УДК 336.743

Д. В. Яковчик, А. К. Крамаренко
Учреждение образования «Брестский государственный технический университет», Брест, Республика Беларусь

ОБЩЕДОСТУПНЫЕ И ЭКСКЛЮЗИВНЫЕ БЛОКЧЕЙНЫ

Введение. Торговые операции в интернете на данный момент стали почти полностью полагаться на доверенные третьи стороны при проведении электронных платежей. Поскольку такая модель, основанная на доверии, страдает от некоторых недостатков (низкая скорость обработки, цензура), требуется реорганизация структуры таких операций. Одним из качественных решений данной проблемы является технология обработки данных, упорядоченных по определенным правилам в связный список. Такая технология называется блокчейн. Первой и наиболее известной системой платежей применившей блокчейн является биткоин. Блокчейн может быть реестром транзакций не только в криптовалютах, а распространяться на различные финансовые операции, идентификацию пользователей и применяться в банковских и государственных учреждениях.

Основная часть. Блокчейн обладает отличием от традиционной централизованной системы цифровых платежей, заключающийся в децентрализации системы. При транзакциях в децентрализованных системах не нужно полагаться на третью сторону, все доверие исходит из математических свойств системы. Также блоки транзакций защищены криптографически, а атаки на такую систему будут иметь высокую стоимость.

Однако блокчейны могут быть как общедоступными, например как используемые в биткоине, так и эксклюзивными. Именно применяемые в банковских и государственных структурах блокчейны являются эксклюзивными. Необходимость в таком разграничении появилась из-за недоверия финансовых организаций к общедоступным блокчейнам в связи с определенным наборам недостатков [1; 2].

Первой проблемой общедоступных систем является неспособность определить участников транзакций. Теоретически, блок в таких системах может создать любой пользователь при наличии достаточных вычислительных ресурсов анонимно, что противоречит законодательству во многих государствах. Однако на практике личность участников транзакций можно установить благодаря использованию специализированного оборудования ASIC — устройства, выполняющего добычу криптовалюты. Также участником может быть включена цифровая подпись для идентификации личности.

Следующей проблемой является конфиденциальность, которую не могут оказать системы, история транзакций которых являются общедоступными. По этой причине транзакции могут быть использованы в противоправных действиях [3]. Также из-за отсутствия подписей при идентификации используются открытые ключи для нескольких платежей. Закрытые же блокчейны могут использовать секреты, которые, например, будут иметь некоторые значения, а у узлов сети к этим значениям не будет доступа.

Также с точки зрения законодательств многих государств криптовалюты имеют проблемы с определением статуса активов. Криптовалюты не являются физическими объектами и не имеют юридического признания как собственность, потому не имеют статуса активов с правом собственности на предъявителя. Однако, криптовалюты могут быть признаны как имущество в некоторых юрисдикциях, где они регулируются законодательством. В таких случаях, владельцы криптовалют обладают определенными правами и обязанностями в соответствии с законодательством. Однако в данном случае общедоступные и закрытые блокчейны не имеют различий, так как их статус остается неопределенным.

Блокчейны с внутренней валютой (токены) могут быть непривлекательным для банковских или государственных учреждений, из-за чего блокчейны без внутренней валюты для таких организаций более предпочтительны. Такой дизайн блокчейна называется «блокчейн без токена» или «безтокенный блокчейн». Вместо токена, в этом типе блокчейна используется система репутации, которая позволяет участникам совершать транзакции и получать вознаграждения на основе своей активности и участия в сети.

Безтокенный блокчейн может быть более привлекательным для учреждений, так как он не требует создания и поддержки внутренней валюты, что может быть сложно и дорого. Кроме того, отсутствие токена может облегчить процесс регулирования и снизить риски для учреждений. Однако, безтокенный блокчейн может иметь свои недостатки, так как он может быть менее привлекательным для инвесторов и пользователей, которые могут предпочесть использование токена в качестве цифрового актива или средства оплаты. Кроме того, система репутации может быть менее прозрачной и объективной, чем использование токена [3; 4].

Следующей проблемой общедоступных блокчейнов является проблема завершенности транзакций. Эта проблема возникает из-за того, что транзакции должны быть подтверждены большинством участников сети, прежде чем они будут считаться окончательными. Это может занять много времени, особенно если сеть перегружена или если транзакции содержат недостаточно высокие комиссии.

Кроме того, в некоторых случаях транзакции могут быть отклонены или отменены после того, как они были отправлены. Это может произойти, например, если участник сети обнаружит ошибку в транзакции или если она была отправлена на адрес, который не существует.

Для решения этой проблемы разработчики блокчейнов реализуют различные механизмы, такие как ускорение транзакций, улучшение алгоритмов консенсуса и увеличение размера блоков. Однако, эти механизмы могут привести к другим проблемам, таким как увеличение размера блокчейна или ухудшение децентрализации сети.

Атака с цензурой транзакций на блокчейн может быть осуществлена, если кто-то получает контроль над достаточно большим количеством узлов (нод), которые обрабатывают транзакции в сети блокчейн. Это может произойти, если атакующий смог получить доступ к приватным ключам [4].

Если атакующий получает контроль над достаточным количеством узлов, он может начать блокировать или отклонять определенные транзакции, что может привести к серьезным последствиям для децентрализованной сети блокчейн. Например, это может привести к задержкам в обработке транзакций, увеличению комиссий за транзакции и ограничению доступа к определенным ресурсам.

Для защиты от такой атаки необходимо использовать механизмы голосования и децентрализации, которые позволяют распределять контроль над узлами между различными участниками сети. Кроме того, важно использовать средства шифрования и многофакторную аутентификацию для защиты приватных ключей, используемых для управления узлами [4].

Заключение. Эксклюзивные блокчейны больше соответствуют законодательству и могут быть привлекательны для учреждений в среднесрочной перспективе. Однако для обычного пользователя все также остается привлекательны общедоступные блокчейны, в которых лучше организуются одноранговые сети между пользователями. Человеческий фактор в общедоступных системах сведен к минимуму. Общедоступные блокчейны могут стать основой инфраструктуры блокчейнов, а эксклюзивные приложения могут строиться на их основе.

Список цитируемых источников

1. *Бакулина, А. А.* Блокчейн как объект оценки : моногр. / А. А. Бакулина, В. В. Григорьев. — Финансовый ун-т при Правительстве Рос. Федерации. — М. : Русайнс, 2021. — 198 с.

2. *Табернакулов, А.* Блокчейн на практике / А. Табернакулов, Я. Койфманн. — М. : Альпина Паблишер, 2019. — 257 с.

3. *Чурилов, А. Ю.* Правовое регулирование применения технологии блокчейн : моногр./ А. Ю. Чурилов. — М. : Юстицинформ, 2021. — 151 с.

4. *Цихилов, А.* Блокчейн: принципы и основы / А. Цихилов. — М. : Альпина Паблишер : Интеллектуальная Литература, 2019. — 186 с.

УДК 004.42

М. В. Яснюк, А. В. Шах

Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь

РАЗРАБОТКА КОМПЬЮТЕРНОЙ ИГРЫ «МАДЖОНГ»

Введение. Невозможно отрицать тот факт, что за последние 30 лет компьютерные игры были значительно развиты, и в настоящее время многие считают игровую индустрию своего рода искусством, наравне с музыкой, живописью и кино. Отличительной особенностью некоторых компьютерных игр является активное участие игрока в событиях виртуального мира, что является причиной полного погружения в атмосферу игры. Целью данной работы является разработка игры «Маджонг» [1].

Программа предлагает на выбор 4 игровых локации. Это лишь визуальная составляющая игры, на сам процесс это не влияет.

Программа также предлагает 3 фигуры на выбор. У каждой фигуры разное время в зависимости от сложности ее разбора.

Суть игры состоит в том, чтобы как можно быстрее собрать предложенную фигуру и при этом не попасть в так называемую «ловушку Маджонга», при которой игра приходит в тупик из-за отсутствия возможности найти вторую фишку. Игра завершается либо при полном разборе фигуры, либо при окончании времени. При любых обстоятельствах программа сообщит об этом.

Основная часть. Для реализации приложения была выбрана среда программирования Visual Studio и объектно-ориентированный язык программирования C#, а также приложение Adobe Photoshop CC 2019 для прорисовки 3D-моделей фишек. Рассматриваемый язык программирования пользуется спросом, но не у всех разработчиков. У Шарпа немало сильных и слабых сторон, зная которые, программист сможет понять, насколько соответствующий «способ создания программного обеспечения» ему подходит [2].

При загрузке игры отображается первое окно, где нужно выбрать локацию на рисунке 1.