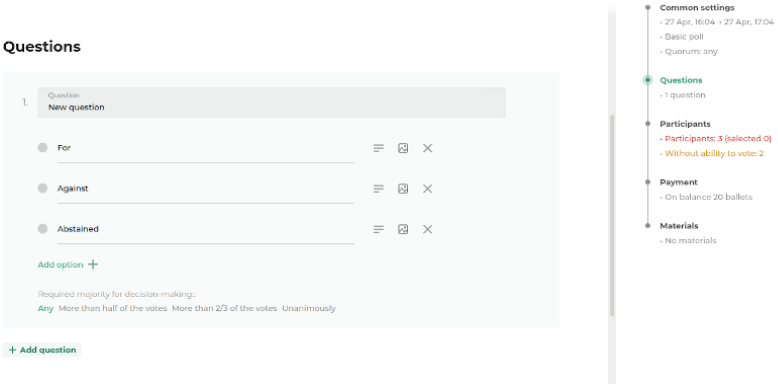
- **Не требуется** кворум отключен, голосование считается состоявшимся при любом числе проголосовавших.
- **Более половины** голосование считается состоявшимся при голосовании $> 50\%$ участников.
- **Более двух третей** голосование считается состоявшимся при голосовании $> 2/3$ участников.
- **Единогласно** голосование считается состоявшимся только при стопроцентной явке зарегистрированных участников.

6. Настройте возможность остановки голосования до его окончания. Для этого нажмите на тумблер **Голосование может быть остановлено до даты его окончания**. В этом случае, администратор может остановить голосование в любой момент после его начала, итоги подводятся в соответствии с распределением голосов до остановки голосования. Если данная опция не выбрана, голосование продолжается до установленного момента его окончания.



7.2.2 Добавление вопросов

Прокрутите страницу ниже, чтобы перейти к карточке добавления вопроса. Чтобы создать новую карточку, нажмите на кнопку **Добавить вопрос**.



В карточке вопроса:

1. Введите текст вопроса в поле **Вопрос**;
2. Добавьте варианты ответов.
3. В случае, если вы выбрали опцию **Множественный выбор**, настройте количество возможных вариантов ответа на вопрос.
4. Установите необходимое большинство для принятия решения по вопросу. Опции в карточке идентичны опциям при настройке кворума голосования.

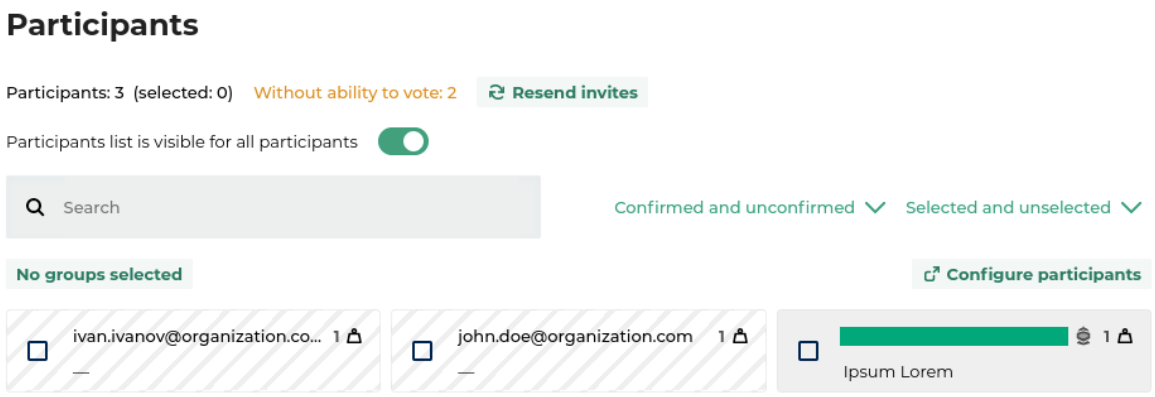
7.2.3 Добавление участников

Перейдите к разделу **Участники**. Чтобы добавить отдельных участников для вашего голосования, поставьте флажки на их карточках. Вы можете выполнять поиск и фильтрацию списка участников при помощи строки поиска и фильтров раздела.

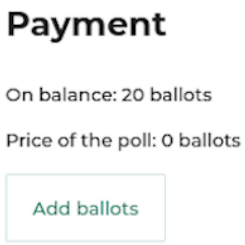
Чтобы добавить ранее настроенную группу участников, нажмите на кнопку **Группы** не выбраны и поставьте флажок напротив группы. Участники, входящие в группу, будут выделены в общем списке.

Если участник, добавленный вами в организацию, не прошел регистрацию в системе WE.Vote, его карточка будет заштрихована серым цветом. Участники, не подтвердившие свои учетные записи в системе до начала голосования, не смогут принять в нем участие (см. раздел *Неподтвержденные участники*).

Чтобы разослать пригласительные письма неподтвержденным участникам, нажмите на кнопку **Разослать повторно**.



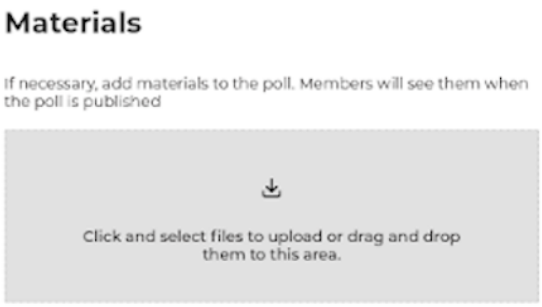
7.2.4 Оплата голосования



В разделе **Оплата** вы увидите текущий баланс вашей учетной записи WE.Vote, а также стоимость голосования количество бюллетеней, необходимое для его проведения. Если бюллетеней на вашем балансе недостаточно для проведения голосования, нажмите кнопку **Пополнить баланс** и приобретите дополнительный пакет бюллетеней.

7.2.5 Загрузка дополнительных материалов

В разделе **Материалы** вы можете прикрепить поясняющие файлы или дополнительные документы для вашего голосования. Участники смогут ознакомиться с ними, когда голосование будет опубликовано. Загруженные материалы доступны для скачивания до начала голосования, а также в его процессе.



7.2.6 Публикация голосования

Для публикации голосования нажмите кнопку Опубликовать в правой части экрана. Чтобы сохранить установленные вами параметры голосования без его публикации, нажмите кнопку **Сохранить черновик**.

> **Внимание:** Публикация голосования необратимое действие. После публикации изменить параметры голосования невозможно.

В выпадающем меню вы можете **Дублировать голосование** для создания копии его черновика, а также **Удалить** его.

7.2.7 Запуск голосования и работа с его результатами

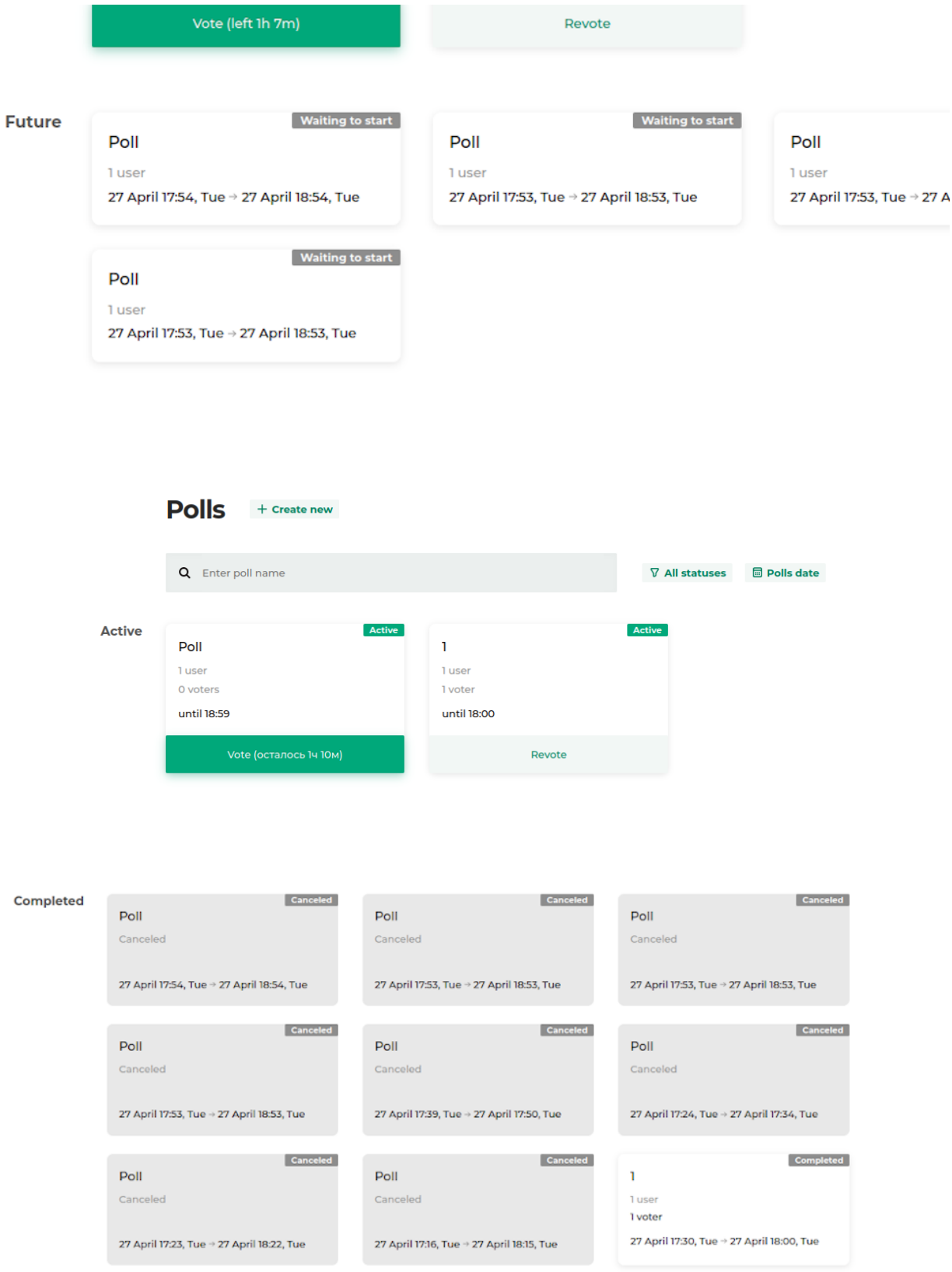
Опубликуйте созданное вами голосование. После публикации изменить его параметры будет невозможно.

До времени старта опубликованное голосование будет находиться в разделе **Будущие** на главной странице сервиса. Его участники смогут ознакомиться с вопросами и дополнительными материалами, однако не смогут голосовать до его начала.

Голосование стартует автоматически в назначенное вами время. После старта оно переместится в раздел **Активные** на главной странице сервиса.

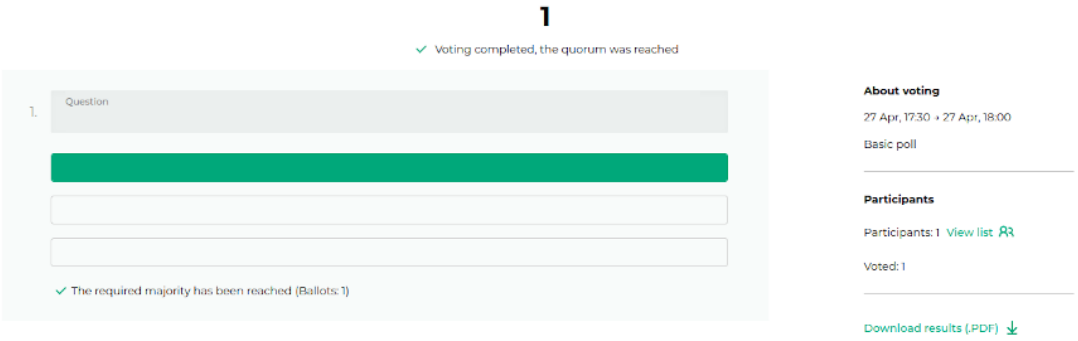
По завершении голосование попадает в раздел **Завершенные** на главной странице сервиса.

Если голосование по какойлибо причине не состоится (отсутствие кворума, неявка участников или сбой сервиса), голосование отменяется и также попадает в **Завершенные** с указанием причины отмены.


Vote (left 1h 7m)
Revote
Future
Waiting to start
Poll
1 user
27 April 17:54, Tue → 27 April 18:54, Tue
Waiting to start
Poll
1 user
27 April 17:53, Tue → 27 April 18:53, Tue
Poll
1 user
27 April 17:53, Tue → 27 A
Waiting to start
Poll
1 user
27 April 17:53, Tue → 27 April 18:53, Tue
Polls
+ Create new
Enter poll name
All statuses
Polls date
Active
Active
Poll
1 user
0 voters
until 18:59
Vote (осталось 1ч 10м)
Active
1
1 user
1 voter
until 18:00
Revote
Completed
Canceled
Poll
Canceled
27 April 17:54, Tue → 27 April 18:54, Tue
Canceled
Poll
Canceled
27 April 17:53, Tue → 27 April 18:53, Tue
Canceled
Poll
Canceled
27 April 17:53, Tue → 27 April 18:53, Tue
Canceled
Poll
Canceled
27 April 17:53, Tue → 27 April 18:53, Tue
Canceled
Poll
Canceled
27 April 17:39, Tue → 27 April 17:50, Tue
Canceled
Poll
Canceled
27 April 17:24, Tue → 27 April 17:34, Tue
Canceled
Poll
Canceled
27 April 17:23, Tue → 27 April 18:22, Tue
Canceled
Poll
Canceled
27 April 17:16, Tue → 27 April 18:15, Tue
Completed
1
1 user
1 voter
27 April 17:30, Tue → 27 April 18:00, Tue

Нажав на карточку завершенного голосования, вы можете просмотреть свои варианты ответа и параметры проведенного голосования и скачать отчет о голосовании в PDF. Если выбрано открытое голосование, вы также можете просмотреть ответы всех участников голосования.

Как Администратор, вы можете дублировать проведенное голосование для перезапуска.

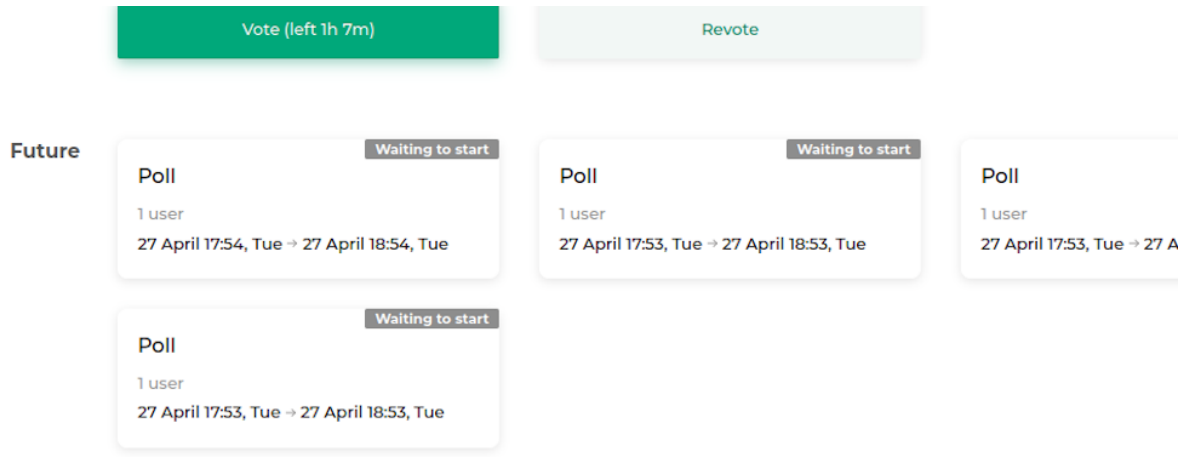


ГЛАВА 8

Участнику

Как участник, вы можете зарегистрироваться в сервисе WE.Vote по приглашению администратора, добавившего вас в созданную им организацию или создавшего голосование с вашим участием. Для получения дополнительной информации о процессе регистрации см. раздел **Регистрация в сервисе**.

8.1 Участие в голосовании



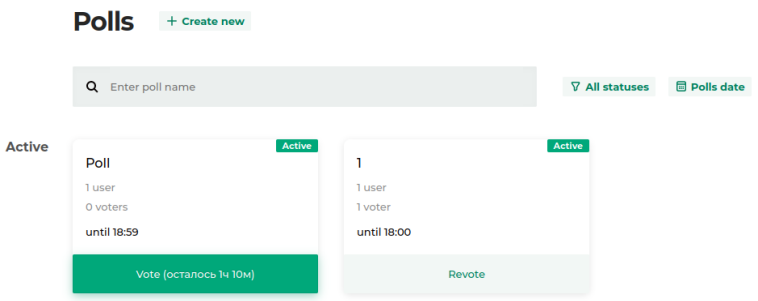
В основном окне сервиса вам доступны все голосования с вашим участием:

- **Будущие** голосования, запланированные и созданные администратором.
- **Активные** голосования, которые проводятся в настоящее время.
- **Завершенные** голосования, проведение которых завершилось по истечении запланированного периода, а также отмененные голосования.

До времени старта опубликованное голосование будет находиться в разделе **Будущие**. Вы можете ознакомиться с вопросами и дополнительными материалами голосования, однако не сможете проголосовать до его начала.

Голосование стартует автоматически в назначенное вами время. После старта оно переместится в раздел **Активные**.

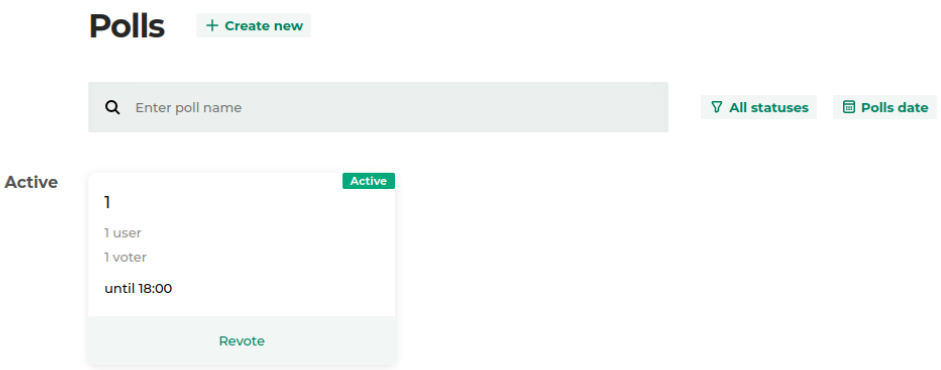
Участники могут голосовать в активном голосовании до момента его завершения. На карточке голосования отображается оставшееся время его проведения.



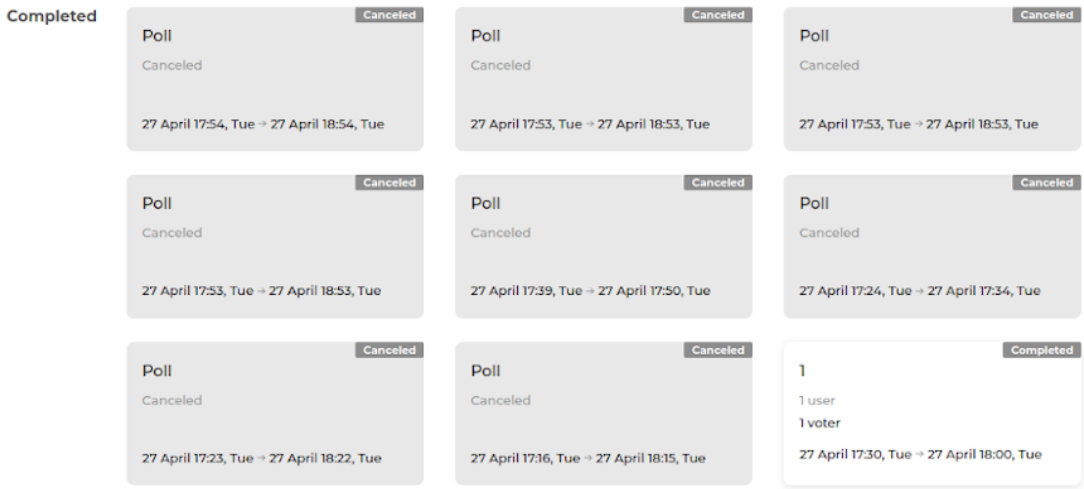
Для того, чтобы отдать свой голос, нажмите на карточку активного голосования и перейдите к списку вопросов. Выберите ваши варианты ответа на каждый из них и нажмите кнопку **Проголосовать**. При длительном бездействии сервиса, для доступа к этой кнопке может потребоваться ввод пароля от вашего аккаунта в целях исключения доступа к голосованию посторонних лиц.

Затем ваши варианты ответа будут зашифрованы и отправлены в базу данных.

Пока голосование активно, вы можете изменить ваши варианты ответов. Для этого нажмите кнопку **Переголосовать** на карточке голосования, измените варианты ответов и проголосуйте заново.

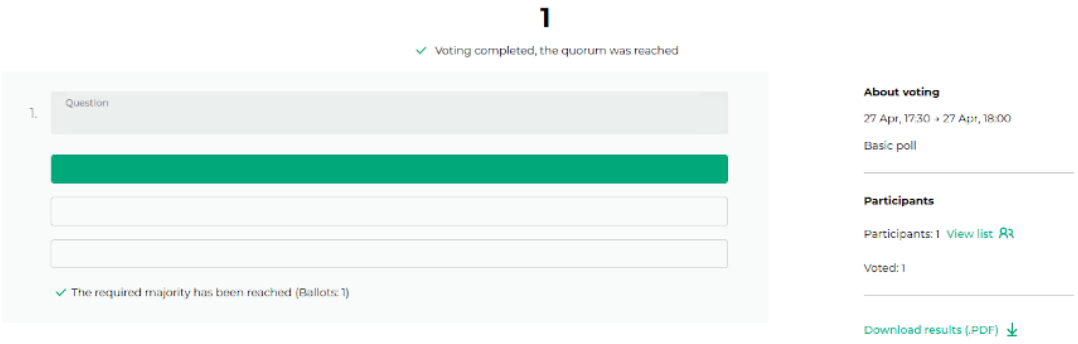


8.1.1 Работа с результатами голосования



По завершении голосование попадает в раздел **Завершенные** на главной странице сервиса. Если голосование по какойлибо причине не состоится, голосование отменяется и также попадает в **Завершенные** с указанием причины отмены.

Нажав на карточку завершенного голосования, вы можете просмотреть свои варианты ответа и параметры проведенного голосования и скачать отчет о голосовании в PDF. Если выбрано открытое голосование, вы также можете просмотреть ответы всех участников голосования.


1
Voting completed, the quorum was reached
1.
Question
The required majority has been reached (Ballots: 1)
About voting
27 Apr, 17:30 - 27 Apr, 18:00
Basic poll
Participants
Participants: 1 View list
Voted: 1
Download results (.PDF)

ГЛАВА 9

Устранение неполадок

9.1 Я не могу опубликовать голосование

Если при создании голосования обнаруживаются несоответствия в заданных вами параметрах, вы не сможете опубликовать голосование.

- Проверьте дату и время начала голосования. Время начала голосования должно быть позднее текущего времени, поскольку сервису требуется время на создание смартконтракта голосования.
- Проверьте количество бюллетеней на счету. Если количество участников больше количества доступных бюллетеней, вы не сможете опубликовать голосование.

9.2 Я не могу проголосовать в активном голосовании

Если вы утратили вашу seedфразу и восстановили доступ в аккаунт, вы не сможете принять участие в голосованиях, активных на момент восстановления аккаунта.

9.3 Голосование завершилось с ошибкой

Ниже приведен перечень ситуаций, которые могут привести к завершению голосования с ошибкой. Конкретная причина ошибки указывается в карточке завершенного голосования.

- Установленный кворум голосования не был набран. Пересмотрите параметры голосования и измените кворум, либо проинформируйте участников о необходимом кворуме. Затем создайте и запустите голосование повторно, продублировав его.
- Не проголосовал ни один из зарегистрированных участников. Создайте голосование заново, продублировав его, и проконтролируйте, что все участники вашего голосования были проинформированы о нем и зарегистрировались.

- Для голосования не зарегистрировался ни один из приглашенных участников. Создайте голосование заново, продублировав его, и проконтролируйте, что все участники вашего голосования были проинформированы о нем и зарегистрировались. Статус регистрации участников досупен в разделе **Участники** клиента.
- Технические неполадки сервиса WE.Vote. Обратитесь в службу технической поддержки Waves Enterprise.

ГЛАВА 10

Архитектура системы

Система WE.Vote основан на блокчейнплатформе Waves Enterprise и представляет собой несколько серверов, развернутых в блокчейнсети.

Система может быть развернута двумя способами:

- в виде нескольких серверов в сети Waves Enterprise Mainnet;
- в виде частной блокчейнсети, состоящей из серверов организации.

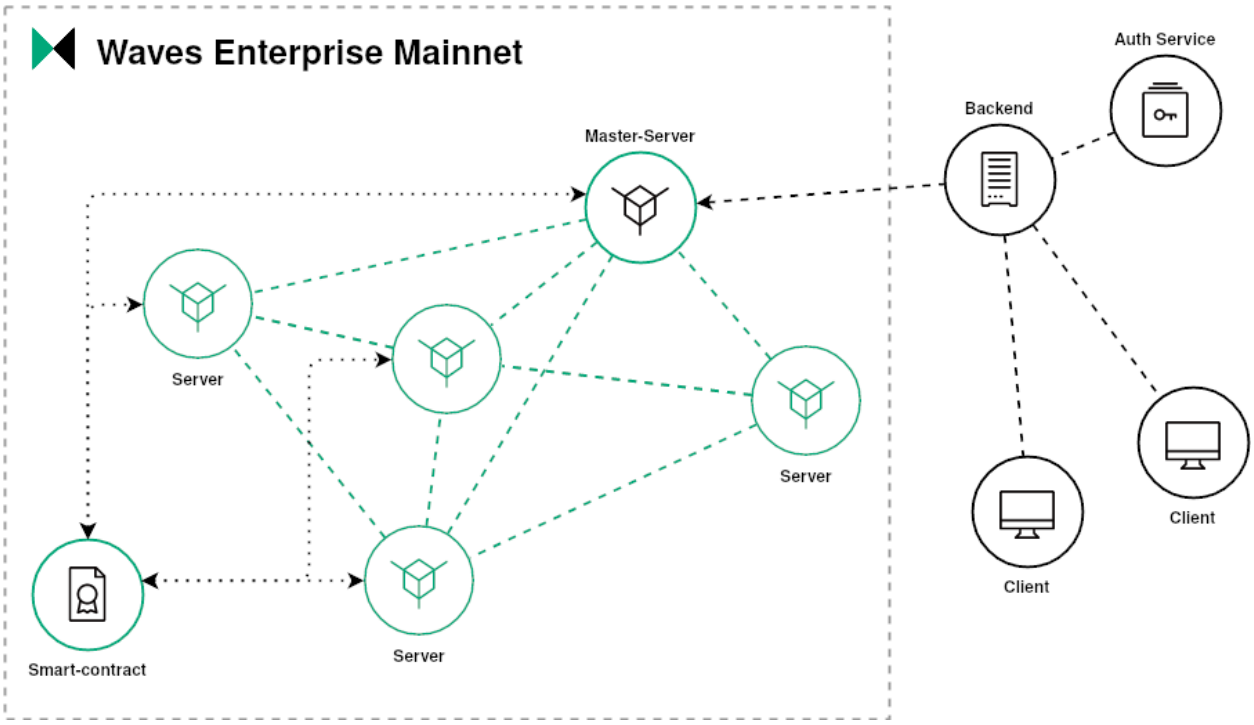


Рис. 1: Архитектура системы WE.Vote

Основные компоненты системы:

1. **Сервер** узел системы, состоящий из следующих элементов:

- **Нода** узел блокчейнсети, обрабатывающий транзакции, формирующий блоки и реализующий алгоритм консенсуса.
- **Криптографический сервис** сервис, участвующий в процессе распределенной генерации главного ключа и производящий частичную расшифровку результатов голосования.

2. **Мастерсервер** главный узел системы, который, помимо функций сервера, осуществляет функционирование системы в целом:

- создание новых голосований;
- мониторинг доступности криптографических сервисов;
- формирование главного публичного ключа голосования;
- необходимость опубликовать результаты голосования.

3. **Смартконтракт онлайнголосования** блокчейнприложение, выполняющее следующие функции:

- хранение правил голосования и списков участников;
- регистрация публичных данных, полученных при распределенной генерации ключа;
- проверка и хранение отправленных голосов и результатов голосования.

4. **Бэкэнд** серверная часть системы, которая:

- обрабатывает запросы клиентской части;
- взаимодействует с мастерсервером;
- хранит конфиденциальные данные, касающиеся голосования.

5. **Клиент** клиентская часть системы, состоящая из следующих компонентов:

- **Клиентское приложение** вебприложение, обеспечивающее взаимодействие пользователя с сервисом.
- **Сервис шифрования** сервис, выполняющий шифрование заполненного бюллетеня на публичной части главного ключа.

ГЛАВА 11

Криптографические алгоритмы

Для обеспечения конфиденциальности передаваемых и обрабатываемых данных, сервис применяет набор современных криптографических алгоритмов.

Общий вид работы криптографических алоритмов сервиса представлен на схеме:

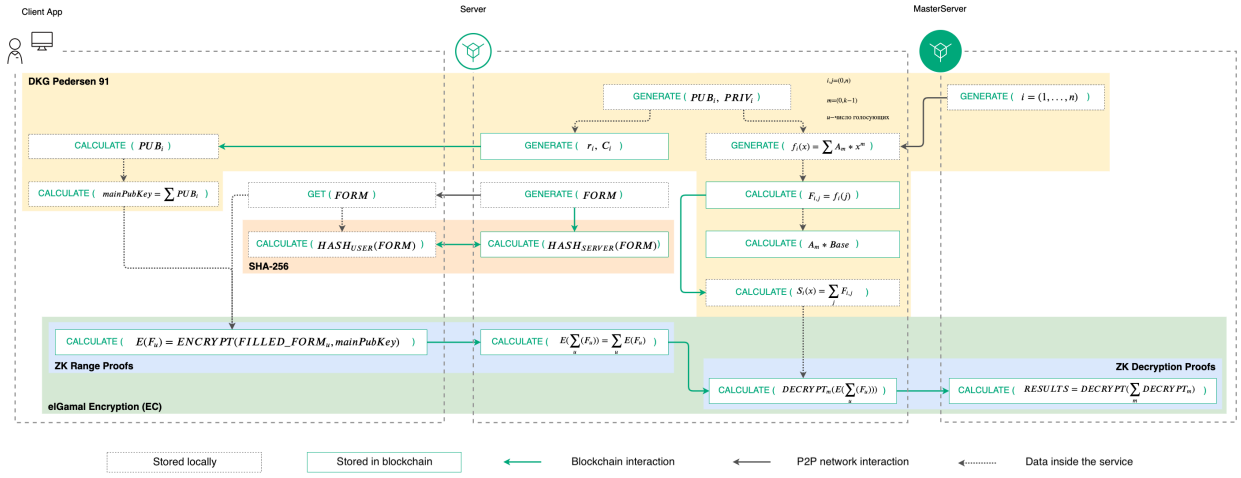


Рис. 1: Порядок работы криптографических алгоритмов

11.1 Генерация ключей

В основе взаимодействия компонентов системы лежит криптографический протокол **MPC (MultiParty Computation)**, который используется для генерации ключевых пар.

Он позволяет нескольким участникам независимо друг от друга производить криптографические вычисления на основе собственных секретных данных, не имея при этом информации о секретных данных друг друга. В процессе вычисления участники не обмениваются секретными данными, независимо генерируя набор приватных ключей для общего публичного ключа. Такой метод позволяет избавиться от единой точки отказа: в собранном виде ключевая пара не существует ни на одном из серверовучастников.

Применяемый протокол MPC использует принцип **«K из N»**, соответствующий схеме разделения секрета Шамира:

- для расшифровки данных не требуется участие всех **N** сторон, участвовавших в процессе шифрования: расшифровка может быть произведена с использованием меньшего порогового количества **K** сторон;
- при этом,**K 1** и менее сторон не имеют возможности расшифровать данные.

Этот принцип позволяет поддерживать работу сервиса даже при нарушении функционирования нескольких серверов системы, при этом обеспечивая высокую степень защиты данных. Каждый из серверовучастников протокола MPC формирует собственные публичный и приватный ключи, а также **общий публичный ключ (MainPublicKey)**, обмениваясь с другими участниками несекретными данными о своих вычислениях при помощи транзакций в блокчейнсети.

Для формирования общего публичного ключа применяется **алгоритм распределенной генерации ключей (Distributed Key Generation, DKG)** за авторством Торбена Педерсена (**DKG Pedersen 91**), перенесенный на эллиптические кривые **secp256k1** и **P256**. В процессе генерации участвуют сервисы криптографических операций серверов системы, общаясь друг с другом посредством транзакций на собственные ноды. Для каждого нового голосования запускается процесс генерации нового общего публичного ключа.

Процесс распределенной генерации общего публичного ключа по **DKG Pedersen 91** выглядит следующим образом:

1. После публикации нового голосования, мастерсервер опрашивает доступные сервисы криптографических операций серверовучастников. Но основе полученных данных, он формирует список из **N** сервисов и присваивает каждому из них порядковый номер от **1 до N**.
2. Каждый криптографический сервис генерирует публичный и приватный ключи для участия в голосовании.
3. Каждый криптографический сервис публикует в блокчейн обязательство (**Pedersen commit**) и соответствующий скаляр C_iи r_i. Обязательство и скаляр публикуются для участников голосования.
4. После получения C_iи r_i, каждый участник голосования (сервис шифрования клиента) вычисляет публичные ключи каждого криптографического сервиса.
5. На основе публичных ключей, участники голосования вычисляют общий ключ голосования.

Для реализации схемы разделения секрета Шамира **«K из N»**, сервисы криптографических операций выполняют следующий алгоритм:

1. Каждый сервис криптографических операций случайным образом генерирует полином $f_i(x)^{K\ 1}$.
2. Каждый сервис криптографических операций вычисляет для N других серверов значения полинома в соответствии с их порядковыми номерами т.н. «тени» $F_{i,\ j}$.

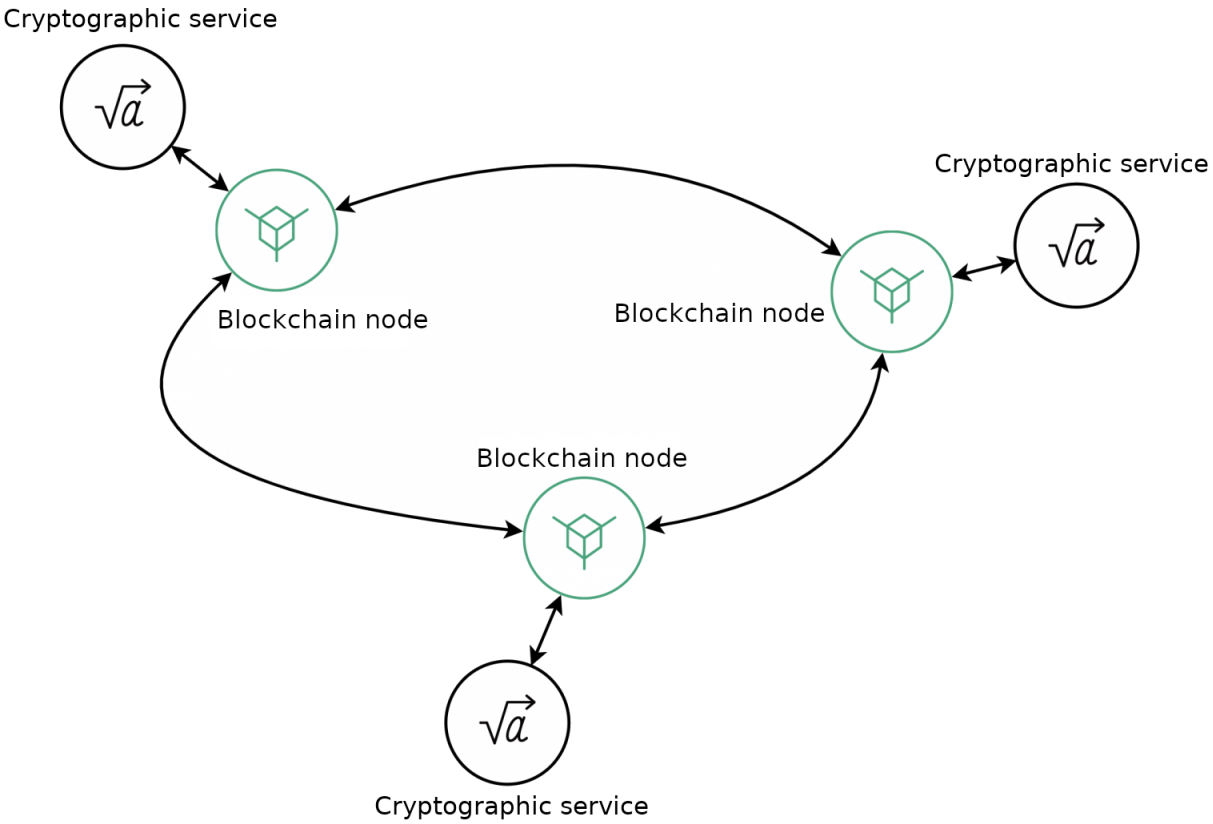


Рис. 2: Схема работы алгоритма распределенной генерации ключей

3. Сервисы криптографических операций публикуют в блокчейн вычисленные «тени» и значения коэффициентов полиномов для всех остальных серверов.
4. Сервисы криптографических операций проверяют корректность опубликованных «теней» и вычисляют приватный ключ, необходимый для дешифровки.

Данный процесс позволяет восстановить зашифрованные итоги проведенного голосования, даже если некоторые из серверов будут недоступны.

11.2 Шифрование

Бюллетени не передаются в рамках системы в открытом виде. Для их шифрования на стороне клиента применяется **криптосистема ЭльГамаля**, также основанная на эллиптических кривых. Эта криптосистема реализует метод **гомоморфного шифрования относительно сложения**: в результате операции сложения над шифротекстом, сервис шифрования генерирует зашифрованную сумму исходных значений.

$$ENCRYPTED(1) + ENCRYPTED(1) = ENCRYPTED(2)$$

Для реализации этого метода шифрования, каждый бюллетень представляется в виде матрицы, где каждая строка это отдельный вопрос, а ячейки строки варианты ответа на вопрос. Каждая из ячеек изначально представлена в виде нуля, а выбранные участником варианты ответов меняют значение соответствующей ячейки на единицу. Дополнительно, каждая ячейка заполненного бюллетеня подвергается шифрованию, после чего публикуется в блокчейн.

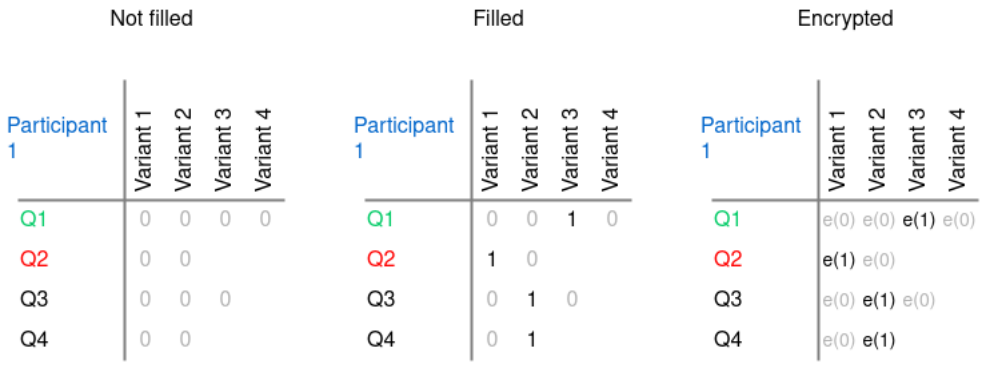


Рис. 3: Процедура шифрования бюллетеней

Затем, при помощи гомоморфного шифрования, зашифрованные ячейки, соответствующие каждому из вариантов ответа, суммируются отдельно каждым сервером системы:

В результате, каждый из серверов системы независимо получает результаты голосования без раскрытия результатов голосования каждого из участников.

Такой процесс позволяет решить следующие проблемы, с которыми сталкиваются онлайнголосования:

- Голос участника невозможно подделать: он не передается в открытом виде и даже не расшифровывается.
- Участника невозможно принудить к голосованию за тот или иной вариант: помимо полной анонимизации результатов голосования, участник имеет возможность изменить свой выбор в ходе голосования. При подсчете система будет учитывать только последний бюллетень, отправленный от имени публичного ключа участника.

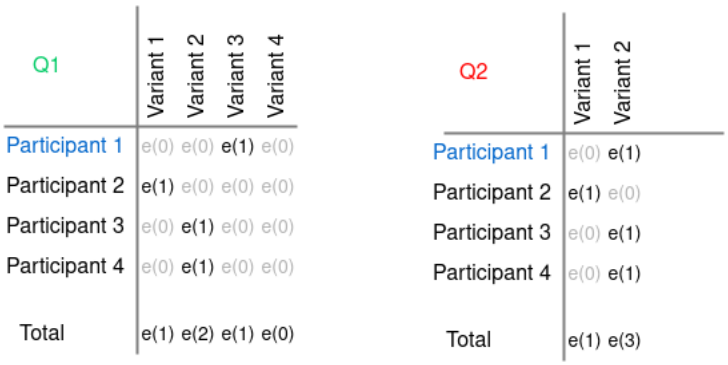


Рис. 4: Процедура сложения зашифрованных ответов

11.3 Доказательства с нулевым разглашением (ZKP)

Криптосистема ЭльГамаля позволяет избежать компрометации результатов голосования со стороны организатора или внешнего злоумышленника. Однако, она не защищает бюллетень от компрометации самим участником голосования: поскольку применяется алгоритм сложения зашифрованных результатов голосования, участник может изменить данные на стороне своего клиентского приложения. Внеся изменения в вариант ответа и отправив «валидный» бюллетень в систему для последующего шифрования и сложения, он может добиться нужного числа голосов за тот или иной вариант.

Поэтому, помимо шифрования бюллетеней и закрытого подсчета результатов голосования, для подтверждения целостности бюллетеней применяется техника **доказательств с нулевым разглашением (ZeroKnowledge Proofs, ZKP)**. Эта техника позволяет доказать обладание информацией без ее раскрытия в том числе, корректность зашифрованного значения без его раскрытия.

В общем виде, принцип работы доказательств с нулевым разглашением иллюстрируется «Пещерой АлиБабы»:

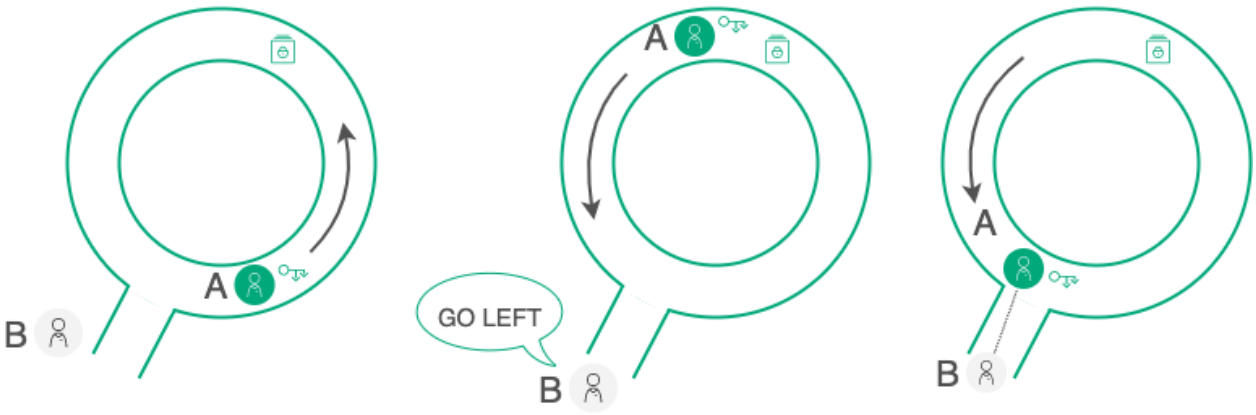


Рис. 5: Иллюстрация техники доказательства с нулевым разглашением

Участник **A** обладает ключом, открывающим дверь в лабиринте, и хочет доказать это участнику **B**, но не хочет показывать ключ. Чтобы **B** мог убедиться в верности утверждения **A**, они организуют серию испытаний:

1. **A** заходит в лабиринт пока **B** отвернулся. **B** не знает в какую сторону пошел **A**.
2. **B** дает **A** указание выйти с какойлибо стороны, например слева.

3. Если **A** действительно обладает ключом, он может появиться с любой стороны и выполняет указание **B**.

Шанс того, что **A** просто повезло, и он, не имея ключа, изначально пошел налево составляет 50/50. Поэтому они повторяют испытание несколько раз, пока вероятность «везения» не станет пренебрежимо малой: в результате, **B** будет располагать достаточными доказательствами, что **A** действительно обладает ключом. При этом, **B** не увидит самого ключа, не получит никакой информации, которой обладает **A** (направление, которое **A** выбирает в каждом испытании) но, в результате серии испытаний, он получит вероятностное доказательство, с любой необходимой точностью.

В применении к процессу голосования в системе WE.Vote, для взаимодействия между участниками применяются **неинтеркативные доказательства с нулевым разглашением (NonInteractive ZeroKnowledge Proofs, NIZK)**.

Сам процесс подтверждения подразделяется на два отдельных алгоритма:

1. Доказательство корректности диапазона в бюллетене (ZeroKnowledge Range Proofs)

Данное доказательство используется при публикации зашифрованного бюллетеня, до начала подсчета голосов.

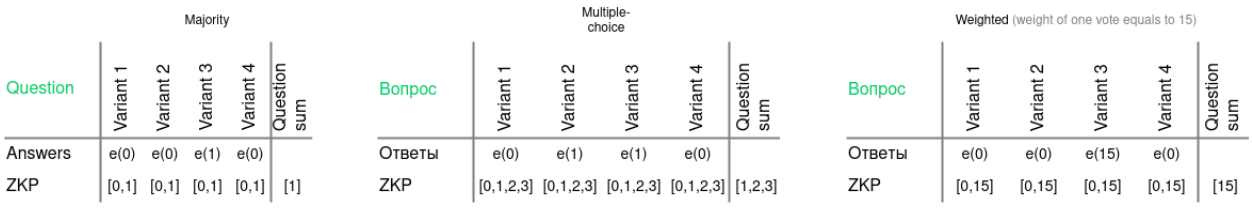


Рис. 6: Иллюстрация доказательства корректности диапазона в бюллетене

Для **мажоритарного голосования**, процесс доказательства выглядит следующим образом:

1. К каждой из заполненных и зашифрованных ячеек прикладывается NIZK, доказывающее, что в ячейке зашифровано одно из значений **0** или **1**. При этом, само значение не раскрывается.
2. Дополнительно, к каждой из ячеек прикладывается доказательство, что зашифрованная сумма всех ячеек строкивопроса равна **1**.

Таким образом, подтверждается, что участник голосования может поставить значение **1** в одну ячейку в ряду (выбрать один из предложенных вариантов ответа).

Для **голосования с множественным выбором**, где участник может выбрать несколько ячеек строки, процесс усложняется:

1. К каждой заполненной и зашифрованной ячейке прикладывается NIZK для диапазона **[0, 1 . . . N]** участник может выбрать как все **N** вариантов ответа, так и некоторые из них.
2. Доказательство суммы ячеек по отдельному вопросу может приклдываться для диапазона **[1. . . N]** (участник может выбрать от **1** до **N** вариантов, но не может оставить вопрос без ответа), либо для значения **N** (участник распределяет доступное количество голосов между вариантами ответа).

Для **взвешенного голосования**, когда каждый участник отдает количество голосов, равное его весу в системе (например, пропорциональное доле владения в компании), процесс доказательства выглядит следующим образом:

1. К каждой из заполненных и зашифрованных ячеек прикладывается NIZK, доказывающее, что в ячейке зашифровано одно из значений **0** или **N**, где **N** вес участника.

2. В качестве доказательства суммы ячеек, прикладывается значение **N**, поскольку при взвешенном голосовании участник может поставить значение **N** в одну ячейку в ряду, как и при мажоритарном голосовании.

Система принимает к подсчету только те бюллетени, все ZKP которых прошли проверку подлинности. То есть, злоумышленник может исказить данные в своем бюллетене, воспользовавшись тем, что система не раскрывает его содержимого однако, в таком случае бюллетень все равно не пройдет валидацию.

2. Доказательство расшифровки (ZeroKnowledge Decryption Proofs)

Данное доказательство применяется при публикации каждым сервисом криптографических операций результатов предварительной расшифровки итогов голосования. Поскольку сервисы действуют независимо друг от друга, на этом этапе существует опасность подмены данных одного или нескольких отдельных сервисов. Доказательство расшифровки позволяет убедиться, что каждый сервис расшифровал и опубликовал именно результаты голосования, а не иную информацию.

Для этого каждый из сервисов прикладывает к своему результату расшифровки доказательство, используя алгоритм ZKP ChaumPedersen. Этот алгоритм доказывает известность числа X для двух соотношений:

- **A** = **X** * **B**;
- **C** = **X** * **D**.

При этом, **A**, **B**, **C** и **D** являются точками, лежащими на одной кривой.

Благодаря приложенному доказательству, любой квалифицированный наблюдатель может самостоятельно произвести следующие операции:

- выполнить гомоморфное сложение валидных бюллетеней и получить итоговые суммы результатов голосования для сравнения;
- проверить доказательства расшифровки итоговых сумм от каждого отдельного сервиса криптографических операций;
- провести итоговую расшифровку результатов голосования с использованием публичных данных, размещенных в блокчейне в ходе голосования.

Доказательство расшифровки исключает вероятность подмены данных при компрометации одного или нескольких серверов системы.

ГЛАВА 12

Как работает WE.Vote

Процесс голосования в системе WE.Vote разделен на четыре основных этапа. В данном разделе описана работа элементов системы для каждого из этапов. Пользовательские сценарии работы приведены в разделе **Как пользоваться сервисом**.

12.1 1.Создание голосования и приглашение участников

Администратор создает голосование в клиентском приложении WE.Vote. Голосование содержит следующие данные:

- описание голосования;
- дата и время проведения голосования;
- список вопросов и ответов к ним;
- список участников голосования;
- дополнительные документы для ознакомления участников голосования.

Дата и время проведения голосования передаются в блокчейн в открытом виде.

Описание голосования, список вопросов и ответов, а также дополнительные документы хэшируются, их хэшсуммы также публикуются в блокчейне. Этот процесс позволяет избежать подмены данных:

- при изменении исходных данных меняется их хэшсумма;
- подмена данных обнаруживается на стороне участника путем сверки полученных данных с их хэшсуммами, опубликованными в блокчейне.

Также при создании голосования в блокчейн отправляются публичные ключи приглашенных участников. При этом, персональные и контактные данные учетных записей не передаются в сеть: при голосовании транзакция подписывается приватным ключом участника, а публичный ключ становится его единственным открытым идентификатором.

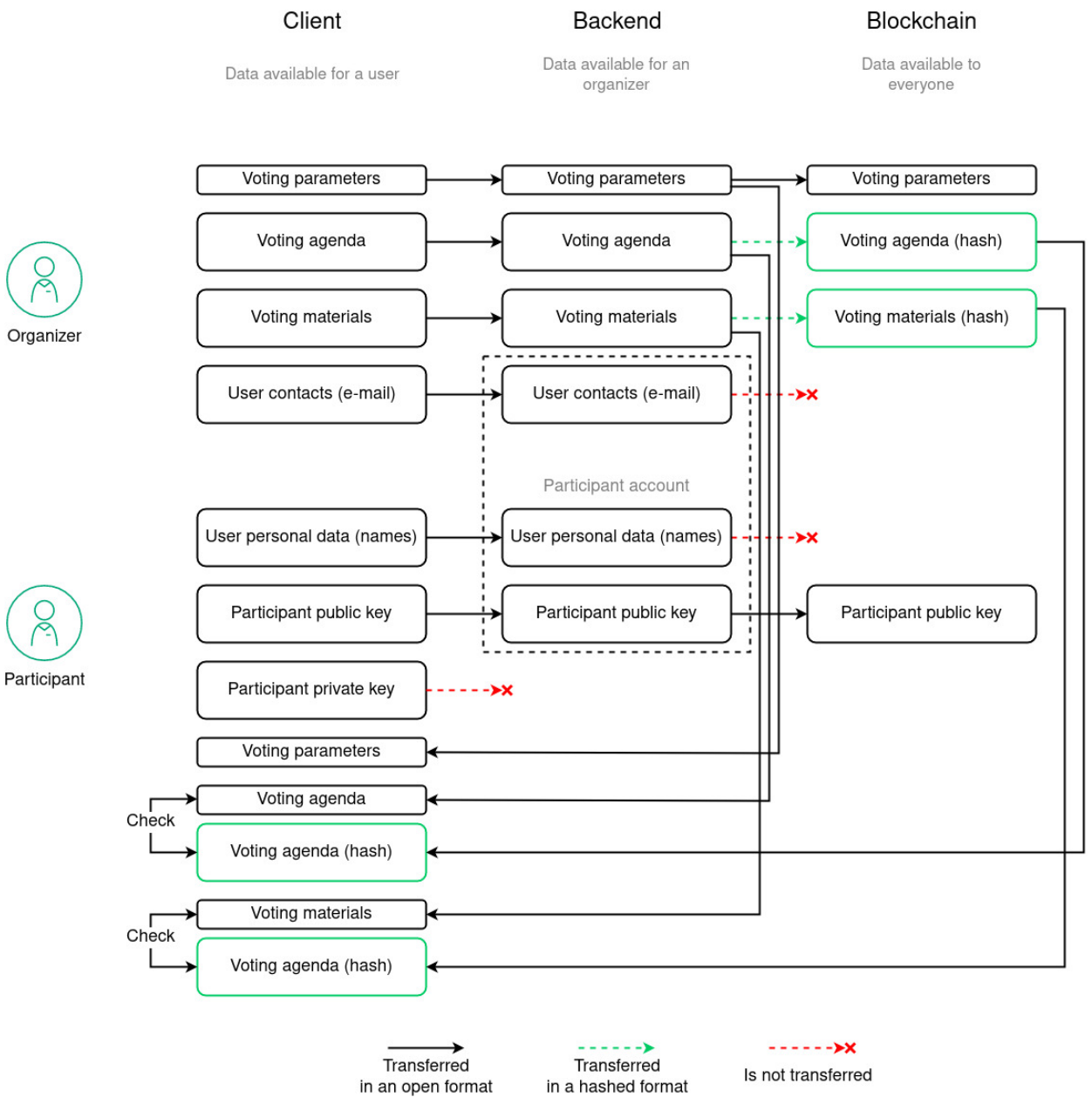


Рис. 1: Схема процесса создания голосования

Исходные данные, опубликованные в блокчейне в виде хэшсумм, также не передаются по сети из соображений конфиденциальности: они сохраняются в локальной базе сервера и доступны только участникам голосования при успешной аутентификации. Это позволяет надежно ограничить доступ не только к результатам голосования, но и к его повестке.

12.2 2. Формирование и публикация общего публичного ключа (MainPublicKey)

Мастерсервер получает из блокчейна данные о подготовке нового голосования, после чего определяет список доступных криптографических сервисов на серверах. На каждый из них мастерсервер отправляет запрос на создание ключевой пары для голосования. В ответ на запрос, каждый криптографический сервис возвращает публичную часть созданного ключа (см. раздел *Генерация ключей*).

Мастерсервер генерирует из полученных публичных ключей общий публичный ключ и публикует его в блокчейн на адрес голосования. В дальнейшем, общий публичный ключ используется сервисами шифрования участников для шифрования заполненных бюллетеней.

После формирования и публикации общего публичного ключа, система получает все необходимые данные для инициации голосования:

- исходные данные голосования сохранены локально в БД каждого сервера;
- хэшсуммы данных опубликованы в блокчейне и служат для контроля целостности материалов голосования;
- общий публичный ключ, необходимый для шифрования голосов участников, также опубликован в блокчейне.

При этом, ни один из участников не располагает какимлибо общим приватным ключом, при помощи которого можно было бы осуществить расшифровку бюллетеней. Соответственно, ни организатор голосования, ни сами участники не имеют возможности подменить данные в бюллетенях, а подсчет голосов осуществляется путем гомоморфного сложения зашифрованных результатов с предварительным и последующим контролем целостности данных (см. разделы **Шифрование и Доказательства с нулевым разглашением главы Криптографические алгоритмы**).

12.3 3. Проведение голосования

После формирования и публикации общего публичного ключа в блокчейне, система ожидает установленного времени начала голосования. Каждый из приглашенных администратором участников голосования получает уведомление о голосовании по электронной почте.

Зарегистрировавшись на сервере и получив доступ к своей учетной записи (см. раздел *Регистрация в сервисе*), участник может ознакомиться с вопросами и материалами голосования. При этом, клиентское приложение участника запрашивает у сервера сохраненные данные голосования. Запрос подписывается соответствующим ключом, выданным участнику при регистрации.

Получив от сервера метариалы голосования, клиентское приложение участника вычисляет их хэшсуммы и сравнивает их с суммами, сохраненными в блокчейне на стадии создания голосования. Это гарантирует участнику целостность данных.

С началом голосования, участник получает возможность дать ответы на вопросы, внесенные в повестку:

1. участник заполняет бюллетень;
2. клиентское приложение шифрует заполненный бюллетень при помощи общего публичного ключа;

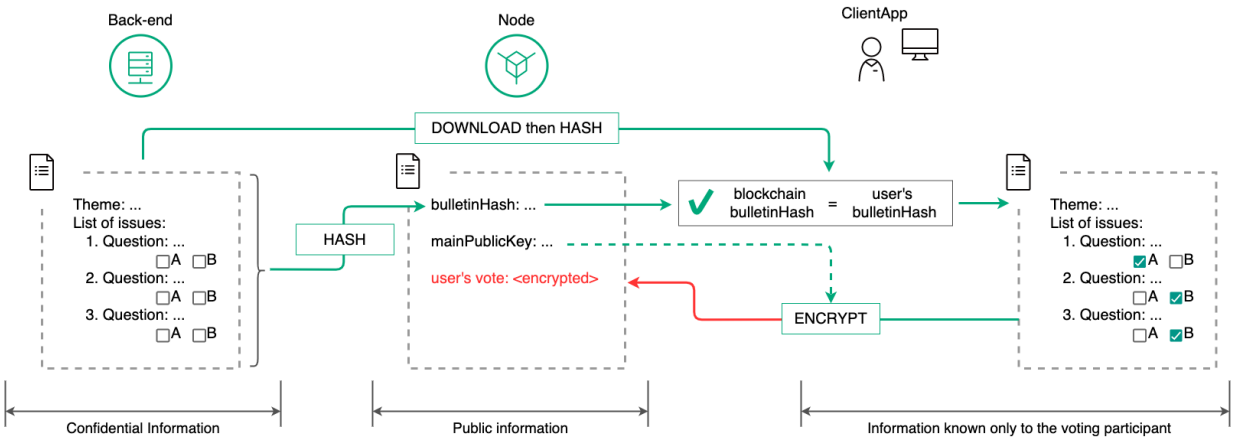


Рис. 2: Схема процесса проведения голосования

3. клиентское приложение подписывает транзакцию на публикацию зашифрованного бюллетеня в блокчейн ключом участника.

Данные, публикуемые в блокчейн, общедоступны. Поэтому транзакция на публикацию зашифрованного бюллетеня доступна всем участникам голосования. Однако, ни один из них не имеет возможности ознакомиться с опубликованными ответами, поскольку не располагает приватным ключом, соответствующим общему публичному ключу голосования.

При публикации зашифрованного бюллетеня, криптографический сервис проверяет корректность установленных диапазонов, не расшифровывая данных бюллетеня (см. раздел *Доказательство корректности диапазона в бюллетене*). Если установлен факт подмены данных, транзакция отклоняется.

В ходе голосования, каждый участник имеет возможность изменить свои варианты ответов. При этом, клиентское приложение шифрует и публикует в блокчейне новый бюллетень участника при помощи повторной транзакции. К подсчету голосов принимается только последний зашифрованный бюллетень, опубликованный участником.

По истечении периода голосования, который был определен администратором при его создании, любые транзакции от участников голосования отклоняются системой.

12.4 4. Подведение итогов голосования

По завершении голосования, все сервера системы независимо проводят подсчет голосов. Подсчет голосов производится без расшифровки результатов голосования, поскольку ни один криптографический сервис не имеет общего приватного ключа для расшифровки.

Результаты голосования по каждому из вопросов подсчитываются путем гомоморфного сложения зашифрованных величин (см. раздел *Шифрование*). В результате, каждый криптографический сервис независимо получает зашифрованное значение суммы голосов участников для каждого из вопросов.

Затем, каждый криптографический сервис приступает к предварительной расшифровке итогов голосования. Для этого сервис применяет собственный приватный ключ, который использовался на шаге **2** для генерации общего публичного ключа. В результате расшифровки, каждый сервис получает нечитаемый предварительный итог голосования.

На этом этапе производится контроль целостности результатов расшифровки при помощи алгоритма **ZKP ChaumPedersen** (см. раздел *Доказательство расшифровки*). Это позволяет убедиться, что данные голосования не были скомпрометированы какимлибо из криптографических сервисов.

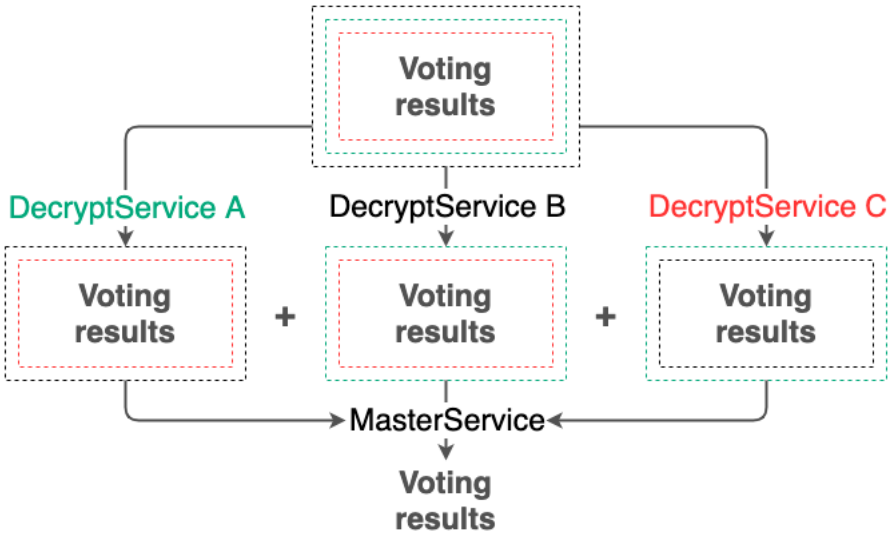


Рис. 3: Схема финального подсчета результатов

Предварительно расшифрованные итоги голосования от каждого сервиса публикуются в блокчейне при помощи транзакций на соответствующие ноды.

Мастерсервер собирает результаты предварительной расшифровки, опубликованные в блокчейне. Затем криптографический сервис мастерсервера суммирует полученные предварительные итоги голосования и окончательно расшифровывает их. Готовые результаты голосования публикуются в блокчейн.

При этом, в случае выхода из строя одного или нескольких серверов, мастерсервер имеет возможность собрать и расшифровать итоговые результаты голосования, благодаря схеме разделения секрета Шамира. Если в формированиии общего публичного ключа участвовало $\mathbf{N}$ серверов, для расшифровки результатов достаточно собрать $\mathbf{K} < \mathbf{N}$ предварительно расшифрованных результатов голосования.

ГЛАВА 13

Часто задаваемые вопросы

13.1 Что такое WE.Vote?

Это платформа на базе блокчейна, позволяющая организовать и провести доверенное голосование для любой организации, в которой предусмотрен механизм коллективного принятия решений.

13.2 Чем отличается голосование на блокчейне от традиционных методов?

- **Децентрализация процедуры голосования.** Это означает, что все действия по голосованию хранятся одновременно на компьютерах всех его участников. Чтобы нарушить голосование или подменить результаты, надо взломать все компьютеры, участвующие в голосовании.
- **Прозрачность голосования.** Распределенный консенсус позволяет предоставить единую версию результатов голосования, согласованную всеми участниками.
- **Конфиденциальность результатов голосования.** Применение криптографических алгоритмов для шифрования результатов позволяет исключить мошенничество с итогом голосования.

13.3 Соблюдается ли анонимность голосования?

Да. Более того, вы можете настроить видимость участников в процессе создания голосования. В зависимости от выбранных настроек, его участники могут видеть или не видеть электронные адреса друг друга.

13.4 Как устроено голосование на блокчейне?

В целом, голосование с применением блокчейна похоже на обычное: применяются те же концепции, подходы и процессы. При создании голосования, вы оперируете общеизвестными параметрами, а при участии в голосовании просто отвечаете на вопросы повестки в клиентском приложении.

Разница заключается в формате работы с данными: все данные голосования хранятся не централизованно на какомлибо сервере, а децентрализовано на компьютерах участников голосования. Наряду с применением криптографических алгоритмов, это позволяет сделать голосование максимально прозрачным и безопасным.

13.5 Как проходит процедура голосования?

Процесс проведения голосования состоит из трёх этапов:

1. Создание голосования:

- Администратор определяет повестку и параметры голосования;
- Система генерирует общий публичный ключ (MainPublicKey) голосования.

2. Проведение голосования:

- Участник отвечает на вопросы повестки;
- Система шифрует бюллетень участника.

3. Подведение итогов голосования:

- Система подводит итоги голосования путем суммирования зашифрованных ответов в бюллетенях каждого участника;
- Система расшифровывает результаты и выводит их для просмотра.

13.6 Можно ли изменить голос в процессе голосования?

Да. До окончания голосования вы можете сколько угодно раз изменить ваши варианты ответов. Для обработки голосов система примет последний вариант вашего бюллетеня.

13.7 Когда будут доступны результаты?

Как правило, результаты доступны через 510 минут после окончания голосования: примерно столько требуется системе WE.Vote для подсчета и расшифровки результатов.

13.8 Применяется ли шифрование результатов?

Да. Система шифрует как ваш бюллетень, так и результаты голосования.

13.9 Можно ли изменить голосование после запуска?

Нет. После запуска голосования никто не может вносить какиелибо изменения в его параметры и повестку. Как участник, вы можете изменить только выбранные вами варианты ответов на вопросы повестки.

13.10 Можно ли подделать результаты голосования?

Практически невозможно. Информация о параметрах голосования и его результатах передается, хранится и обрабатывается только в зашифрованном виде. Технология блокчейна применяется как для хранения данных, так и для контроля их целостности при передаче при помощи хэшсумм. Чтобы подделать или изменить результаты блокчейнголосования, придется взломать не менее 51% компьютеров участников и подменить данные непосредственно во время проведения голосования. Однако, в таком случае расшифровать результаты будет невозможно: скомпрометированные данные не пройдут проверку целостности.

ГЛАВА 14

Словарь терминов

Блокчейн

Децентрализованный, распределённый и общедоступный цифровой реестр, записывающий информацию таким образом, что любая соответствующая запись не может быть изменена задним числом без внесения изменений во все последующие блоки

Гомоморфное шифрование

Форма шифрования, позволяющая выполнять определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполненных с открытым текстом

Криптографическая защита целостности данных

Механизм защиты посредством шифрования данных для безопасного хранения и защиты информации от нежелательных пользователей.

Консенсус

Способ получения согласованного результата группой участников

Мейннет

Основная сеть, в которой выполняются основные функции в виде приемапередачи транзакции, выпуск и хранение токенов

Нода

Узел блокчейн сети, обрабатывающий транзакции, формирующий блоки и реализующий алгоритм консенсуса

Приватный ключ

Строковая комбинация символов для подписания транзакций и доступа к токенам, хранимая приватно. Приватный ключ неразрывно связан с публичным ключом

Публичный ключ

Строковая комбинация символов, неразрывно связанная с приватным ключом. Публичный ключ прикладывается к транзакциям для подтверждения корректности подписи пользователя, сделанной на закрытом ключе

Сервер

Основной узел системы, содержащий Node, DecryptService, CryptoProvider, Backend + Database, API

Смартконтракт

Компьютерный алгоритм, предназначенный для формирования, контроля и предоставления информации о соглашения между участниками

Транзакция

Передача «фактов», производимая участниками в сети, для инициации любых действий

Участник

Участник блокчейна, который направляет транзакции на подтверждение в сеть

Хеш

Уникальная конфигурация символов (буквы, цифры), результат исполнения хешфункции по заданному алгоритму над данными. Хеш однозначно идентифицирует объект

DKG (Distributed Key Generation)

Криптографический процесс, в котором несколько сторон участвуют в расчете общего набора открытых и закрытых ключей

MPCпротокол (MultiParty Computation)

Криптографический протокол, позволяющий нескольким участникам произвести вычисление, зависящее от тайных входных данных каждого из них, таким образом, чтобы ни один участник не смог получить никакой информации о чужих тайных входных данных

ZeroKnowledge Range Proofs

Интерактивный криптографический протокол, позволяющий одной из взаимодействующих сторон («The verifier» — проверяющей) убедиться в достоверности какоголибо утверждения (обычно математического), не имея при этом никакой другой информации от второй стороны («The prover» — доказывающей)

ГЛАВА 15

Официальные ресурсы

- Официальный сайт блокчейнплатформы Waves Enterprise
- Github проекта
- Официальный сайт блокчейнплатформы Waves