Секция «Информационное общество, цифровая экономика и информационная безопасность»

Технология распределенного реестра в системах защиты информации

Научный руководитель – Крылов Григорий Олегович

Тараненко Дмитрий Александрович
Аспирант
Финансовый университет, Факультет анализа рисков и экономической безопасности, Информационная безопасность, Москва, Россия
E-mail: ostrvi@mail.ru

После того, как Satoshi Nakamoto опубликовал The Bitcoin Whitepaper[n1] в конце 2008 года, технология распределенного реестра[1] в основном рассматривалась в качестве драйвера цифровой экономики. Несмотря на то, что главные преимущества указанной технологии прозрачность проводимых транзакций, децентрализованность и открытость весьма полезны при заключении контрактов и проведении сделок, поскольку все участники процесса знают о шагах своих партнеров, а скомпрометировать хранимые в реестре данные очень сложно. Эти свойства привели к тому, что распространение технологии столкнулось с противоборством со стороны правительственных и традиционных финансовых институтов, поскольку в системе, построенной на блокчейн, как в первой криптовалюте Bitcoin[n2], отсутствует необходимость в посреднике для проведения транзакций, поэтому сильно усложняется контроль. Однако применимость технологии распределенного реестра не ограничена криптовалютами. Блокчейн становится подспорьем в таких сферах жизни общества, в которых необходимо обеспечить сохранность данных: IoT, юриспруденция, медицина, страхование и др. Решения, основанные на технологии распределенного реестра, относятся к числу наиболее часто обсуждаемых вариантов для повышения кибербезопасности[n3]. Ниже рассмотрим, как блокчейн используется для обеспечения информационной безопасности.

1. Децентрализованные решения для хранения данных. В современном мире объем конфиденциальных данных постоянно растет. Эти данные весьма привлекательны для киберпреступников[2], а традиционное хранение всего массива конфиденциальных данных в одном месте очень удобно для хакеров. Решения для хранения данных на основе технологии распределенного реестра набирают популярность. Например, облако данных разработанное компанией Apollo[n4] позволяет пользователям архивировать данные в блокчейне и предоставлять разрешение на доступ третьим сторонам. Ключ криптографического доступа может быть отозван в любое время, что еще больше снижает риск взлома. Благодаря децентрализованному характеру технологии распределенного реестра, киберпреступники больше не имеют единой точки входа и не могут получить доступ ко всем хранилищам данных в случае их проникновения. Эта функция является одной из основных причин, по которым блокчейн сейчас часто рассматривается как решение для обеспечения конфиденциальности данных.

2. Безопасность IoT[3] устройств. Киберпреступники часто получают доступ к информационным системам, используя слабые стороны периферийных устройств. IoT устройства, такие как интеллектуальные термостаты, дверные звонки, даже камеры безопасности, очень уязвимы, поскольку им не уделяется должного внимания при разработке и внедрении системы защиты информации. Блокчейн также может защитить весь обмен данными между IoT устройствами[n5]. Его можно использовать для обеспечения весьма безопасной передачи данных в режиме реального времени и обеспечения своевременной

связи между устройствами, расположенными на большом расстоянии друг от друга. Кроме того, IoT устройства могут сформировать групповой консенсус относительно нормальных явлений в данной сети и заблокировать любые узлы, которые ведут себя подозрительно, что не будет требовать централизованного органа управления сетью и проверки данных, проходящих через нее.

3. Безопасный DNS[4]. DNS весьма централизован, поэтому киберпреступники могут взломать связь имени домена с IP-адресом[5] и направлять пользователей на сайты мошенников или просто сделать сайт недоступным. Кроме того, DNS-атаки можно сочетать с DDoS-атаками[6], что делает веб-сайты совершенно непригодными для использования в течение длительных периодов времени. Сегодня такая проблема решается созданием журналов и включением оповещений о подозрительных действиях в режиме реального времени[n6]. Система, основанная на блокчейне, может повысить безопасность веб-сайтов. Поскольку он децентрализован, хакерам будет намного сложнее найти и использовать отдельные уязвимости. Информация о имени домена может храниться неизменным образом в распределенном реестре, а подключение может обеспечиваться с использованием умных контрактов.

4. Обеспечение безопасности при обмене сообщениями. Мессенджеры и социальные сети становятся очень популярными платформами для общения, но при этом собирается много метаданных пользователей. Одни системы обмена сообщениями используют сквозное шифрование, а другие начинают использовать блокчейн для обеспечения безопасности передаваемой информации[n7]. В настоящее время большинству приложений обмена сообщениями не хватает стандартного набора протоколов безопасности и единой структуры API[7] для обеспечения связи между мессенджерами. Возникающие безопасные коммуникационные экосистемы блокчейна решают эту проблему и работают над созданием новой системы унифицированных коммуникаций, что является хорошим решением, поскольку он защищает обмен данными и обеспечивает связь между различными платформами обмена сообщениями.

Технология распределенного реестра обеспечивает фундаментально иной подход к кибербезопасности, ключевым фактором которого является децентрализация. Когда контроль доступа, сетевой трафик и даже сами данные больше не хранятся в одном месте, киберпреступникам становится гораздо сложнее их использовать. Новые угрозы в сети Интернет будут возникать постоянно и блокчейн может послужить мощным инструментом, который будет использован для повышения надежности информационных систем.

[1] Здесь и далее, в целях упрощения, термин технология распределенного реестра употребляется взаимозаменяемо с термином блокчейн.

[2] Здесь и далее, в целях упрощения, термин киберпреступник употребляется взаимозаменяемо с термином хакер.

[3] Internet of Things

[4] Domain Name System

[5] Internet Protocol Address

[6] Distributed Denial of Service attack

[7] Application Programming Interface

Источники и литература

1) Nakamoto, Satoshi Bitcoin: A Peer-to-Peer Electronic Cash System // bitcoin.org URL: https://bitcoin.org/bitcoin.pdf (Accessed 01.03.2020).

2) Поппер Н. Цифровое золото: невероятная история Биткойна или о том, как идеалисты и бизнесмены изобретают деньги заново / Н. Поппер. – М.: Вильямс, 2016. – 350 с.

3) Andrew Arnold, 4 Promising Use Cases Of Blockchain In Cybersecurity // forbes.com URL: https://www.forbes.com/sites/andrewarnold/2019/01/30/4-promising-use-cases-of-blockchain-in-cybersecurity/#73cd1b833ac3 (Accessed 01.03.2020).

4) The Apollo data cloud // apollocurrency.com URL: // forbes.com URL: https://apollocurrency.com/en/platform (Accessed 01.03.2020). (Accessed 01.03.2020).

5) IoT Security Maturity Model: Description and Intended Use // Industrial Internet Consortium URL: https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_FINAL_Updated_V1.1.pdf (Accessed 01.03.2020). (Accessed 01.03.2020).

6) Tail Log Files // SolarWinds Worldwide URL: https://www.papertrail.com/solution/tail-log-files/ (Accessed 01.03.2020).

7) 10 Startups Using Blockchain To Transform Messaging [Market Map] // disruptordaily.com URL: https://www.disruptordaily.com/blockchain-market-map-messaging/ (Accessed 01.03.2020).