УДК 004.832.2 Вестник УрФО № 4(54) / 2024, с. 15–21

Кротова Е. Л., Субботина Ю. В., Ермаков Д. Г., Тишин К. Л.

10.14529/secur240402

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ПРИ РАЗРАБОТКЕ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Проведен сравнительный анализ самых востребованных блокчейн проектов на применимость для решения задачи разработки протокола электронного голосования. Выделены те принципы технологии blockchain, которые позволяют улучшить существующие решения в области электронного голосования Разработаны критерии оценки надежности разрабатываемого протокола. Показано, что технология blockchain и принципы, на которых она базируется, позволяют использовать ее положительные качества для создания электронной системы голосования, в которой предусмотрено устранение недостатков существующих систем электронного голосования, сформулированных ранее.

Ключевые слова: *технология блокчейн, P2P протоколы, электронное голосование, КОИБ*

Krotova E. L., Subbotina Yu. V., Ermakov D. G., Tishin K. L.

USING BLOCKCHAIN TECHNOLOGY TO DEVELOP AN ELECTRONIC VOTING SYSTEM

A comparative analysis of the most popular blockchain projects was carried out to determine their applicability for solving the problem of developing an electronic voting protocol. The principles of blockchain technology are highlighted that make it possible to improve existing solutions in the field of electronic voting. Criteria for assessing the reliability of the protocol being developed have been developed. It is shown that blockchain technology and the principles on which it is based make it possible to use its positive qualities to create an electronic voting system, which provides for the elimination of the shortcomings of existing electronic voting systems formulated earlier.

Keywords: *blockchain technology, P2P protocols, e-voting, PECs*

Понятие «электронное голосование» можно определить как совокупность различных способов выражения воли избирателя, объединенных обязательным условием: подсчет голосов осуществляется с помощью специальных программно-технических устройств без вмешательства человека. В постановлении ЦИК России от 27 августа 2014 года № 248/1529–6 «О Порядке электронного голосования с использованием комплексов для электронного голосования на выборах, проводимых в Российской Федерации» дается следующее определение: «Электронное голосование – голосование без использования бюллетеня на бумажном носителе, с использованием комплекса средств автоматизации ГАС «Выборы». Таким образом, в России электронное голосование не включает использование оптических машин для сканирования бумажных бюллетеней.

В день голосования избиратель имеет право выбрать способ участия в выборах: дистанционно (электронно) или традиционно (на избирательном участке).

Анализируя мировой опыт электронного голосования, можно отметить, что в большинстве стран электронное голосование охватывает любую форму выражения воли граждан, где для обработки голосов используются программно-технические средства. Формы электронного голосования могут быть различными, но процесс передачи информации – протокол – един.

Выборы остаются одной из проблемных тем в общественном восприятии. Итоги, процесс голосования, свобода выбора, анонимность – все это вызывает сомнения. В связи с этим вырос интерес к новым технологиям тайного голосования, особенно к дистанционному электронному голосованию (ДЭГ).

Впервые ДЭГ было применено в единый день голосования 8 сентября 2019 года в Москве на выборах депутатов городской думы. Оно проводилось как эксперимент в трех округах столицы. В 2020 году ДЭГ использовалось в общероссийском голосовании по поправкам в Конституцию РФ в Москве и Нижегородской области. В 2021 году ДЭГ применялось на выборах в Госдуму РФ в семи регионах, в 2022 году – в восьми регионах, а в 2023 году – уже в 25 регионах.

ДЭГ имеет несколько преимуществ по сравнению с традиционной системой голосования:

Удобство для избирателей: возможность голосовать в любом месте, что особенно важно для маломобильных граждан или тех, кто находится не по месту прописки.

Увеличение явки: избиратели могут голосовать, не выходя из дома.

Исключение человеческого фактора: автоматический подсчет голосов обеспечивает большую точность и скорость.

Снижение затрат: отсутствие необходимости в привлечении большого числа людей для организации процесса и аренде специальных площадок делает выборы дешевле и проще в подготовке.

Основным препятствием для широкого внедрения электронного голосования остается стереотип о ненадежности результатов информационных систем. Люди часто не доверяют результатам, полученным через Интернет. В данной работе рассматриваются вопросы обеспечения информационной безопасности электронных выборов с использованием протоколов с нулевым разглашением.

Объектом исследования в данной теме являются протоколы с нулевым разглашением и протоколы на основе технологии блокчейн.

Предметом исследования является определение области использования электронного голосования, построенного на основе протоколов с нулевым разглашением и на основе технологии блокчейн.

Научно-техническая проблема определена тем, что в условиях активного развития информационных технологий и повышенного интереса граждан к анонимности, важной проблемой для отрасли становится приобретение статуса конфиденциальной информации при реализации конституционного права свободного выбора. Одним из наиболее эффективных методов решения проблемы является усовершенствование системы с использованием протоколов с нулевым разглашением и на основе технологии блокчейн.

Исследуя возможность использования технологии блокчейн для электронного голосования было выявлено, что основной характеристикой программного обеспечения является уровень доверия в системе.

Доверие к системе основывается на вычислительной работе хэш-функции, которая преобразовывает данные в код определенной длины, т.е. шифрует записи. С помощью полученного кода определенной длины третья сторона понимает, что данные,

которые были переданы достоверны, при этом даже не зная самих данных. Аргументом такой функции может быть сообщение или файл, а значение - цепочка битов определенной длины, например, 256 бит. Выходное значение функции называется «хэшем» или «дайджестом» сообщения. Значение всегда одно и то же для определенного аргумента. Если изменится хотя бы один символ в аргументе, то полученный хэш будет совершенно другим. Так как функция является криптографической, то ее расчет в обратном направлении требует невыполнимых вычислений [1-7]. Мы исключаем возможность принятия поддельных операций и реестров с несоответствиями, так как они требуют практические неосуществимых по времени вычислений.

Допустим, что в распределенном реестре есть 4 участника: Мы, Алиса, Боб, и Чарли. Все транслируют друг другу сообщения об операциях и нам нужно каким-то образом, прийти к согласию насчет правильного реестра, который каждый из участников транслирует. Сначала реестр делится на блоки, каждый из которых состоит из списка операций и доказательства выполнения, то есть числа, вместе с которыми хэш блока начинается с какого-то количества нулей. Блок действителен, только если в нем есть доказательства выполнения работы, аналогично операции, которая подтверждается только если ее подписывает отправитель. Мы доверяет тому реестру, над которым было проведено больше всего вычислений. Если они одинаковые по длине, то нужно дождаться нового блока, который изменит это равенство.

Также для того, чтобы мы, Алиса, Боб и Чарли достигли согласия о текущем состоянии данных во всех блоках, в блокчейн встраивается специальный механизм под названием алгоритм консенсуса. Соблюдение правил этого алгоритма дает гарантию того, что все транзакции достоверны. То есть алгоритм консенсуса говорит нам о том, что все участники (мы, Алиса, Боб, Чарли), подключенные к блокчейну были согласны с добавлением нового блока в цепочку. Наиболее востребованными среди лучших блокчейн-проектов являются: Proof-of-Work, Proof-of-Stake, PoA, DPoS.

Говоря об идеальной системе голосования стоит заметить, что достичь ее невозможно, но рассмотрим, каким требованиям должна удовлетворять наша система [5].

1. Все голоса должны быть учтены и учтены корректно.

2. Верифицируемость избирателей. Возможность голосования должна быть предоставлена всем лицам, обладающим избирательным правом.

3. Один избиратель – один голос, не должно допускаться двойное голосование.

4. Голосование должно быть анонимным.

5. Голосование должно исключать возможность какого-либо контроля за волеизъявлением гражданина или принуждения к нему.

6. Голосование не должно создавать предпосылок для манипуляций на основе политических взглядов.

7. Должна обеспечиваться неизменность поданного голоса. К тому же данные о волеизъявлении избирателей не могут быть изменены или удалены.

8. Процесс голосования должен быть прозрачен, поскольку цель выборов – не просто выбрать победителя, но и убедить проигравших в том, что они проиграли.

9. Конфиденциальность голосов. Должна отсутствовать возможность подсчета промежуточных результатов голосования до его завершения. Конфиденциальность достигается за счет шифрования бюллетеней и невозможности расшифрования до окончания голосования.

10. Должна обеспечиваться прозрачность исполнения и неизменность программного кода, реализуемого в виде смарт-контрактов.

11. Должна обеспечиваться защита и неизменность данных, используемых в процессе голосования: списка избирателей, ключах, используемых для шифрования бюллетеней на различных этапах криптографического протокола, и так далее.

12. Децентрализованное хранение данных, при этом каждый участник должен обладать абсолютно идентичной со всеми копией, подтвержденной свойствами консенсуса в сети. [6]

13. Должна обеспечиваться возможность просматривать транзакции и отслеживать ход голосования, полностью отражающегося в цепочках блоков, от его начала до записи рассчитанных итогов.

14. Проверяемость. Наблюдатель может проверить, что подсчет голосов осуществлялся корректным образом.

Ключевой критерий оценки успешности избирательной системы – это высокий уровень доверия со стороны граждан. Именно этот критерий позволяет избежать волнения среди населения в пост-выборный период и дает возможность стране перейти в будущее без серьезных потрясений. Таким образом, чтобы сделать успешную избирательную систему, нужно добиться максимальной прозрачности как в бизнес-процессах, так и в технических аспектах. Однако при абсолютной анонимности, прозрачность теряется. [7]

Принципы технологии блокчейн

В этом разделе подведем итог и обозначим те принципы технологии blockchain, которые позволяют улучшить существующие решения в области электронного голосования.

• Копии с информацией о транзакциях распространяются среди большого количества участников системы для того, чтобы избежать критических ошибок в случае, если что-то произойдет на одном устройстве.

Этот принцип позволяет соблюдать критерий достаточной отказоустойчивости системы голосования.

• Невозможность внесения изменений или уничтожения записей в блокчейн без консенсуса.

• Использование хэширования для защиты данных и проверки подлинности отправителя и получателя.

Эти принципы позволяют соблюдать критерий надежности системы к взлому или искажению информации третьими лицами.

• Открытый публичный бухгалтерский реестр, который позволяет получить доступ к деталям транзакции с момента создания блокчейна, никак не раскрывая личностей людей, которые участвовали в этих транзакциях.

Этот принцип позволяет соблюдать критерий достаточной прозрачности процесса голосования, который мы выделили раннее для лучшего функционирования системы электронного голосования.

Требования к системе голосования с применением технологии блокчейн

Требования, которые должны быть реализованы для системы голосования на блокчейн:

1. Возможность создания опросов.

После создания пользователем опроса, ему будет присуждаться статус администратора опроса. После чего он будет иметь возможность разграничивать доступ для лиц, которые будут иметь разрешение на участие в созданном опросе (голосовании).

2. Возможность создания списков объектов голосования к опросу.

3. Возможность зарегистрировать участников созданного опроса.

4. Возможность для участников опроса голосовать.

Каждый пользователь при успешном прохождении регистрации должен получать необходимое для подачи голоса число токенов.

5. Обеспеченная прозрачность процесса голосования.

Каждый пользователь должен иметь возможность посмотреть результаты голосования и цепочки блоков в реальном времени.

6. Обеспечение отказоустойчивости системы.

Система продолжит работу, если одно из устройств с базой данных голосования выйдет из строя, так как копия базы данных хранится на устройствах всех участников сети, где запущено децентрализованное приложение.

7. Отсутствие возможности вносить любые несанкционированные изменения, влияющие на подсчет голосов

У злоумышленника должна отсутствовать возможность влияния на ход голосования и его результаты из-за устойчивости системы к взлому.

В ходе аналитической работы был выявлен ряд целей, к которым стремиться любая система электронного голосования:

- повышение скорости подсчета голосов;
- сокращение роли человека в подсчете голосов;
- повышение доверия к результатам голосования.

С опорой на успешный мировой опыт автоматизации голосования и на характеристики/критерии, следование которым свидетельствовало бы об улучшении текущих решений, предложено следующее решение сформулированной проблемы: использование технологии blockchain при разработке системы электронного голосования. Так как технология blockchain и принципы, на которых она базируется, позволяют использовать ее положительные качества для создания

электронной системы голосования, в которой предусмотрено устранение недостатков существующих систем электронного голосования, сформулированных ранее. Данное решение соответствует всем критериям более эффективной системы электронного голосования, которые были выявлены в ходе анализа, а именно:

• Критерий достаточной прозрачности процесса голосования. Подсчет голосов должен осуществляться корректным образом без возможности его фальсификации.

• Критерий достаточной отказоустойчивости системы голосования. Недостаточность отказоустойчивости системы, может привести к тому, что если машина, занимающаяся обработкой голосов, выйдет из строя, то это приведет к нарушению всего процесса голосования.

• Критерий надежности системы голосования. Принцип построения архитектуры системы голосования должен обеспечивать отсутствие единой «точки отказа» этой системы.

С опорой на успешный мировой опыт автоматизации голосования [4, 5, 7, 10, 12] и на характеристики/критерии, следование которым свидетельствовало бы об улучшении текущих решений, предложено следующее решение сформулированной проблемы: использование технологии blockchain при разработке системы электронного голосования. Так как технология blockchain и принципы, на которых она базируется, позволяют использовать ее положительные качества для создания электронной системы голосования, в которой предусмотрено устранение недостатков существующих систем электронного голосования, сформулированных ранее. Данное решение соответствует всем критериям более эффективной системы электронного голосования, которые были выявлены в ходе изучения теоретических основ технологии блокчейн и ее анализа, а именно:

1. Критерий достаточной прозрачности процесса голосования. Подсчет голосов должен осуществляться корректным образом без возможности его фальсификации.

2. Критерий достаточной отказоустойчивости системы голосования. Недостаточность отказоустойчивости системы, может привести к тому, что если машина, занимающаяся обработкой голосов, выйдет из строя, то это приведет к нарушению всего процесса голосования.

3. Критерий надежности системы голосования. Принцип построения архитектуры системы голосования должен обеспечивать отсутствие единой «точки отказа» этой системы.

Литература

1. Прасти Н. Блокчейн. Разработка приложений, // Н. Прасти, В.С. Яценков. – СПб.: БХВ–Петербург, 2018. – 256 с.

2. Равал С. Децентрализованные приложения. Технология Blockchain в действии, // С. Равал. – СПб.: Питер, – 2017. – 192 с.

3. Тапскотт Д., Тапскотт А. Технология блокчейн – то, что движет финансовой революцией сегодня, // Д. Тапскотт, А. Тапскотт. – М.: Эксмо, 2017. – 448 с.

4. Насколько надежно электронное голосование [Электронный ресурс]. – Режим доступа: https://www.svoboda.org/a/269300.html, свободный.

5. Норвегия официально отказалась от электронного голосования на выборах: оно контрпродуктивно [Электронный ресурс]. – Режим доступа: http://www.mk.ru/politics/world/2014/06/30/norvegiya–otkazalasv–politike–ot–elektronnogo–golosovaniya.html, свободный.

6. Block The Vote: Could Blockchain Technology Cybersecure Elections? [Электронный ресурс]. – Режим доступа: http://www.forbes.com/sites/realspin/2016/08/30/block–the–votecouldblockchain–technology–cybersecure–elections, свободный.

7. California: The Top to Bottom Review [Электронный ресурс]. – Режим доступа: http://www.votetrustusa.org/index.php?option=com_content&task=view&id =2554&Itemid=113, свободный.

8. IGS Votomatic Prototype Goes to the Smithsonian [Электронный ресурс]. – Режим доступа: https://web.archive.org/web/20070713201451/http://www.igs.berkeley.edu/publications/par/winter2001/votomatic.htm, свободный.

9. Kiwi. Bitcoin testnet sandbox. [Электронный ресурс]. – Режим доступа: https://testnet.manu.backend.hamburg/faucet, свободный.

10. NSW election result could be challenged over iVote security flaw [Электронный ресурс]. – Режим доступа: https://www.theguardian.com/australia–news/2015/mar/23/nsw–electionresult–could–be–challenged–over–ivote–security–flaw, свободный.

11. Peer–to–peer [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf, свободный.

12. Russian Hackers Acted to Aid Trump in Election, U.S. Says [Электронный ресурс]. – Режим доступа: https://www.nytimes.com/2016/12/09/us/obama–russia–election–hack.html, свободный.

13. Slim. Middeware–slim. [Электронный ресурс]. – Режим доступа: https://www.slimframework.com/docs/v3/concepts/middleware.html, свободный.

14. State bans electronic balloting in 4 counties / Touch–screen firm accused of 'reprehensible,' illegal conduct [Электронный ресурс]. – Режим доступа: https://www.sfgate.com/politics/article/State–bans–electronic–balloting–in–4– counties–2784975.php, свободный.

15. Top 100 Cryptocurrencies by Market Capitalization [Электронный ресурс]. – Режим доступа: https://coinmarketcap.com/, свободный.

16. Voting Machine Company Submits to Inquiry [Электронный ресурс]. – Режим доступа: https://www.nytimes.com/2006/10/31/us/politics/31vote.html?_r=1&oref=slogin, свободный.

17. Why machines are bad at counting votes [Электронный ресурс]. – Режим доступа: https://www.theguardian.com/technology/2009/apr/30/e–votingelectronic–polling–systems, свободный.

18. Baudron, O. Practical multi–candidate election system. In proceedings of the twentieth annual ACM symposium on Principles of distributed computing, // Baudron, O., Fouque, P.A., Pointcheval, D., Stern, J., Poupard, G. – ACM, 2001. –pp. 274 – 283.

References

1. Prasti N. Blokcheyn. Razrabotka prilozheniy, // N. Prasti, V.S. Yatsenkov. – SPb.: BKHV–Peterburg, 2018. – 256 s.

2. Raval S. Detsentralizovannyye prilozheniya. Tekhnologiya Blockchain v deystvii, // S. Raval. – SPb.: Piter, – 2017. – 192 s.

3. Tapskott D., Tapskott A. Tekhnologiya blokcheyn – to, chto dvizhet finansovoy revolyutsiyey segodnya, // D. Tapskott, A. Tapskott. – M.: Eksmo, 2017. – 448 s.

4. Naskol'ko nadezhno elektronnoye golosovaniye [Elektronnyy resurs]. – Rezhim dostupa: https://www.svoboda.org/a/269300.html, svobodnyy.

5. Norvegiya ofitsial'no otkazalas' ot elektronnogo golosovaniya na vyborakh: ono kontrproduktivno [Elektronnyy resurs]. – Rezhim dostupa: http://www.mk.ru/politics/world/2014/06/30/norvegiya–otkazalasv–politike–ot–elektronnogo–golosovaniya.html, svobodnyy.

6. Block The Vote: Could Blockchain Technology Cybersecure Elections? [Elektronnyy resurs]. – Rezhim dostupa: http://www.forbes.com/sites/realspin/2016/08/30/block–the–votecouldblockchain–technology–cybersecure–elections, svobodnyy.

7. California: The Top to Bottom Review [Electronic resource]. – Access mode: http://www.votetrustusa.org/index.php?option=com_content&task=view&id =2554&Itemid=113, free.

8. IGS Votomatic Prototype Goes to the Smithsonian [Electronic resource]. – Access mode: https://web.archive.org/web/20070713201451/http://www.igs.berkeley.edu/publications/par/winter2001/votomatic.htm, free.

9. Kiwi. Bitcoin testnet sandbox. [Electronic resource]. – Access mode: https://testnet.manu.backend.hamburg/faucet, free.

10. NSW election result could be challenged over iVote security flaw [Electronic resource]. – Access mode: https://www.theguardian.com/australia–news/2015/mar/23/nsw–electionresult–could–be–challenged–over–ivote–security–flaw, free.

11. Peer–to–peer [Electronic resource]. – Access mode: https://bitcoin.org/bitcoin.pdf, free.

12. Russian Hackers Acted to Aid Trump in Election, U.S. Says [Electronic resource]. – Access mode: https://www.nytimes.com/2016/12/09/us/obama–russia–election–hack.html, free.

13. Slim. Middeware–slim. [Electronic resource]. – Access mode: https://www.slimframework.com/docs/v3/concepts/middleware.html, free.

14. State bans electronic balloting in 4 counties / Touch–screen firm accused of 'reprehensible,' illegal conduct [Electronic resource]. – Access mode: https://www.sfgate.com/politics/article/State–bans–electronic–balloting–in–4– counties–2784975.php, free.

15. Top 100 Cryptocurrencies by Market Capitalization [Электронный ресурс]. – Режим доступа: https://coinmarketcap.com/, свободный.

16. Voting Machine Company Submits to Inquiry [Электронный ресурс]. – Режим доступа: https://www.nytimes.com/2006/10/31/us/politics/31vote.html?_r=1&oref=slogin, свободный.

17. Why machines are bad at counting votes [Электронный ресурс]. – Режим доступа: https://www.theguardian.com/technology/2009/apr/30/e–votingelectronic–polling–systems, свободный.

18. Baudron, O. Practical multi–candidate election system. In proceedings of the twentieth annual ACM symposium on Principles of distributed computing, // Baudron, O., Fouque, P.A., Pointcheval, D., Stern, J., Poupard, G. – ACM, 2001. –pp. 274 – 283.

Кротова Елена Львовна, кандидат физико-математических наук, доцент кафедры «Высшая математика», Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

Субботина Юлия Владимировна, ведущий инженер кафедры «Высшая математика», аспирант кафедры «Высшая математика», Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: yulyia.urazbaeva@mail.ru

Ермаков Дмитрий Германович, кандидат физико-математических наук, старший научный сотрудник отдела дифференциальных уравнений Лаборатории научно-информационных ресурсов, Федеральное государственное бюджетное учреждение науки Институт математики и механики им. Н. Н. Красовского Уральского отделения Российской академии наук (ИММ УрО РАН). 620108, г. Екатеринбург, ул. Софьи Ковалевской, д. 16.; кандидат физико-математических наук, доцент, Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». 620002, Екатеринбург, ул. Мира, 19. E-mail: Dmitry.Ermakov@mail.ru

Тишин Константин Львович, аспирант кафедры «Высшая математика», Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: konstantinlvovich777@gmail.com

Krotova Elena Lvovna, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. E-mail: lenkakrotova@yandex.ru

Subbotina Yulia Vladimirovna, Leading engineer of the Department of Higher Mathematics, postgraduate student of the Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. E-mail: yulyia.urazbaeva@mail.ru

Yermakov Dmitry Germanovich, Candidate of Physical and Mathematical Sciences, Senior Researcher, Department of Differential Equations, Laboratory of Scientific and Information Resources, Federal State Budgetary Scientific Institution, N. N. Krasovsky Institute of Mathematics and Mechanics, Ural Branch of the Russian Academy of Sciences (IMM UB RAS). 620108, Yekaterinburg, Sofya Kovalevskaya St., 16; Candidate of Physical and Mathematical Sciences, Associate Professor, Federal State Autonomous Educational Institution of Higher Education "Ural Federal University named after the first President of Russia B. N. Yeltsin". 620002, Yekaterinburg, Mira St., 19. E-mail: Dmitry.Ermakov@mail.ru.

Tishin Konstantin Lvovich, postgraduate student, Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. E-mail: konstantinlvovich777@gmail.com.