DOI 10.17587/issn.1684-6400

ISSN 1684-6400

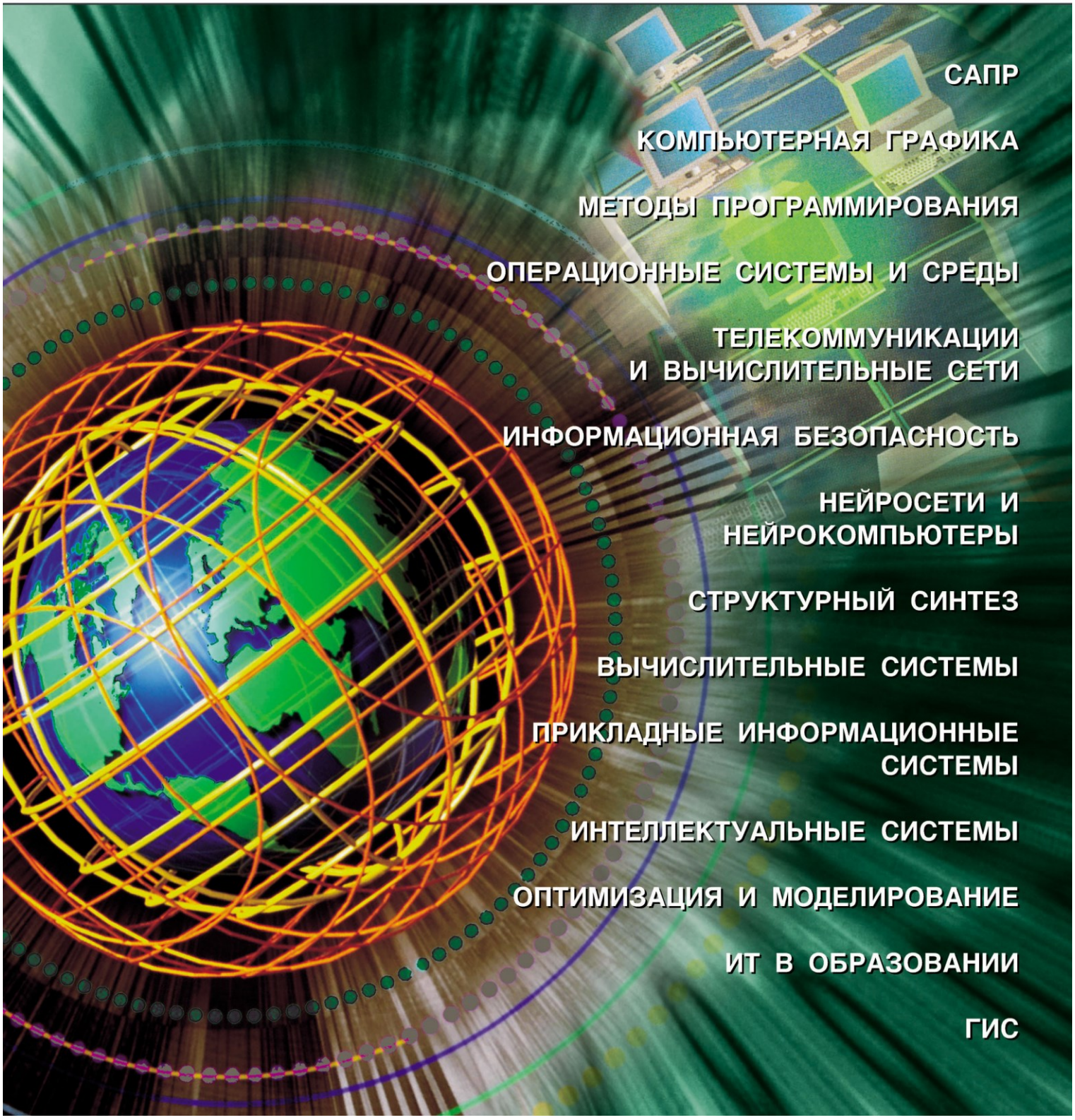
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Том 25

2019

№ 2

ТЕОРЕТИЧЕСКИЙ И ПРИКЛАДНОЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ



ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Том 25
2019
№ 2

ТЕОРЕТИЧЕСКИЙ И ПРИКЛАДНОЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

Издается с ноября 1995 г.

DOI 10.17587/issn.1684-6400

УЧРЕДИТЕЛЬ

Издательство "Новые технологии"

СОДЕРЖАНИЕ

Информация о журнале доступна по сети Internet по адресу **http://novtex.ru/IT.**
Журнал включен в систему Российского индекса научного цитирования и базу данных RSCI на платформе Web of Science.
Журнал входит в Перечень научных журналов, в которых по рекомендации ВАК РФ должны быть опубликованы научные результаты диссертаций на соискание ученой степени доктора и кандидата наук.

УДК 004:338 DOI: 10.17587/it.25.75-85

Н. К. Трубочкина, д-р техн. наук, проф., e-mail: ntrubochkina@hse.ru,
С. К. Поляков, бакалавр, e-mail: savvapolyakov1@gmail.com,
Национальный исследовательский университет "Высшая школа экономики", г. Москва

Система электронного голосования на основе технологии блокчейн с использованием смарт-контракта

В современном демократическом цифровом обществе возрастает актуальность проведения открытых и объективных голосований с использованием новых информационных технологий. Существующие решения практически используемых систем голосования сосредоточены на технических и юридических проблемах, а не на применении новых информационных технологий в стадии самого голосования. В статье проанализированы проблемы современных избирательных систем, и на основании анализа их недостатков предложены метод, алгоритмы и программная реализация системы голосования на основе применений технологии блокчейн со специальной программной реализацией смарт-контрактов, в которой недостатки существующих систем устранены.

Ключевые слова: *новые информационные технологии, блокчейн, смарт-контракт, электронное голосование, система голосования*

Введение

В настоящее время демократическое голосование является одним из популярнейших методов решения общественно важных вопросов в развитых странах. Наиболее распространенным методом голосования является бумажная система. Данный метод обладает определенными недостатками, среди которых технические (фальсификации, ошибки в подсчетах, отсутствие прозрачности проведения), социальные и экономические (высокая стоимость для бюджета). Электронные системы голосования не получили своего распространения из-за проблем с безопасностью, верификацией результатов или некорректной работой программного обеспечения [7, 8].

Технология блокчейн (от *англ. blockchain* — цепочка блоков данных) предлагает новые возможности для разработки совершенно иных видов цифровых услуг благодаря ключевым особенностям этой технологии, таким как прозрачность и защищенность процесса передачи данных. Разработчики имеют возможность вывести систему голосования на новый информационно-технологический уровень, отвечающий современным требованиям. Применение смарт-контрактов в сочетании с технологией блокчейн поможет решить большую часть существующих проблем современных систем голосования.

Технология блокчейн основывается на транзакционной модели. Принцип работы технологии блокчейн изображен на рис. 1. Каждый пользователь имеет свой "кошелек" с уникаль-

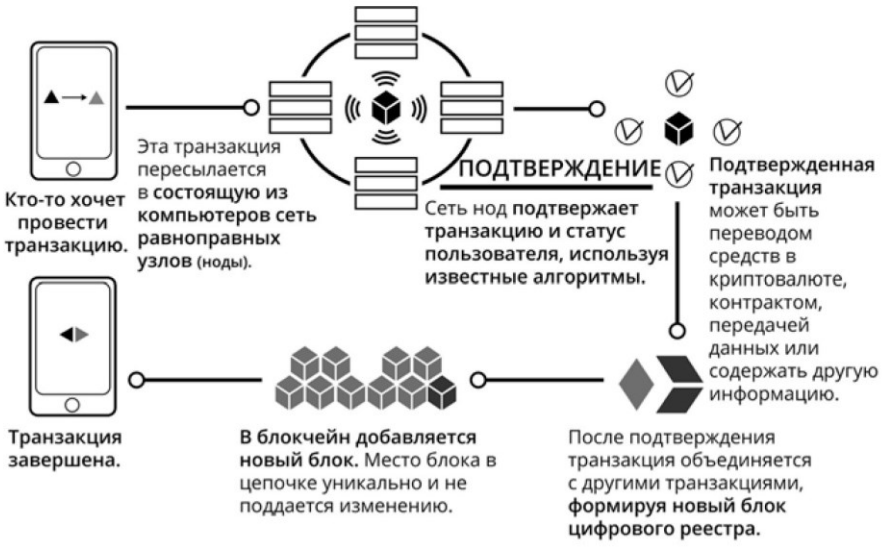


Рис. 1. Принцип работы технологии блокчейн

ными публичными/приватными ключами, которыми подтверждается любое действие пользователя. Транзакции (от *англ. transaction* — сделка, отправление), которые проводят все пользователи системы, хранятся в последовательных блоках. Так как хэш (от *англ. Hash*) данных предыдущего блока используется при генерации следующего, обеспечивается неизменность данных внутри блокчейна.

При изменении любого блока автоматически все последующие блоки становятся не валидными. Блокчейн устроен таким образом, что все транзакции хранятся одновременно на всех узлах в полном объеме, и они не могут быть удалены или изменены.

За счет этих ключевых особенностей технологии блокчейн идея его применения в системах голосования становится актуальной и оправданной. Блокчейн дает возможность заменить устаревшую технологию голосования, когда голос избирателя выражен физическим объектом, на передачу цифрового "токена" (от *англ. Token* — жетон). Как и во многих аналогичных случаях, переход процесса из физического мира в цифровой сокращает экономические издержки и повышает надежность.

Объективными преимуществами использования технологии блокчейн в процессе голосования являются:

1. Прозрачность процесса голосования. Любой человек получит возможность контролировать ход голосования, так как блокчейн дает возможность развернуть узел с полной копией всех данных, и каждый сможет самостоятельно их проанализировать.

2. Анонимность голоса. Любой из избирателей при получении доступа к голосованию генерирует индивидуальный публичный и приватный ключ, который он имеет право не разглашать другим участникам голосования. Никто, кроме него, не будет знать, что конкретный "кошелек", с которого был отправлен голос, принадлежит этому человеку.

3. Подлинность и надежность результатов. Результаты голосования, проведенного с помощью технологии блокчейн, невозможно сфальсифицировать, так как любой участник может проверить, сколько токенов-голосов было выпущено в начале голосования, и как они распределялись по кошелькам после.

4. Экономическая целесообразность и скорость обработки данных. Голосование всегда сопряжено с организационными сложностями, а также экономическими и временными затратами на проведение голосования и последующую обработку данных. Децентрализация, которая лежит в основе технологии блокчейн, позволит моментально увидеть результаты голосования, а для грамотного распределения нагрузки каждый субъект (регион/город) может использовать собственный узел системы.

Обзор и анализ систем цифрового голосования

Блокчейн-технология в системах цифрового голосования вызывает большой интерес, что приводит к появлению значительного числа исследований. В работах [1—3, 10] исследуются проблемы традиционных избирательных систем. Авторы сходятся во мнении, что существующие методы, в частности электронные системы, не могут обеспечить достаточный уровень прозрачности и надежности, что негативно сказывается на доверии избирателей. В данных исследованиях разбирается принцип работы технологии блокчейн, а также преимущества ее использования в системе выборов.

В табл. 1 представлен обзор и анализ работ о системах голосования на основе технологии блокчейн.

Необходимо подчеркнуть, что безопасность голосования всегда является самой большой проблемой при рассмотрении вопроса о внедрении цифровой системы голосования [6, 9]. Все авторы сходятся в том, что с учетом осо-

Таблица 1

Обзор и анализ аналогов

Содержание	Lubin J. (2016) [10]	Boucher P. (2016) [3]	Ben Ayed A. (2017) [2]	Barnes A., Brake C., Perry T. (2018) [1]
Анализ существующих избирательных систем	+	+	+	+
Обзор технологии блокчейн	+	—	+	—
Перспективы применения технологии блокчейн в избирательных системах	+	+	+	+
Практическая реализация системы голосования на основе технологии блокчейн	—	—	—	—

бенностей технологии блокчейн не может быть никаких сомнений в способности системы защитить данные от потенциальных атак и фальсификаций. Система голосования является сложным механизмом, при разработке которой нужно учитывать как человеческий фактор, так и особенности проведения голосований в конкретной стране.

Несмотря на то что авторы объясняют теоретическую основу технологии, описывают перспективы и достоинства подобной системы, *ни одно из рассмотренных выше исследований*

- *не определяет структуру работы системы голосования на практике, и*
- *в них отсутствуют конкретные методы, алгоритмы и программы для практической реализации системы.*

С учетом анализа недостатков указанных исследований была поставлена задача разработки системы голосования на основе технологии блокчейн, структуры ее работы, а также конкретных алгоритмов и программ для ее практической реализации.

Новизна

На основе изучения недостатков существующих систем голосования, а также анализа исследований, проведенных в области электронных голосований, предлагается *новая концепция смешанной избирательной системы*, основанная на использовании технологии блокчейн и написании смарт-контрактов.

Концепция, предложенная в данной работе, предполагает возможность ее внедрения в избирательную систему уже сейчас. Она позволит избежать возможности фальсификаций, сделает процесс голосования прозрачным и защищенным, сократит государственные издержки на проведение процедуры и подсчет голосов.

Предлагаемая система предполагает проведение голосования за счет смарт-контракта (от *англ. Smart contract* — "умного контракта"), написанного на языке Solidity и исполняемого в блокчейн-среде Ethereum ("Эфириум") [4].

Метод смарт-контракта

Самый доступный способ провести электронное голосование на базе блокчейна — разработать и запустить смарт-контракт (приложение) в уже существующих блокчейн-сетях.

Смарт-контракт — это программный код, способный контролировать и автоматически осуществлять определенные действия и записывать их в блокчейн, далее мы более подробно коснемся этой темы.

Среда разработки

В качестве платформы для реализации предлагаемой системы была выбрана сеть Ethereum ("Эфириум"), так как данная платформа предоставляет широкие возможности для разработки D-Apps (*с англ.* — децентрализованные приложения) и смарт-контрактов. На данном блокчейне уже работают несколько проектов [13]: проект правительства Москвы "Активный гражданин", проект удаленной идентификации IDChain РосЕвроБанка и Microsoft [14], проект по обмену реквизитами банков (банки "Открытие", Сбербанк, АФТ, ВТБ) [12].

Алгоритмы

Рассмотрим алгоритм работы технологии блокчейн на конкретном примере голосования:

1. Избиратель хочет выбрать определенного кандидата, т. е. перевести свой токен (*голос*) на адрес выбранного им кандидата.

2. Эта транзакция пересылается в состоящую из компьютеров сеть равноправных узлов, называемых "нодами" (*от англ. Node* — узел). Сеть нода необходима для того, чтобы обработать (подтвердить) данную транзакцию. *Преимуществом* является то, что данная сеть может быть **децентрализована**, что снизит вероятность специального вмешательства в работу системы и повысит доверие избирателей.

3. Сеть нода подтверждает транзакцию и статус пользователя, используя специальные алгоритмы. В других системах подтвержденная транзакция может быть не только "голосом", а также передачей денег или данных.

4. После подтверждения транзакция объединяется с другими подтвержденными транзакциями, формируя новый блок цифрового реестра.

5. Данный блок добавляется в блокчейн с использованием хэша предыдущего блока, тем самым место каждого блока в цепочке становится уникальным и не подлежит изменению, так как в случае попытки изменить конкретный блок все последующие блоки становятся не валидными.

6. В итоге, транзакция завершена и записана в блокчейн, что гарантирует ее достоверность и защищенность, а выбранный кандидат

получает "голос", что автоматически отображается для всех наблюдателей.

Алгоритм голосования с использованием смарт-контракта — суть предлагаемого метода — изображен на рис. 2.

Рис. 2. Алгоритм голосования с использованием смарт-контракта

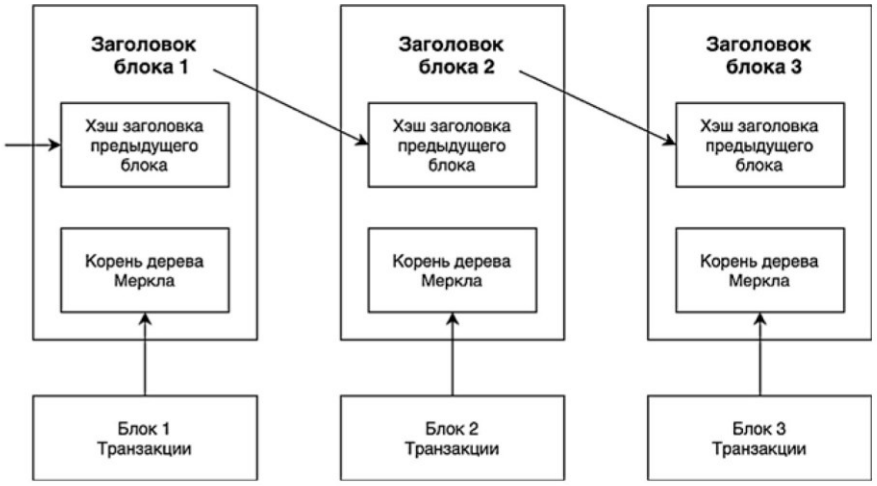


Рис. 3. Блокчейн — последовательность блоков

Основная технология — блокчейн

Технология блокчейн (*последовательность блоков*) была впервые представлена анонимным разработчиком (или группой разработчиков) под псевдонимом Сатоши Накамато и была использована в электронной валюте Bitcoin, которая позволила проводить финансовые операции через Интернет, без потребности в финансовом учреждении или регуляторе [11]. Блокчейн — это упорядоченная структура данных, которая содержит блоки транзакций (рис. 3).

Транзакции, которые проводят все пользователи системы, хранятся в последовательных блоках. Исходный блок называется Genesis Block или "Блок 0". Genesis block создается по описанию, которое содержится в конфигурационном файле, разработчик блокчейна прописывает только его. Соответственно, в нулевом блоке не содержится ссылок на предыдущий блок.

Структура блока транзакций

В табл. 2 представлена структура блока транзакций согласно спецификации протокола, где

- version — версия блока;
- prev_block — хэш предыдущего блока (parent block);
- merkle_root — хэш всех транзакций в блоке;
- timestamp — дата и время создания блока;

Таблица 2

Структура блока согласно спецификации протокола

Размер поля	Наименование	Тип данных	Примечание
4	version	int32_t	Информация о версии блока
32	prev_block	char[32]	Хэш-значение предыдущего блока, на который ссылается данный блок
32	merkle_root	char[32]	Ссылка на дерево Меркла, которое является хэшем всех транзакций, связанных с этим блоком
4	timestamp	uint32_t	Запись временной метки Unix при создании блока
4	bits	uint32_t	Вычислительная сложность, используемая для блока
4	nonce	uint32_t	Код, используемый для создания этого блока (вычисления хэша)
?	txn_count	var_int	Номер транзакции
?	txns	tx[]	Транзакции блока, в формате "tx"

- bits, nonce — параметры майнинга (от англ. Mining — генерация новых блоков);
- txn_count, txns — число транзакций в блоке и их список.

Первые шесть параметров (все, кроме txn_count и txns) образуют заголовок блока (header). Именно хэш заголовка называют хэшем блока, т. е. сами транзакции непосредственного участия в хэшировании не принимают, вместо этого они заносятся в особую структуру — дерево Меркла.

Алгоритм Secure Hash Algorithm (SHA-256)

Для генерации 256-битного хэша фиксированного размера используется алгоритм Secure Hash Algorithm (SHA-256) (рис. 4).

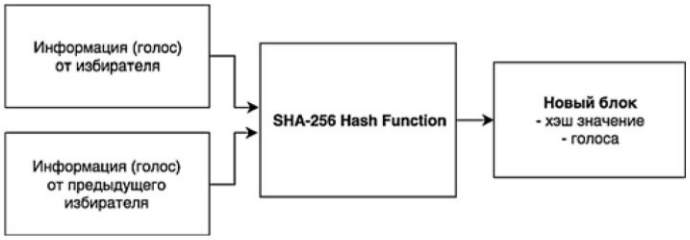


Рис. 4. Схема хэширования в блокчейн-системе голосования

SHA-256 является самой популярной криптографической хэш-функцией [5]. Данный алгоритм является строго односторонней функцией, и может принимать в качестве входного текст любого размера и зашифровывать его до 256-байтового двоичного значения.

Поскольку хэш данных предыдущего блока используется при генерации следующего, обеспечивается неизменность данных внутри блокчейна. При изменении любого блока автоматически все последующие блоки становятся не валидными. Блокчейн устроен таким образом, что все транзакции хранятся одновременно на всех узлах в полном объеме, и они не могут быть удалены или изменены.

Алгоритм построения дерева Меркла

Дерево Меркла [11] — это структура данных, также известная как бинарное дерево хэшей (рис. 4), которая позволяет проводить упрощенную верификацию транзакций.

Построим дерево Меркла, используя распространенный алгоритм двойного хэширования SHA-256:

1. Считаются хэши всех транзакций в блоке, допустим, транзакции A:

$$\text{hash (A)} = \text{SHA256(SHA256(A))} = H_A.$$

2. После этого считаются хэши от суммы хэшей транзакций, допустим, транзакций A и B:

$$\text{hash } (H_A + H_B) = \\ = \text{SHA256(SHA256}(H_A + H_B)) = H_{AB}.$$

3. Точно так же считаем хэши от суммы получившихся хэшей:

$$\text{hash } (H_{AB} + H_{CD}) = \\ = \text{SHA256(SHA256}(H_{AB} + H_{CD})) = H_{ABCD}.$$

4. Далее продолжаем выполнять алгоритм по рекурсии. Так как дерево бинарное, то на каждом шаге оно должно иметь четное число элементов. Поэтому если, например, у нас только три транзакции, то последняя транзакция просто дублируется (рис. 5).

5. Процесс продолжается до тех пор, пока не получится один единственный хэш — он и называется merkle_root (данное значение записывается в заголовок (header) блока).

Теперь для проверки информации о транзакции нет необходимости пересчитывать все хэши, достаточно запросить доказательство Меркла (состоит из корня дерева Меркла и ветви, включающей хэши от запрашиваемой транзакции до корня). Сложив запрошенные хэши и сравнив их с корнем, убеждаемся, что транзакция находится на своем месте.

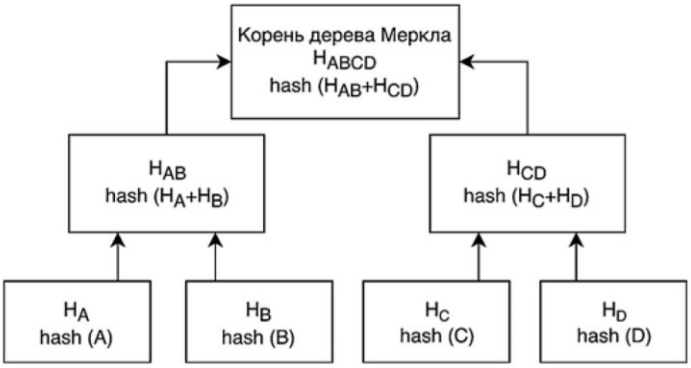


Рис. 5. Структура дерева Меркла

Смарт-контракт (алгоритм)

Смарт-контракт — условие или алгоритм, предназначенный для заключения и поддержания контрактов, реализованных в блокчейне. Смарт-контракты дают возможность осуществлять конфиденциальные и надежные транзакции без участия внешних посредников.

Для корректной работы и исполнения условий смарт-контракта:

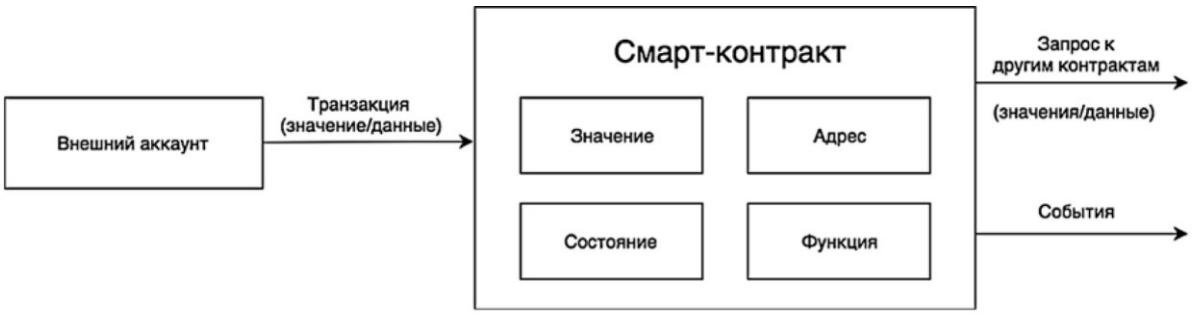


Рис. 6. Алгоритм работы смарт-контракта

- необходима среда, которая позволяет автоматизировать выполнение контракта, такая как блокчейн;
- для реализации поставленной проектной задачи также важно, что транзакции внутри блокчейна являются отслеживаемыми, прозрачными, без возможности изменить или удалить транзакцию;
- все условия контракта должны иметь прозрачную логику исполнения и математическое описание;
- смарт-контракт автоматизированно определяет достижение или нарушение своих пунктов, отталкиваясь от запрограммированных условий.

Из всего вышесказанного следует, что основная идея смарт-контрактов состоит не только в автоматизации выполнения условий, но и в достоверности их исполнения.

Алгоритм работы смарт-контракта показан на рис. 6.

Смарт-контракт размещается в блокчейне, где вся его логическая структура помещается в ***программный блок***.

Программный блок связывает все сведения, имеющие отношение к определенному смарт-контракту. Данные сведения могут исполнять роль входа и выхода программного кода контракта и могут запускать какие-либо действия за пределами блокчейна.

Обязательными свойствами смарт-контракта являются:

1) применение метода электронной подписи на базе публичных или приватных ключей, находящихся у двух и более сторон соглашения;

2) существование приватной децентрализованной среды, в которой вносится смарт-контракт;

3) суть договора и существование обязательных для его исполнения инструментов;

4) точно отображенные условия его выполнения, подтверждаемые подписью участников договора, и надежность источника данных.

Значительное число различных договорных отношений как между людьми, так и между человеком и государственными органами возможно реализовать частично или полностью самовыполняемыми. Криптография, которая лежит в основе смарт-контрактов, предоставляет более высокий уровень безопасности и защищенности, чем традиционные договоры, основанные исключительно на праве. Также смарт-контракты могут снижать экономические издержки, риски неоднозначных трактовок договора, риски использования "юридических махинаций" и человеческий фактор.

Исходя из вышесказанного, можно отметить следующие основные преимущества смарт-контрактов, в сравнении с традиционными контрактами:

1. Экономия и скорость — системы на основе блокчейна устраняют посредников и автоматизируют множество процессов.

2. Защищенность — смарт-контракт хранится в блоке в зашифрованном виде, а также многократно продублирован.

3. Надежность — выполнение условий смарт-контракта гарантируется математическими законами, а технология блокчейн исключает подмену информации.

4. Точность — минимизация человеческого фактора снижает вероятность ошибок.

Практическая реализация системы голосования

Требования к системе голосования

1. *Аутентификация.* Иметь возможность голосовать должно определенное число людей, имеющих на это право. Система не должна поддерживать процесс самостоятельной регистрации, список избирателей должен быть подготовлен и загружен заранее. Непосредственно перед голосованием избиратель должен пройти дополнительный процесс аутентификации, в противном случае его голос ("токен") не дол-

жен использоваться. Также процесс дополнительной аутентификации на избирательном участке не даст возможность третьим лицам использовать "голос" избирателя вне его ведома.

2. *Анонимность*. Система голосования должна исключать какие-либо связи между личностью избирателя и его "голосом" (токеном). Избиратель и его выбор должен оставаться полностью анонимным во время и после голосования.

3. *Точность*. Результаты должны быть абсолютно объективными, каждый "голос" (токен) должен учитываться, не может быть изменен, продублирован или удален.

4. *Открытость*. Система должна иметь возможность проверки процесса голосования в режиме реального времени.

5. *Защищенность*. Система должна быть абсолютно защищена от различного вида программных атак, перехвата информации третьими лицами или вмешательства в процесс голосования.

6. *Масштабируемость*. Система должна быть рассчитана на возможность проведения голосований федерального или муниципального масштабов.

Ограничения системы

Предполагается, что избиратели будут использовать защищенные устройства для голосования. Несмотря на то что технология блокчейн гарантирует безопасность и объективность процесса голосования, злоумышленник имеет возможность изменить выбор избирателя с помощью вредоносного программного обеспечения, установленного на устройстве голосования. Также особенностью технологии блокчейн является невозможность изменения выбора в случае ошибки пользователя. Избиратель может отдать свой голос, т. е. осуществить выбор, только один раз.

Предлагаемая последовательность осуществления процедуры электронного голосования на базе технологии блокчейн с использованием смарт-контракта

Разработана последовательность осуществления процедуры электронного голосования на базе технологии блокчейн с использованием смарт-контракта (рис. 7). В данной последовательности продуман процесс от прихода избирателя на участок, его аутентификации до голосования за конкретного кандидата. Для работы подобной системы разработан смарт-контракт, который включает в себя:

1. Структуры (программы) "Голосующий" и "Кандидат". Для реализации функционирования системы структура "Кандидат" содержит поля: имя и подсчет голосов, отданных за данного кандидата. Структура "Голосующий" включает в себя поля для:
- зачисления токена (голоса) после успешной авторизации, для осуществления голосования;
- данных о кандидате, за которого избиратель отдал свой голос;
- полученного хэша избирателя;
- индикатора, голосовал ли данный избиратель.

2. Функции (программы) "Голосования", "Авторизации", "Создания голосования", "Подсчета голосов", "Завершения голосования".

Установка предлагаемой системы на избирательных участках происходит следующим образом: на первом участке вручную запускается genesis block, который создается по описанию, содержащемуся в конфигурационном файле.

Также при создании процедуры голосования в смарт-контракт загружаются:
- список с номерами паспортов избирателей (предоставляет сторонний ответственный орган);
- список кандидатов;
- время проведения голосования.

Далее система генерирует пары вида [номер паспорта, псевдослучайный пин-код].

Голосующий предъявляет паспорт сотруднику избирательной комиссии, и его просят придумать произвольное дополнительное число или слово.

После этого система вычисляет хэш от трех параметров: [номер паспорта, псевдослучайный пин-код, сгенерированный системой, дополнительное число].

Данное дополнительное число (слово) используется в качестве "salt" (соль), для того, чтобы:
- исключить перехват сотрудниками избирательного органа пин-кодов избирателей;
- сделать невозможным подбор злоумышленниками хэша.

Далее полученный хэш автоматически отправляется в смарт-контракт в функцию auth (авторизации), и у пользователя появляется возможность проголосовать. После этого пользователь в терминале голосования вводит свои данные, пин-код, дополнительное слово или код — на основании этих данных считывается хэш и сравнивается с тем, который записан

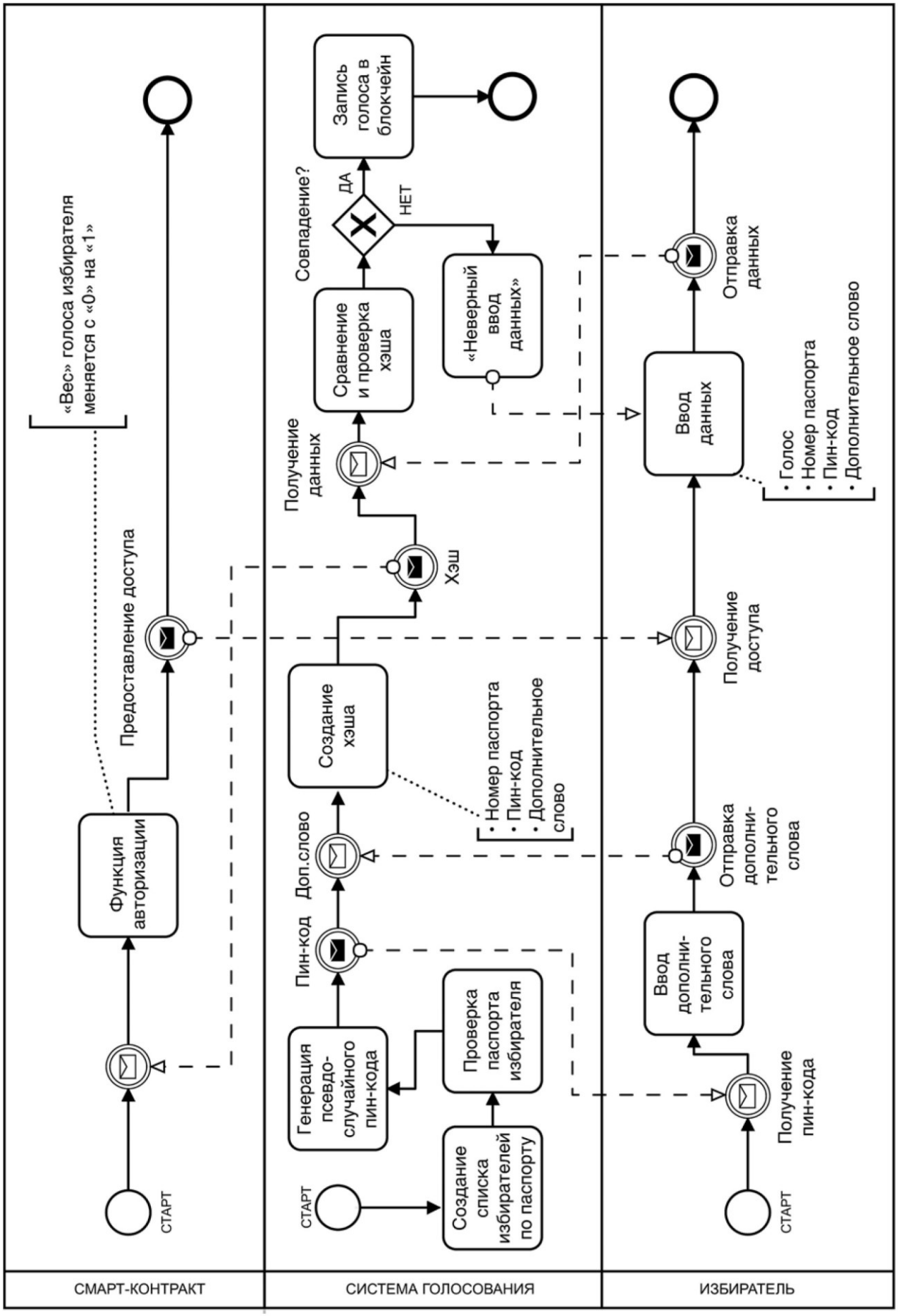


Рис. 7. Предлагаемая последовательность осуществления процедуры электронного голосования на базе технологии блокчейн с использованием смарт-контракта

в смарт-контракт. После полной авторизации он голосует.

При желании разработанную систему голосования можно интегрировать с государственным сервисом gosuslugi ("Госуслуги"), что значительно упростит процесс верификации, и дополнительное число (salt) не будет требоваться. Для этого необходима заблаговременная регистрация каждого участника голосования в сервисе государственных услуг. В таком случае ЦИК обязан предоставлять сервису список с номерами паспортов граждан, имеющих право участвовать в конкретном голосовании, а система государственных услуг должна выдавать пин-код каждому участнику голосования, с помощью которого он сможет пройти идентификацию на избирательном участке.

Программная реализация разработанных алгоритмов

Для работы данной системы голосования необходимо, как минимум, создать структуры и функции в смарт-контракте (рис. 8—13):

- структуры "Голосующий" и "Кандидат" (рис. 8);

Структуры "Голосующий" и "Кандидат"

```
struct Candidate
{
        string name;
        uint voteCount;

}

struct Voter
{
        bool voted;
        uint votedId;
        uint weight;
}
```

Рис. 8. Пример программного кода смарт-контракта, описывающий структуры "Голосующий" и "Кандидат"

- функция авторизации (рис. 9);

Функция авторизации

```
function authorize(string voter){
        require (msg.sender == owner);
        require (!voters[voter].voted);
        voters[voter].weight = 1;
}
```

Рис. 9. Пример программного кода смарт-контракта, функция авторизации

- функция голосования (рис. 10);

Функция голосования

```
function vote(uint votedId){
        require (now<electionEnd);
        require (!voters[msg.sender].voted);
        //TODO: look documentation
        require (votedId>=0);
        require (votedId<=candidates.length);

        voters[msg.sender].voted = true;
        voters[msg.sender].votedId = votedId;


        candidates[votedId].voteCount += voters[msg.sender].weight;
```

Рис. 10. Пример программного кода смарт-контракта, функция голосования

- конструктор новых голосований (рис. 11);

Конструктор новых голосований

```
//Конструктор: название выборов, длительность, набор кандидатов
constructor (string _name, uint durationHours, string[] candidateNames){
        owner = msg.sender;
        name = _name;
        //Обратим внимание, now - это время блока!
        electionEnd = now + (durationHours* 1 hours);
        //TODO: look documentation
        for (uint i=0; i<candidateNames.length; i++){
                candidates.push(Candidate(candidateNames[i], 0));
        }
```

Рис. 11. Пример программного кода смарт-контракта, функция создания новых голосований

- функция подсчета голосов (рис. 12);

Функция подсчета голосов

```
function votesFor(uint id) view public returns (uint) {
 require (id>=0);
 require (id<candidates.length);
 return candidates[id].voteCount;
}
```

Рис. 12. Пример программного кода смарт-контракта, функция подсчета голосов

- функция завершения процедуры голосования (рис. 13).

Функция завершения процедуры голосования

```
function end(){
 require (msg.sender == owner);
 require (now>=electionEnd);
 for (uint i = 0; i<candidates.length; i++)
 {
  emit ElectionResult(candidates[i].name,candidates[i].voteCount);
 }
}
```

Рис. 13. Пример программного кода смарт-контракта, функция завершения голосования

На этом цикл разработки системы голосования (обзор и анализ аналогов (наличие недостатков) — постановка задачи — разработка концепции — метод — алгоритмы — программы — последовательность осуществления

процедуры электронного голосования на базе технологии блокчейн с использованием смарт-контракта) завершен.

Заключение

На основании обзора систем цифрового голосования и анализа их недостатков разработана функционально полная система электронного голосования и схема проведения выборов на основе технологии блокчейн при использовании смарт-контракта, написанного на языке Solidity и исполняемого в блокчейн-среде Ethereum.

Данная система при последующей доработке и внедрении может позволить создавать и проводить достоверную и прозрачную процедуру голосования, сократить издержки государства на проведение избирательных компаний.

Разработанную систему голосования можно применить во многих случаях, например, в следующих:

1. Выборы президента, мэра города, главы региона, но в этом случае нужно будет дополнительно реализовать систему сетевых узлов для равномерного распределения нагрузки на сеть.

2. Выборы в научных и образовательных учреждениях (выборы в Академии наук, выборы лучшего преподавателя в университете, главы студенческого совета).

3. Муниципальные выборы.

Особенностью результатов данного исследования является тот факт, что систему электронного голосования с предлагаемой структурой при доработке для конкретных задач, а также посредством решения вопросов масштабируемости можно внедрить в работу государственных органов, научных и образовательных учреждений уже в ближайшее время.

Кроме того, предусмотрена возможность интеграции подсистемы авторизации пользователя с существующими государственными электронными услугами.

Список литературы

1. **Barnes A., Brake C., Perry T.** Digital Voting with use of Blockchain Technology. URL: https://www.economist.com/sites/default/files/plymouth.pdf (дата обращения: 14.08.18).

2. **Ben Ayed A.** A conceptual Secure Blockchain — Based Electronic Voting System // International Journal of Network Security & Its Applications (IJNSA). 2017. Vol. 9, N. 3. URL: http://aircconline.com/ijnsa/V9N3/9317ijnsa01.pdf (дата обращения: 14.08.18).

3. **Boucher P.** What if blockchain technology revolutionized voting // European Union. 2016. URL: http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA(2016)581918_EN.pdf (дата обращения: 14.08.18).

4. **Ethereum** Homestead Documentation (2016) (http://www.ethdocs.org/en/latest/) (дата обращения: 14.08.18).

5. **ElGamal T.** A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Info. Theory. 1985. Vol. 31. P. 469—472. URL: https://ieeexplore.ieee.org/document/1057074/ (дата обращения: 14.08.18).

6. **Evans D., Paul N.** Election Security: Perception and Reality // IEEE Privacy Magazine. 19.02.04. URL: https://ieeexplore.ieee.org/document/1264850/ (дата обращения: 14.08.18).

7. **Gerlach J., Grasser U.** Three Case Studies from Switzerland: E-voting // Berkman Center Research Publication. 02.04.09. URL: https://www.alexandria.unisg.ch/52680/ (дата обращения: 14.08.18).

8. **Ibrahim S., Kamat M., Salleh M., Aziz S. R. A.** Secure E-Voting with Blind Signature // Proceeding of the 4th National Conference of Communication Technology. 14.01.03. URL: https://ieeexplore.ieee.org/document/1188334/ (дата обращения: 14.08.18).

9. **Jan J., Chen Y., Lin Y.** The Design of Protocol for e-Voting on the Internet // Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology. 19.10.01. URL: https://ieeexplore.ieee.org/document/962831/) (дата обращения: 14.08.18).

10. **Lubin J.** How Blockchain Will Disrupt Our Election System // Internet resource "Futurism". 7.11.2016. URL: https://futurism.com/how-blockchain-will-disrupt-our-election-system/ (дата обращения: 14.08.18).

11. **Nakamoto S.** A Peer-to-Peer Electronic Cash System. // The Cryptography Mailing list. 31.10.08. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 14.08.18).

12. **Крупные** российские банки "входят во вкус" технологии блокчейн. 2017. URL: https://ria.ru/economy/20170727/1499301891.html (дата обращения: 14.08.18).

13. **Поляков К.** Как власти Москвы внедряют блокчейн в городские проекты. URL: https://rb.ru/opinion/blockchain-moscow/ (дата обращения: 14.08.18).

14. **"РосЕвроБанк"** разработал прототип системы удаленной идентификации клиентов на базе технологии блокчейн от Microsoft. 2017. URL: https://news.microsoft.com/ru-ru/rosevrobank-razrabotal-prototip-sistemy-udalennoj-identifikatsii-klientov-na-baze-tehnologii-blokchejn-ot-microsoft/ (дата обращения: 14.08.18).

N. K. Trubochkina, Dr. Tech. Sc., Professor, e-mail: ntrubochkina@hse.ru,
S. K. Poliakov, Baccalaureate, e-mail: savvapolyakov1@gmail.com,
National Research University the Higher School of Economics, Moscow

The Concept of Electronic Voting Based on Blockchain

In modern democratic digitalized society the topicality of open and objective elections with the use of innovative information technology grows. Existing solutions of practically used voting systems are concentrated on technical and law problems instead of using innovative information technologies on the stage of the voting itself. The article analyzes problems of modern election systems, and offers reasonable methods, algorithms and software implementation of voting system based on blockchain technology with with special software implementation of smart-contracts in which flaws of existing systems are eliminated.

Keywords: *innovative information technology, blockchain, smart-contract, electronic voting, voting system*

DOI: 10.17587/it.25.75-85

References

1. **Barnes A., Brake C., Perry T.** Digital Voting with use of Blockchain Technology, available at: https://www.economist.com/sites/default/files/plymouth.pdf (date of access: 14.08.18).

2. **Ben Ayed A.** A conceptual Secure Blockchain — Based Electronic Voting System, *International Journal of Network Security & Its Applications (IJNSA)*, 2017, vol. 9, no. 3, available at: http://aircconline.com/ijnsa/V9N3/9317ijnsa01.pdf (date of access: 14.08.18).

3. **Boucher P.** What if blockchain technology revolutionized voting, European Union, 2016, available at: http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA(2016)581918_EN.pdf (date of access: 14.08.18).

4. **Ethereum** Homestead Documentation, 2016, available at: (http://www.ethdocs.org/en/latest/ (date of access: 14.08.18).

5. **ElGamal T.** A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Trans. Info. Theory*, 1985, vol. 31, pp. 469—472, available at: https://ieeexplore.ieee.org/document/1057074/) (date of access: 14.08.18).

6. **Evans D., Paul N.** Election Security: Perception and Reality, *IEEE Privacy Magazine*, 19.02.04, available at: https://ieeexplore.ieee.org/document/1264850/ (date of access: 14.08.18).

7. **Gerlach J., Grasser U.** Three Case Studies from Switzerland: E-voting, Berkman Center Research Publication, 02.04.09, available at: https://www.alexandria.unisg.ch/52680/ (date of access: 14.08.18).

8. **Ibrahim S., Kamat M., Salleh M., Aziz S. R. A.** (2003) Secure E-Voting with Blind Signature, *Proceeding of the 4th National Conference of Communication Technology*, 14.01.03, available at: https://ieeexplore.ieee.org/document/1188334/ (date of access: 14.08.18).

9. **Jan J., Chen Y., Lin Y.** The Design of Protocol for e-Voting on the Internet, *Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology*. 19.10.01. (https://ieeexplore.ieee.org/document/962831/) (date of access: 14.08.18).

10. **Lubin J.** How Blockchain Will Disrupt Our Election System // *Internet resource "Futurism",* 7.11.2016, available at: https://futurism.com/how-blockchain-will-disrupt-our-election-system/ (date of access: 14.08.18).

11. **Nakamoto S.** A Peer-to-Peer Electronic Cash System // The Cryptography Mailing list, 31.10.08, available at: https://bitcoin.org/bitcoin.pdf (date of access: 14.08.18).

12. ***Krupnye*** *rossijskie banki "vhodât vo vkus" tehnologii blokčejn* (Large Russian banks "get into the taste" of the blockchain technology), 2017, available at: https://ria.ru/economy/20170727/1499301891.html (date of access: 14.08.18) (in Russian).

13. **Polâkov K.** *Kak vlasti Moskvy vnedrâût blokčejn v gorodskie proekty* (How Moscow authorities are introducing the blockchain into urban projects), available at: https://rb.ru/opinion/blockchain-moscow/ (date of access: 14.08.18) (in Russian).

14. ***"RosEvroBank"*** *razrabotal prototip sistemy udalennoj identifikacii klientov na baze tehnologii blokčejn ot Microsoft* ("RosEvroBank" developed a prototype of the remote client identification system based on the Microsoft blockchain technology), 2017, available at: https://news.microsoft.com/ru-ru/rosevrobank-razrabotal-prototip-sistemy-udalennoj-identifikatsii-klientov-na-baze-tehnologii-blokchejn-ot-microsoft/ (date of access: 14.08.18) (in Russian).