**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc9)

[1 СИСТЕМЫ ПЕРЕВОДА СРЕДСТВ МЕЖДУ ЭЛЕКТРОННЫМИ КОШЕЛЬКАМИ, СУЩЕСТВУЮЩИЕ СИСТЕМЫ ПЕРЕВОДА СРЕДСТВ МЕЖДУ ЭЛЕКТРОННЫМИ КОШЕЛЬКАМИ, ОСНОВАННЫЕ НА АЛГОРИТМАХ ZKP 5](#_Toc10)

[1.1 Система перевода средств между электронными кошельками и её общие характеристики 5](#_Toc11)

[1.2 Обзор существующих аналогов 7](#_Toc12)

[1.3 Обоснование выбора инструментальных средств 11](#_Toc13)

[ЗАКЛЮЧЕНИЕ 13](#_Toc14)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 14](#_Toc15)

# ВВЕДЕНИЕ

В современном мире наблюдается рост тенденций на внедрение блокчейн технологий в различных отраслях, в том числе и в экономической сфере. Это связано с тем, что данные технологии позволяют не только упростить и увеличить эффективность финансовых операций, но и обеспечить безопасность и прозрачность транзакций, что является неотъемлемым аспектом при проведении операций, связанных с денежными средствами.

При использовании приложений для электронных платежей остро стоит проблема о конфиденциальности данных, об их секретности. Большинство таких систем включают в себя сервисы для аутентификации, невозможности отрицания авторства. Такие возможности могу быть реализованы при помощи простых криптографических протоколов, например, TLS (Transport Layer Security). Протокол TLS – это протокол шифрования и аутентификации, он работает на транспортном уровне сетевой модели OSI, где отвечает за создание безопасных сессий обмена данными между браузером и сервером.

Однако существуют такие операции, которые невозможно защитить при помощи простых протоколов шифрования, вроде TSL. К таким операциям можно отнести электронные платежи, при проведении которых сохранение конфиденциальности является неотъемлемой частью, ведь при несоответствии приложения стандартам безопасности возникают риски утечки личных и финансовых данных пользователей. Также участники таких систем могут стать жертвой мошенничества, поскольку простые протоколы шифрования могут иметь уязвимости, из-за которых становится возможным получить доступ к персональным данным пользователей.

Более тонкие операции, такие как проведение электронных платежей, требуют внедрения более сложных криптографических алгоритмов, чтобы избежать возможности утечки пользовательских данных.

В связи с этим, актуальным является задача разработки системы перевода средств между электронными кошельками на основе алгоритмов доказательства с нулевым разглашением (Zero Knowledge Proof), что и является целью данной курсовой работы. Доказательство с нулевым разглашением (ZKP) представляет собой криптографический протокол, который позволяет одной стороне (доказывающему, prover, P) убедить другую сторону (проверяющего, verifier, V) в истинности какого-либо утверждения, не раскрывая при этом никакой информации, подтверждающей это утверждение. ZKP может быть интерактивным, когда доказывающий повторяет процесс доказательства для каждого проверяющего, а также неинтерактивным, когда доказывающий создаёт доказательство, которым может воспользоваться каждый человек, использующий то же доказательство.

Существует множество вариантов реализации алгоритмов доказательства с нулевым разглашением, например, протокол парольной аутентификации SRP (Secure Remote Password Protocol), или неинтерактивный криптографический протокол zk-SNARKs, но в данной курсовой работе будет использоваться набор криптографических протоколов Idemix.

# 1 СИСТЕМЫ ПЕРЕВОДА СРЕДСТВ МЕЖДУ ЭЛЕКТРОННЫМИ КОШЕЛЬКАМИ, СУЩЕСТВУЮЩИЕ СИСТЕМЫ ПЕРЕВОДА СРЕДСТВ МЕЖДУ ЭЛЕКТРОННЫМИ КОШЕЛЬКАМИ, ОСНОВАННЫЕ НА АЛГОРИТМАХ ZKP

## **1.1 Система перевода средств между электронными кошельками и её общие характеристики**

Предметная область настоящей курсовой работы – Система перевода средств между электронными кошельками на основе алгоритмов ZKP.

Основной целью данной области является обеспечение приватности и безопасности проводимых финансовых транзакций, путём внедрения в систему сложных криптографических протоколов, а именно алгоритмов доказательства с нулевым разглашением.

Одной из задач криптографии является двусторонняя интерактивная игра, в которой доказывающая сторона доказывает истинность некоторого утверждения другой стороне, проверяющей, не раскрывая сущности доказательства. Такая игра называется протоколом интерактивного доказательства или IP-протоколом (interactive proof – IP). Доказательство, получаемое при помощи такого IP-протокола, является секретным, потому что, во-первых, проверяющая сторона, убедившись в истинности доказанного утверждения, не способна самостоятельно повторить доказательство, и, во-вторых, после завершения протокола никто извне не способен понять сообщения, которыми обменивались стороны в процессе доказательства.

Такая конфиденциальность необходима во многих приложениях, в которых проводятся операции с использованием персональных данных, раскрытие которых может привести к фальсификации, подделыванию или краже личных данных. Например, при проведении голосований необходимо сохранять анонимность голосующих, чтобы предотвратить возможное принуждение или подтасовывание результатов, или при проведении электронных платежей, в процессе которых используются финансовые данные пользователей.

Доказательство с нулевым разглашением должно обладать следующими свойствами:

* Полнота: при корректном утверждении и при соблюдении обеими сторонами принципов протокола, проверяющий может однозначно убедиться в корректности и истинности утверждения;
* Устойчивость: при ложном утверждении проверяющая сторона должна иметь возможность убедиться в ложности утверждения;
* Нулевое разглашение: при истинности утверждения проверяющая сторона не сможет узнать ничего, кроме того факта, что утверждение верно. Другими словами, простого знания утверждения (а не секрета) достаточно, чтобы убедиться в том, что доказывающий знает этот секрет.

ZKP относится к «вероятностным доказательствам». Это класс криптографических протоколов, в которых проверяющая сторона может сделать вывод о справедливости утверждения лишь с некоторой вероятностью.

Протоколы ZKP можно разделить на интерактивные и неинтерактивные. В интерактивных протоколах стороны должны быть постоянно «на связи» и обмениваться сообщениями (это называется раунды взаимодействия). А в неинтерактивных протоколах взаимодействие между участвующими сторонами сводится к одному раунду, пересылке ZK-доказательства от доказывающего к проверяющему.

Использование интерактивных протоколов в распределенных реестрах ограничено необходимостью постоянного обмена сообщениями между доказывающим и проверяющим для проведения множества раундов взаимодействия. На практике такие протоколы не изучаются и не применяются в распределенных реестрах.

В отличие от них, неинтерактивные протоколы лучше подходят для распределенных реестров, так как требуют лишь одного раунда взаимодействия: отправки доказательства и ответа при его проверке.

Распределенные реестры характеризуются открытым хранением данных, при этом информация о транзакциях не скрывается. Однако нельзя скрыть отдельные транзакции, данные о них или некоторые поля транзакции.

На рисунках 1.1 и 1.2 представлены алгоритмы работы интерактивного и неинтерактивного протоколов доказательства с нулевым разглашением.

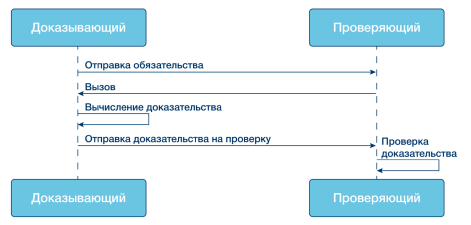


Рисунок 1.1 – Алгоритм работы интерактивного протокола доказательства с нулевым разглашением



Рисунок 1.2 – Алгоритм работы неинтерактивного протокола доказательства с нулевым разглашением

## **1.2 Обзор существующих аналогов**

Алгоритмы доказательства с нулевым разглашением находят практическое применение в различных областях, таких как блокчейн, криптовалюты и децентрализованные финансы (DeFi). ZKP позволяет проверять информацию без её раскрытия, что повышает конфиденциальность и безопасность. Многие проекты DeFi уже используют технологию ZKP для обеспечения большей конфиденциальности в сферах кредитования, займов или торговли. Некоторые блокчейны также внедряют роллапы на основе ZKP или zkEVM (Zero Knowledge Ethereum Virtual Machine).

Для анализа были выбраны только некоторые из существующих решений, а именно: криптовалюта Monero, криптовалюта ZCash.

**1.2.1 Криптовалюта Monero**

Monero (официальные тикер – XMR) – это криптографическая валюта, которая была создана на базе блокчейна ByteCoin, в 2014 году. В основе данной криптовалюты лежит протокол CryptoNote, обеспечивающий высокий уровень анонимности каждой транзакции.

Большинство существующих криптовалют, таких как Bitcoin или Ethereum, имеют прозрачные блокчейны, что означает, что транзакции в них прозрачны и отслеживаемы, также адреса отправителя и получателя могут быть связаны с реальной личностью человека. Monero использует криптографию для защиты адресов пользователей, а также для самих транзакций.

Каждая транзакция Monero по умолчанию «запутывает» адрес отправки и получения, а также суммы транзакции. Такая конфиденциальность означает, что деятельность каждого пользователя Monero повышает конфиденциальность всех других пользователей сети, в отличие от выборочно прозрачных криптовалют, как ZCash.

CryptoNote в сочетании с обфускацией («запутыванием») транзакций приводят к «пассивному смешиванию», когда все транзакции в сети анонимны и в случае необходимости каждый участник сможет применить правдоподобное отрицание. На рисунке 1.3 представлен принцип шифрования транзакции по протоколу CryptoNote.

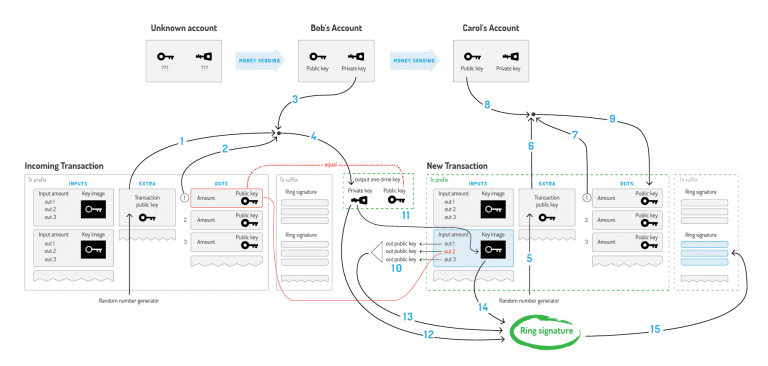


Рисунок 1.3 – Принцип работы протокола CryptoNote

Можно выделить следующие недостатки данной криптовалюты:

* Monero много раз подвергалась критике за свою анонимность, поскольку власти считают, что это способствует распространению нелегальной информации и товаров. Однако анонимность в сети не является абсолютной, и существуют уязвимости, которые могут быть использованы для нарушения приватности транзакций;
* Транзакции в сети являются довольно тяжеловесными, их объём в 8 раз больше чем транзакции Bitcoin, что отражается на скорости выполнения транзакций;
* Также, в 2018 году была обнаружена уязвимость, благодаря которой было возможным «сжигать» депозит, выраженный в криптовалюте, но эта проблема была устранена после выпуска патча с названием Devs Patch.

**1.2.2 Криптовалюта ZCash**

ZCash (официальный тикер – ZEC) – криптовалюта, ориентированная на конфиденциальность которая является форком (fork) Bitcoin.

Форк (fork) – копирование исходного кода с внесением в него изменений.

Основной особенностью ZCash является настраиваемость прозрачности транзакций. В данной сети пользователи сами могут выбирать либо защищённые (частные), либо прозрачные (публичные) детали транзакции.

В основе функции конфиденциальности ZCash лежат алгоритмы доказательств с нулевым разглашением. ZCash представил zk-SNARK, набор инструментов с нулевым кратким неинтерактивным аргументом знаний, при помощи которого обеспечивается шифрование транзакций в блокчейне, при этом проверяя их легитимность посредством сетевого консенсуса.

ZCash использует два типа адресов кошельков: z-адреса (частные) и t-адреса (прозрачные). В зависимости от адресов, используемых отправителем и получателем, существуют 4 типа транзакций:

* Частные транзакции: обе стороны используют z-адреса кошельков, сохраняя детали и суммы транзакций анонимными;
* Публичные транзакции: обе стороны используют t-адреса кошельков, благодаря чему все детали транзакции прозрачны;
* Деэкранирующие транзакции: отправитель использует z-адрес, а получатель – t-адрес, в результате чего раскрываются данные о получателе и сумме транзакции;
* Экранирующие транзакции: отправитель использует t-адрес, а получатель – z-адрес, в этом случае общедоступными становятся данные отправителя, а также сумма транзакции.

На рисунке 1.4 представлен процесс проведения транзакции в сети ZCash

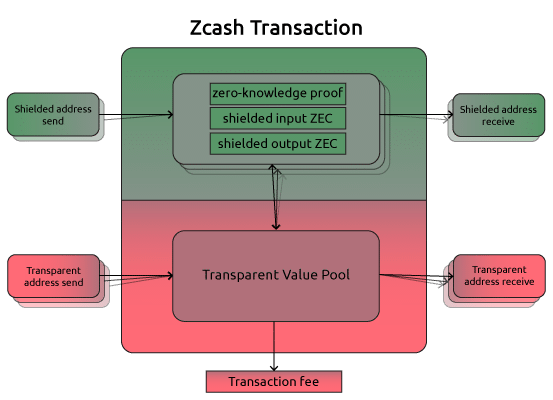


Рисунок 1.4 – Принцип проведения транзакции в ZCash

К недостаткам данной криптовалюты можно отнести низкую скорость проведения транзакций, из-за множества сложных математических вычислений, а также то, что официально поддерживается только на операционной системе Linux.

## **1.3 Обоснование выбора инструментальных средств**

Реализацию системы перевода средств между электронными кошельками на основе алгоритмов ZKP было решено проводить с использованием Hyperledger Fabric и Identity Mixer.

Hyperledger Fabric – это блокчейн-платформа, написанная на языке программирования Go с открытым исходным кодом от Linux Foundation. С её помощью можно создавать блокчейн-приложения и управлять доступом и разрешениями для данных в цепочке блоков. Также, как и другие блокчейн-технологии он использует реестр, смартконтракты и систему, с помощью которых участники управляют своими транзакциями.

Основное отличие HLF (Hyperledger Fabric) от других блокчейн-систем заключается в том, что он является «закрытым и контролируемым». В отличие от открытых систем, позволяющих неидентифицированным пользователям участвовать в работе сети (например, механизм консенсуса PoW в Bitcoin), участники блокчейнов Hyperledger Fabric обязаны проходить регистрацию с получением сертификатов. В дальнейшем, уровень доступа к отдельным структурам блокчейна может быть настроен с помощью анализа идентификаторов, например, отдельные группы участников могут создавать каналы, которые будут являться отдельным регистром транзакций, доступным только им.

Реестр Hyperledger Fabric имеет состоящую из двух компонент подсистему: world state (состояние мира) и transaction log (журнал транзакций). Каждый участник имеет копию реестра каждой сети Hyperledger Fabric, в которой он состоит.

Компонент world state описывает состояние реестра в определенный момент времени. Это база данных реестра. Компонент transaction log записывает все транзакции, которые привели к текущему world state; это обновленная история для world state. В реестре, тогда, это комбинация базы данных world state и истории transaction log.

Реестр имеет сменное хранилище данных для world state. По умолчанию, это база LevelDB, работающая со структурами данных типа «ключ — значение». В сменном transaction log нет необходимости, он просто записывает значения «до» и «после» базы данных реестра при использовании блокчейн-сети.

Все смартконтракты Hyperledger Fabric написаны через чейнкоды и вызываются через внешнее приложение, когда ему требуется провзаимодействовать с реестром. В большинстве случаев, чейнкод взаимодействует только с базой данных реестра – компонентом world state (например, совершая поисковые запросы).

Чейнкод может быть написан на нескольких языках программирования. В настоящее время поддерживаются Go и Node.js.

Identity Mixer (Idemix) – набор криптографических протоколов, обеспечивающих надежную аутентификацию вкупе с сохраняющими конфиденциальность свойствами, такими как анонимность, возможность совершать транзакции без выдачи сторон транзакции, и несвязность (unlinkability), возможность совершить одной identity несколько транзакций, не выдав, что все эти транзакции были совершены одной и той же identity.

В процессе Idemix участвуют три актора: пользователь (user), издатель (issuer) и верификатор (verifier). На рисунке 1.5 представлен процесс взаимодействия акторов.

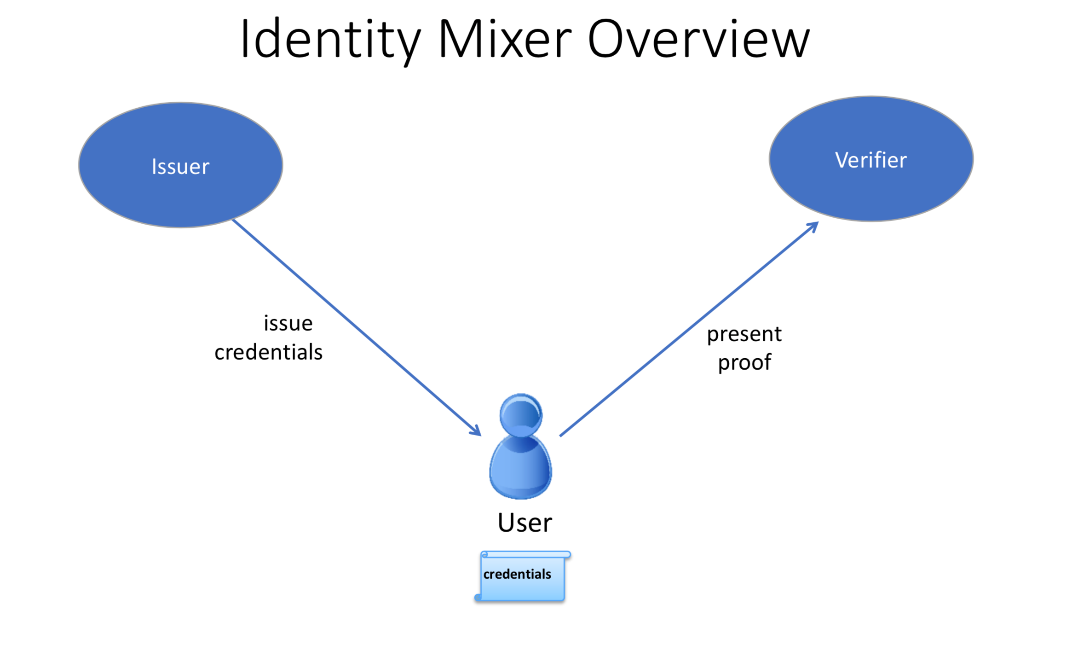


Рисунок 1.5 – Процесс взаимодействия акторов в Idemix

Издатель удостоверяет набор атрибутов пользователя - выпускает цифровой сертификат, далее именуемый «удостоверение» (credential).

Потом пользователь генерирует доказательство с нулевым разглашением, что он владеет удостоверением и также выборочно раскрывает атрибуты по собственному желанию. Так как доказательство ничего не разглашает, оно не раскрывает никакой другой информации про верификатора, издателя или кого-либо еще.

# ЗАКЛЮЧЕНИЕ

В данном разделе был проведён анализ системы перевода средств между электронными кошельками на основе алгоритмов ZKP. Были рассмотрены принципы работы протоколов доказательства с нулевым разглашением.

Было выяснено, что стандартные протоколы шифрования не могут обеспечить полную безопасность конфиденциальных данных в системах перевода средств между электронными кошельками, и для обеспечения лучшей защищенности необходимо использовать более тяжелые криптографические протоколы, например, доказательства с нулевым разглашением.

Также были рассмотрены некоторые аналоги данной курсовой работы. Были рассмотрены две криптографические валюты Monero и ZCash, изучены принципы их функционирования, а также алгоритмы протоколов, которые используются ими для шифрования данных. Также были выделены основные недостатки данных аналогов.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Mao, W. (2003). Modern Cryptography: Theory and Practice. Prentice Hall.
2. Goldwasser, S., Micali, S., and Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing, 18(1), pp. 186–208.
3. Blum, M., Feldman, P., and Micali, S. (1988). Noninteractive Zero-Knowledge and Its Applications. Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, pp. 103–112.