

3. M.Çuriýew. Maglumatlary goramak. Ýokary okuw mekdepleri üçin okuw kitaby. –A.: Türkmen döwlet neşirýat gullugy, 2013, 206 s.

УДК 681.3:553.98(574.4)

Б.С. Гафуров¹, М.А. Гельдыева², Г.Д. Базарова², А.Р. Аннаева²

¹“Dragon Oil” (Turkmenistan) Ltd

²Международный университет нефти и газа имени Ягшыгельди Какаева
Ашхабад, Туркменистан

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В КИБЕРБЕЗОПАСНОСТИ

***Аннотация.** Блокчейн - это распределённая цифровая электронная книга. Впервые об этой технологии стало известно с появлением криптовалюты биткойн. Эта статья описывает применение технологии блокчейн как безопасной цифровой инфраструктуры, в частности в аутентификации пользователей и управлении личных данных.*

B.S. Gafurov¹, M.A. Geldiyeva², G.D. Bazarova², A.R. Annayeva²

¹“Dragon Oil” (Turkmenistan) Ltd

²Yagshigeldi Kakaev International University of Oil and Gas
Ashgabat, Turkmenistan

FEATURES OF USING BLOCKCHAIN TECHNOLOGY IN CYBERSECURITY

***Abstract.** Blockchain is a distributed digital ledger. This technology first made headlines with the emergence of the bitcoin cryptocurrency. This article describes the application of blockchain technology as a secure digital infrastructure, particularly in user authentication and personal data management.*

В современном цифровом веке информация свободно и быстро распространяется по просторам глобальной сети Интернет. При этом, такие технологии как блокчейн имеют особую важность в такой быстроразвивающейся среде. При этом, технология блокчейн находит множество применений в сфере кибербезопасности. Эти два понятия, кибербезопасность и блокчейн, подобны стражам цифровой сферы, неустанно работающим над обеспечением безопасности и целостности наших данных и транзакций.

Технология блокчейн является основой многих цифровых инноваций, и ее значение в обеспечении безопасности данных имеет первостепенное значение. Блокчейн - это децентрализованная,

распределённая технология реестра, которая регистрирует и сохраняет транзакции на нескольких компьютерах. Этот реестр воспроизводится на тысячах компьютеров - "узлах" – размещённых в разных точках мира и находится в открытом доступе. Но при всей своей открытости он также надежен и безопасен [1]. Каждая запись или блок связаны с предыдущей, образуя цепочку, что и привело к названию "блокчейн". Эта распределённость, в связи с отсутствием центральной точки отказа, делает её очень безопасной.

Кибербезопасность - это совокупность различных мер безопасности, включая инструменты, политики, руководства, действия, обучение, лучшие практики и технологии, используемые организациями или отдельными лицами для защиты активов и сетевой среды [2]. С годами появление новых киберугроз и увеличение масштабов и частоты кибератак усилили важность надежных инициатив по кибербезопасности с использованием современных технологий блокчейн.

В традиционных централизованно управляемых и проверяемых системах наличие единой точки отказа может сделать систему мишенью для кибератак, таких как вредоносные ПО, атаки типа "отказ в обслуживании" (Denial of Service - DoS) и распределённые атаки типа "отказ в обслуживании" (DDoS) [3]. В отличие от этого, технология блокчейн обеспечивает высокую безопасность децентрализованной системы, где транзакции не контролируются никакими сторонними организациями. В частности, блокчейн представляет собой цепочку блоков с временной меткой, коллективно поддерживаемую каждым участвующим узлом [4].

Теперь перейдём на непосредственное рассмотрение применения технологии блокчейн в области аутентификации пользователей и управления личными данными.

Технология блокчейн делает информацию о личности проверяемой и проверяемой за считанные секунды. Благодаря решениям для идентификации и аутентификации на основе блокчейна пользователям не нужно беспокоиться о том, что в процесс проверки будут вовлечены третьи лица или что конфиденциальная информация будет передана кому-то ещё кроме проверяющего. Это обеспечивает более надёжную защиту от мошенничества и кражи личных данных, поскольку все данные пользователей криптографически защищены и хранятся только в приложениях для идентификационных кошельков.

Управление идентификацией

Управление идентификацией, или управление идентификацией и доступом (УИД), применяется в любой ситуации, когда кто-то

использует процесс входа в систему для использования приложения или веб-сайта и имеет определенные уровни доступа к информации, технологиям или услугам [5]. УИД используется в самых разных случаях, будь то вход на веб-сайты для личного пользования или использование технологий сотрудником для выполнения своей работы в организации.

Поскольку в результате использования старых, менее безопасных систем управления идентификацией по всему миру возникло множество проблем, включая утечку данных, масштабные взломы и передачу конфиденциальной информации людей без их ведома, все больше нормативных требований предъявляется к сбору, хранению, использованию и передаче персональных данных.

К счастью, технология управления идентификацией на основе блокчейна может эффективно решить эти проблемы, повысив безопасность, эффективность, точность и доступность данных. Решения для идентификации на основе блокчейна становятся все более популярными, поскольку они предлагают безопасный и экономически эффективный способ управления цифровыми идентификационными данными [5]. Пользователи хранят свои идентификационные данные и учетные данные в децентрализованном приложении идентификационного кошелька, а блокчейн позволяет мгновенно проверять эти данные без необходимости обращаться к эмитенту. Идентификационные кошельки предоставляют пользователям больше контроля над их личной информацией.

Централизованное управление идентификацией - это когда единый орган собирает и хранит данные пользователей. Федеративное управление идентификацией позволяет авторизованным пользователям получать доступ к нескольким приложениям и доменам с помощью единого набора учетных данных, например, когда люди используют свои учетные записи Google или Facebook для входа в приложения и на веб-сайты. Федеративная система идентификации также называется единой системой входа (SSO).

Одним из главных недостатков централизованных и федеративных систем идентификации является то, что личные данные людей становятся более уязвимыми для утечки, стоит так же учитывать возможность кражи личных данных. Поскольку так много пользовательских данных хранится в одном месте, хакеры потенциально могут получить доступ к большому объёму данных. В последние годы утечка личных данных пользователей была самым распространенным типом утечки, составляя 97 % из всех случаев. Централизованные системы также создают единую точку отказа. Хотя

федеративные системы упрощают вход в систему, риск заключается в том, что если пароль будет украден, то все остальные ресурсы и сайты, которые вы используете с единой учетной записью, могут быть раскрыты.

Применение блокчейн в цифровой идентификации пользователей

Давайте перечислим несколько примеров применения блокчейн в цифровой идентификации пользователей:

- ✓ Безопасная проверка личности: Системы цифровой идентификации, использующие блокчейн, могут мгновенно и безопасно проверять личность и учётные данные людей для различных целей, таких как открытие банковских счетов или доступ к государственным услугам. Проверка личности на основе блокчейна обеспечивает повышенную безопасность, так как устраняет необходимость в централизованных услугах по проверке личности третьими лицами и предотвращает мошенничество и кражу личности.
- ✓ Медицинские записи: Пациенты могут создавать и управлять своей собственной цифровой идентификацией, а медицинские работники - безопасно проверять записи и истории болезни пациентов. Это может привести к повышению качества обслуживания, обеспечивая при этом конфиденциальность и безопасность данных.
- ✓ Управление цепочками поставок: Цифровые идентификаторы на основе блокчейна могут использоваться для отслеживания и управления информацией о цепочке поставок, обеспечивая большую прозрачность и безопасность. Создавая цифровые идентификаторы для товаров, менеджеры цепочек поставок могут отслеживать перемещение товаров по цепочке поставок, обеспечивая подлинность продукции и предотвращая подделки и мошенничество.

Управление идентификацией и доступом - это система процессов, политик и технологий, обеспечивающих доступ к технологическим ресурсам, информации и услугам только авторизованным лицам.

К проблемам традиционных систем управления идентификацией относятся:

- ❖ Риск утечки данных;
- ❖ Неприятные впечатления пользователей, которым приходится управлять большим количеством учётных записей для входа в систему;

- ❖ Дорогостоящие процессы проверки;
- ❖ Кража личных данных;
- ❖ Отсутствие права собственности на данные и контроля над ними;
- ❖ Недоступность идентификационных данных.
- ❖ Технология управления идентификацией на основе блокчейн может эффективно решить эти проблемы и имеет следующие преимущества:
- ❖ Обеспечение большей безопасности данных;
- ❖ Возможность более быстрой проверки;
- ❖ Сокращение расходов;
- ❖ Предотвращение мошенничества с идентификацией;
- ❖ Создание проверяемого следа записей;
- ❖ Содействие соблюдению правовых норм в отношении данных;
- ❖ Создание автоматизированных процессов;
- ❖ Повышение доступности идентификационных данных.

Список использованных источников

1. "Blockchains: The great chain of being sure about things". Журнал «The Economist.» Выпуск от 31 октября 2015 г.
2. Международный союз электросвязи (ITU). Кибербезопасность; 2010. <https://www.itu.int/net/itunews/issues/2010/09/20.aspx>
3. "A framework of blockchain-based secure and privacy preserving E-government system. Wireless Networks". Elisa N, Yang L, Chao F, and Cao Y., 2018 г.
4. "Blockstack: design and implementation of a global naming system with blockchains." Ali M, Nelson J, Shea R, and Freedman MJ. USENIX Annual Technical Conference. Denver, USA; 2016.
5. "Towards Blockchain-based Identity and Access Management for Internet of Things in Enterprises." Martin Nuss, Alexander Puchta, and Michael Kunz, 2021.