Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИЧЕРСИТЕТ»**

**(МОСКОВСКИЙ ПОЛИТЕХ)**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Отчет выполнения по Проектной деятельности

**«Оценка уязвимостей смарт-контрактов»**

Выполнила: Николаец Д.И

Студент 3-го курса

Группы 171-361

Москва 2020

**Цели задачи 1** проекта «Оценка уязвимостей смарт-контрактов»:

* Анализ 4-5 Blockchain-платформ для написания смарт-контрактов, выделение особенностей Blockchain-платформ, преимуществ и недостатков, а также описание характеристики. Принцип разработки смарт -контрактов на каждой из Blockchain-платформ
* Сравнение проанализированных Blockchain-платформ и выбор наиболее оптимальной платформы.

**Результат работы:**

* Рассмотрен сравнительный анализ Blockchain платформ Дана оценка проблеме доверительных отношений между участниками сделки и описан способ предотвращения проблем, при их возникновении. Приведены примеры глобальных и приватных Blockchain - платформ, их характеристики, а также плюсы и минусы использования данных структур.
* На основе плюсов и минусов Blockchain-платформ сформирован вывод какую платформу целесообразно использовать для работы со смарт-контрактами.

Как выбрать правильную платформу для работы со смарт-контактами и на что стоит обратить внимание в первую очередь?

Для того, чтобы заключить любую сделку, необходимо обратиться к нотариусу или адвокату, оплатить документы и ждать их оформление. Зачастую, многие пункты этих документов содержат ссылки на законодательные статьи, которые можно интерпретировать под себя, обойти. В случае невыполнения условий сделки, в реальной жизни людям приходится обращаться в суд, снова тратить деньги на процесс и доказывать свою правоту. При заключении таких сделок вообще не может идти речь о доверии участников договора.

Smart-контракты дают возможность безопасно обмениваться деньгами, акциями, собственностью и другими активами напрямую, без участия посредников.

Для этого была разработана программа, которая следит за выполнением обязательств обеих сторон, прописанных в контракте, а также автоматически взымает штрафы за нарушение или невыполнение условий сделки. Умные контракты обеспечивают безопасность сделки и лишены риска неоднозначной трактовки условий, благодаря тому, что основаны на криптографии. Это более выгодные сделки в материальном плане, так как человеку не нужно платить юристам, посредникам или подавать в суд при невыполнении контракта. При чем выполнение условий сделки происходит автоматически с минимальными затратами на их сопровождение, без привлечения третьих лиц (посредников).

Умный контракт (англ. Smart contracts) — электронный алгоритм, описывающий набор условий, выполнение которых влечет за собой некоторые события в реальном мире или цифровых системах. Для реализации умных контрактов требуется децентрализованная среда, полностью исключающая человеческий фактор, а для возможности использования в умном контракте передачи стоимости требуется криптовалюта.

Для анализа я выбрала 5 популярных Blochain-platform: ***Ethereum***, ***EOS, NEO, WAVES, STELLAR***. Рассмотрим характеристики платформ, их преимущества и недостатки.

***Ethereum*** является первой блокчейн платформой в которой возможно исполнение тьюринг-полных смарт-контрактов. Полнота по Тьюрингу в смарт-контрактах позволяет выполнить любую математически вычислительную функцию. Ethereum завоевал популярность у пользователей благодаря возможности выпуску токенов на платформе Эфириума, легкому проведению ICO или DAICO, созданию децентрализованных приложений, а также весьма гибким возможностями по созданию смарт-контрактов.

В настоящий момент Ethereum является самой популярной криптовалютой среди разработчиков и наиболее распространенной по числу децентрализованных приложений. Большинство смарт-контрактов разработанных нашей командой также созданы с помощью языка Solidity и виртуальной машины Ethereum. Сфера применений смарт-контрактов в Ethereum чрезвычайно широка и любую логически поданную идею можно реализовать с помощью данной сети.

***EOS*** на сегодняшний день является второй по популярность блокчейн платформой по применению смарт-контрактов и первой по активному числу транзакций. Отличительной особенностью EOS можно назвать масштабируемость, параллельные вычисления и высокую пропускную способность сети. В EOS используется алгоритм консенсуса Delegated Proof-of-Stake что повышает пропускную способность сети, но плохо сказывается на её децентрализации.

***NEO*** - блокчейн-платформа разрабатываемая сообществом китайских программистов. Изначально блокчейн NEO создавался как альтернатива Ethereum, но с развитием конкуренции в этой области разработчики NEO стали внедрять собственные решения. Монеты NEO были изначально добыты премайном, где половина была продана на ICO и половина осталась в руках разработчиков. Общая эмиссия NEO - 100 миллионов монет.

Интересным отличием NEO является поддержка популярных языков программирования для разработки смарт-контрактов, например таких как Java, F#, C#, Kotlin, Go и Python. Ещё одной особенностью является использование отдельной криптовалюты GAS для оплаты транзакций и выполнения смарт-контрактов, но в отличие от газа в Ethereum криптовалюта GAS автоматически начисляется на баланс пользователя при хранении NEO на аккаунте. Смарт-контракты NEO не поддерживают сторонние библиотеки, а используется только библиотека зависимостей NEO-SmartContract-DevPack. Байт код смарт-контрактов представлен в формате .avm. Развертывание смарт-контракта в блокчейне NEO стоит 100-1000 GAS.

***Stellar*** появился в 2014 году, когда часть команды провела хардфорк Ripple и запустила собственную сеть, предназначенную в первую очередь для валютных операций. Ноды Stellar хранят записи о всех счетах в сети и синхронизируются между собой образуя так называемую бухгалтерскую книгу. Алгоритм консенсуса сети позволяет проводить транзакцию за 4-5 секунд.

Stellar позволяет комфортно управлять микротранзакциями, в сети низкая комиссия и повышенная технологическая совместимость с финансовым рынком. Блокчейн Stellar поддерживает работу смарт-контрактов, однако они обладают ограничениями и сложный функционал на нём невозможен. В то же время на Stellar доступны мультиподписи, атомарность транзакций их последовательность и временные ограничения.

***Waves*** - блокчейн платформа имеющая российское происхождение была основана в 2016 году. Её отличительно особенностью является алгоритм консенсуса LPoS, что расшифровывается как Leased Proof of Stake или арендованное подтверждение доли. Владельцы монет Waves могут отдавать их в аренду нодам и получать за это вознаграждение от её работы при создании новых блоков блокчейна.

В основной сети Waves сегодня работают ограниченные по функционалу смарт-контракты которые позволяют выполнять следующие сценарии: создание токена, заморозка токена, выплаты по расписанию, двухфакторная аутентификация, кошельки с мультиподписью, смарт-аккаунты, смарт-активы, атомарные свопы, работа с оракулом внешних данных.

В таблице представлено сравнение наиболее популярных блокчейн-платформ.

|  |  |  |
| --- | --- | --- |
| Платформа | Достоинства | Недостатки |
| Ethereum | Широкое распространение  Гибкость  Низкий порог вхождения  Четкие рекомендации для разработчиков  Много литературы / справок доступно | Оплата транзакций в сети (gas)  Нагрузка на сеть  Проблемы с безопасностью  Проблемы масштабируемости  Относительно медленное подтверждение транзакции  Дороже, чем другие платформы |
| NEO | Алгоритм консенсуса dBFT  Высокая скорость транзакций  Централизация     * Поддержка многих языков программирования, расширяющая перспективы коммерческого применения платформы. | Разработчики могут самостоятельно влиять на сеть и её участников – замораживать счета, следить за операциями, предоставлять данные властям по их требованию.  Перспективы NEO находятся в большой зависимости от политической воли руководства Китайской Народной Республики.  Отсутствие анонимности. |
| EOS | Высокая масштабируемость  Высокая скорость транзакций  Достаточно широкий функционал  Бесплатные транзакции | Отсутствие главной сети EOS. Чрезмерная централизация |
| STELLAR | Высокая скорость  Микроплатежи | Не очень подходит для разработки более сложных смарт-контрактов  Ограниченный функционал |
| WAVES | Высокая скорость  Имеет сильные стратегические партнерства  Имеет функционирующую децентрализованную биржу  Алгоритм консенсуса LPoS  Приватный блокчейн Vostok | Есть некоторые проблемы в области безопасности |

Рассмотрим непосредственно характеристики блокчейн-платформ.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NAME | Ethereum | Waves-NG | EOS | NEO | Stellar |
| Mainnet launch | 07/2015 | 04/2016 | 06/2018 | 10/2016 | 09/2015 |
| Contract Language | Solidity (Serpent Mutan LLL ) | Ride | C++, С | C#, JAVA, JS, PYTHON.NET | Js,go,python,php,swift, ruby, scala |
| Price | 3-4 цента | 0.001-0.009 $ | 0.03 $ | 0 для своей валюты и 0.001 для других | 1 цент для 10000 транзакций |
| TPS | 12-25 p/s | 100 p/s | Max:4000  Avg:50 | 1000 p/s | 2000 p/s |
| SDK | + | + | + | + | + |
| Consensus mechanixm | PoW | LPos | DPos | dBFT | SCP |
| Block time | 15 seconds | 3 sec | 0.5 sec | 15 Sec | 5 sec |

Cложно выбрать «лучшую» платформу. Все они имеют свои преимущества и недостатки. Что важно иметь в виду, так это выбрать платформу, которая лучше всего подходит для вас.

* Сфера применений смарт-контрактов в Ethereum чрезвычайно широка и любую логически поданную идею можно реализовать с помощью данной сети. Если вы хотите платформу, которая имеет сильное сообщество разработчиков, то вы идете на Ethereum.
* Если вы хотите платформу, которая подчеркивает скорость и масштабируемость, но не очень заботится о децентрализации, то EOS-это именно то, что вам нужно.
* Waves-это перспективная платформа, которая делает ее простой для среднего человека, работающего с blockcano, crowdfunding и помогает ему обналичивать криптовалюты. Если вы хотите платформу, которая обладает высокой масштабируемостью и проводит невероятно быстрые транзакции, то вам подходит Waves. Главным ключевым моментом этой платформы является то, что даже новички могут использовать эту платформу, поскольку это не требует высокого уровня технического языка.
* Блокчейн Stellar поддерживает работу смарт-контрактов, однако они обладают ограничениями и сложный функционал на нём невозможен. В то же время на Stellar доступны мультиподписи, атомарность транзакций их последовательность и временные ограничения.
* Но если вы хотите платформу, которая соединяет банки, платежные системы и людей, то ваш выбор STELLAR. Интегрируйтесь, чтобы быстро, надежно и почти бесплатно перемещать деньги.
* Если вы хотите платформу, которая имеет все преимущества виртуальной машины Ethereum, но отличается большей масштабируемостью и не мешает разработчикам языковыми барьерами, то ваш выбор NEO. В ethereum вам нужно будет научиться основательно кодировать смарт-контракты, в то время как в Neo вы можете даже использовать Javascript для кодирования смарт-контрактов.

Считаю, что лучшей платформой для написания смарт-контрактов является EOS. Рассмотрев ее характеристики, преимущества и недостатки, можно сделать вывод, что платформа EOS является технологически интересной и потенциально востребованной в широком диапазоне применений смарт-контрактов.