УДК 531.7.08

АНАЛИЗ ТЕХНОЛОГИИ ПРИМЕНЕНИЯ БЛОКЧЕЙН СОВМЕСТНО С ТЕХНОЛОГИЕЙ ИНТЕРНЕТ ВЕЩЕЙ ДЛЯ ОБРАБОТКИ И ХРАНЕНИЯ РЕЗУЛЬТАТОВ ИЗМЕРЕНИЙ

Дудник А.С.
Киевский национальный университет имени Тараса Шевченко
Чолышкина О.Г., Луцкий М.Г.
Межрегиональная академия управления персоналом

Миру известно множество цифровых валют, которых объединяет технология блокчейн. С каждым днем эта технология получает все большее признание, значительно расширяя границы и открывая все новые области применения. Сейчас блокчейн используется не только при осуществлении транзакций между пользователями, но и в самых различных сферах человеческой деятельности, включая финансовый рынок, игровую индустрию, госуправление и т. д. Различные решения на базе блокчейна часто реализуются в сочетании с Интернетом вещей (IoT), технологией Big Data (большие данные), искусственным интеллектом (Artificial intelligence, AI) и другими современными технологиями.
Ключевые слова: блокчейн, Интернет вещей, Big Data, искусственный интеллект, безопасность, измерения.

Постановка проблемы. Блокчейн (от англ. block и chain, «цепочка блоков») – распределенная база данных, потенциально доступная каждому (рис. 1). В блокчейне нет централизованного элемента, который мог бы управлять им и каким-либо образом вмешиваться в его работу.

Анализ последних исследований и публикаций. В Интернете вещей применяется технология RFID. Технология RFID-систем включается в себя систему EPC кодирования (в RFID-метку EPC записывается при помощи нулей и единиц; перевод EPC в нули и единицы называется бинарным кодированием EPC) [9, с. 4], систему радиочастотной идентификации и систему информационной сети.

Ключевые технологии Интернет вещей: радиочастотная идентификация, сенсорные технологии, нанотехнологии. Среди них RFID-системы являются основным компонентом данной технологии. RFID-системы используют пассивный механизм сбора данных.

Сегодня технология RFID-систем широко распространена в США, Европе и Японии. Технология Интернета вещей в тестовом режиме нашла практическое применение в военной отрасли. Управление на морских судах было отдано в руководство технологии Интернета вещей. Особая популярность технологии получала в розничной торговле (безопасность и логистика) [2, с. 53].

Определение не решённых раньше задач общей проблемы. Если классическая база данных расположена на централизованных серверах, принадлежащий какой-либо организации или физическому лицу, то блокчейн распределен среди множества участников сети и не может контролироваться никем из них по отдельности.

Цель статьи. Целью работы является создание концепции обледенения технологий блокчейн и Интернета вещей, для улучшения работы сети «Умный дом», благодаря обьеденению приимуществ обеих технологий.

Изложение основного материала. Распределенная архитектура блокчейна обеспечивает высокую степень безопасности, и даже если часть компьютеров сети будет взломана, то это не повредит работе всей системы в целом. В блокчейне можно хранить различные данные, которые верифицируются специальным оборудованием – майнерами.

На основании вышесказанного выделяют 3 основных архитектуры блокчейн (рис. 2):

· **Публичная БЦ (Distributed).** Она является полностью открытой для участников и каждый из них может как осуществлять операции в ней, так и участвовать в их администрировании.

· **БЦ, принадлежащая консорциуму (Decentralized).** В таких блочных цепях процедура согласования возлагается на заранее отобранные узлы.

· **Частная БЦ (Centralized).** Администрирование и согласование процедур в такой сети осуществляется единым органом.

Механизм взаимодействия с приложениями на базе блокчейна напоминает работу с сервисом Google Docs, когда несколько человек обладают одновременным доступом к документу и могут

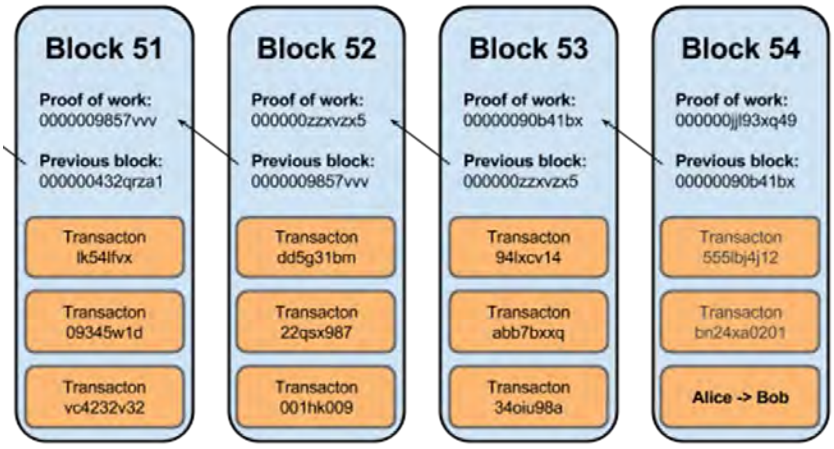

Рис. 1. Принцип работы блокчейн

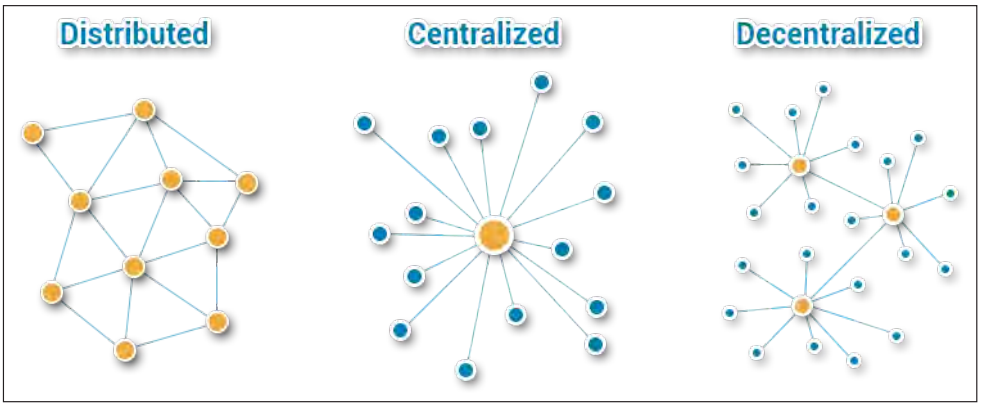

Рис. 2. Архитектуры блокчейн

наблюдать за его изменениями в режиме реального времени.

Таким образом, блокчейн – это общая, постоянно сверяемая, распределенная база данных.

Если разделить историю интернета на этапы, то окажется, что сейчас мы находимся в эпоху развития Интернета вещей (Internet of things, IoT).

Данная концепция зародилась относительно недавно – в 1999 году, но с тех пор изменилось многое. За относительно небольшой промежуток времени развитие IoT проделало путь от концепции, до практического применения в самых различных сферах жизнедеятельности человека (рис. 3).

Простыми словами, IoT – это группа устройств, взаимодействующих не только с пользователями, но и друг с другом.

В качестве примера применения Интернета вещей можно взять системы поддержки принятия решений на фермах, которые собирают данные о почвенных условиях из экологических датчиков, а затем сопоставляют их с историческими данными, прогнозами цен и погодными условиями.

Такие системы способны вырабатывать ценные рекомендации фермерам о том, когда сажать растения, удобрять конкретные земельные участки, начинать собирать урожай и т. д.

Подобных примеров практического применения Интернета вещей можно привести множество.

Чаще всего, использование технологий IoT выражается в новых продуктах и сервисах, способствующих защите окружающей среды, экономии энергии, повышению производительности в промышленности, логистике, сельском хозяйстве, улучшению медицинского обслуживания и т. д.

Первое, с чем ассоциируется применение блокчейна в сфере Интернета вещей – это безопасность и целостность данных. На пример Mirai – ботнет, образованный взломанными «умными» устройствами. Наиболее известный случай (21 октября 2016 года) – массивная DDOS атака на DNS-оператора Dyn (рис. 4). В результате огромное ко-

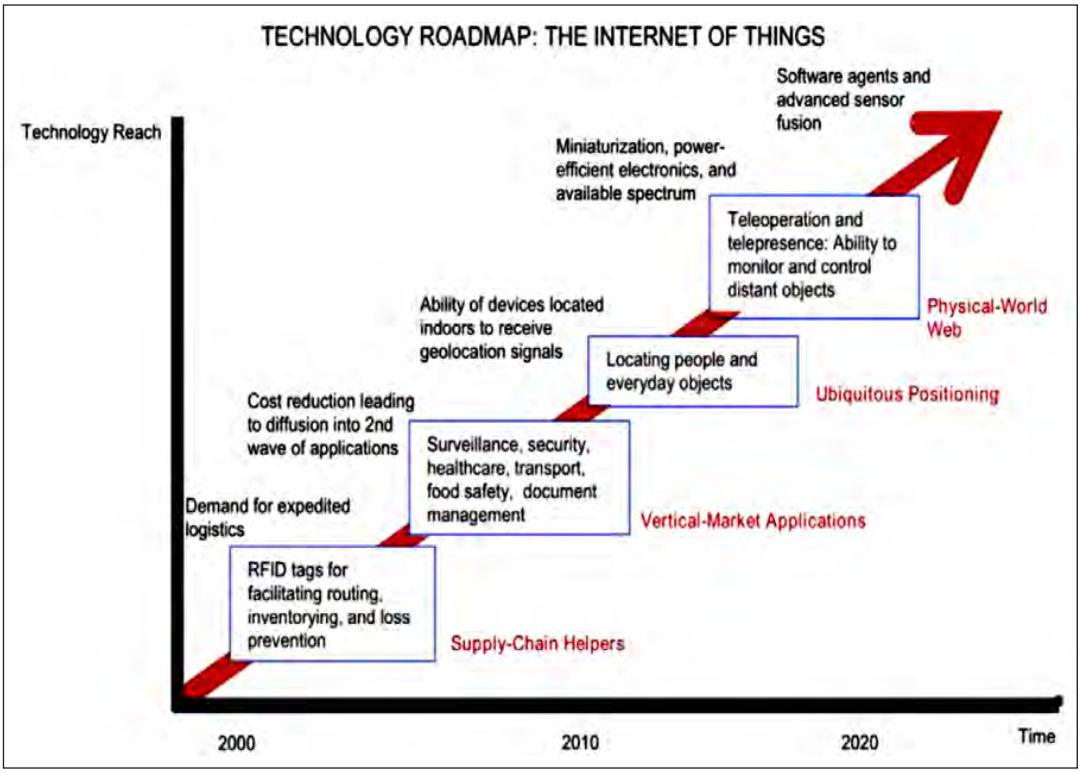

Рис. 3. История и перспективы интернета вещей

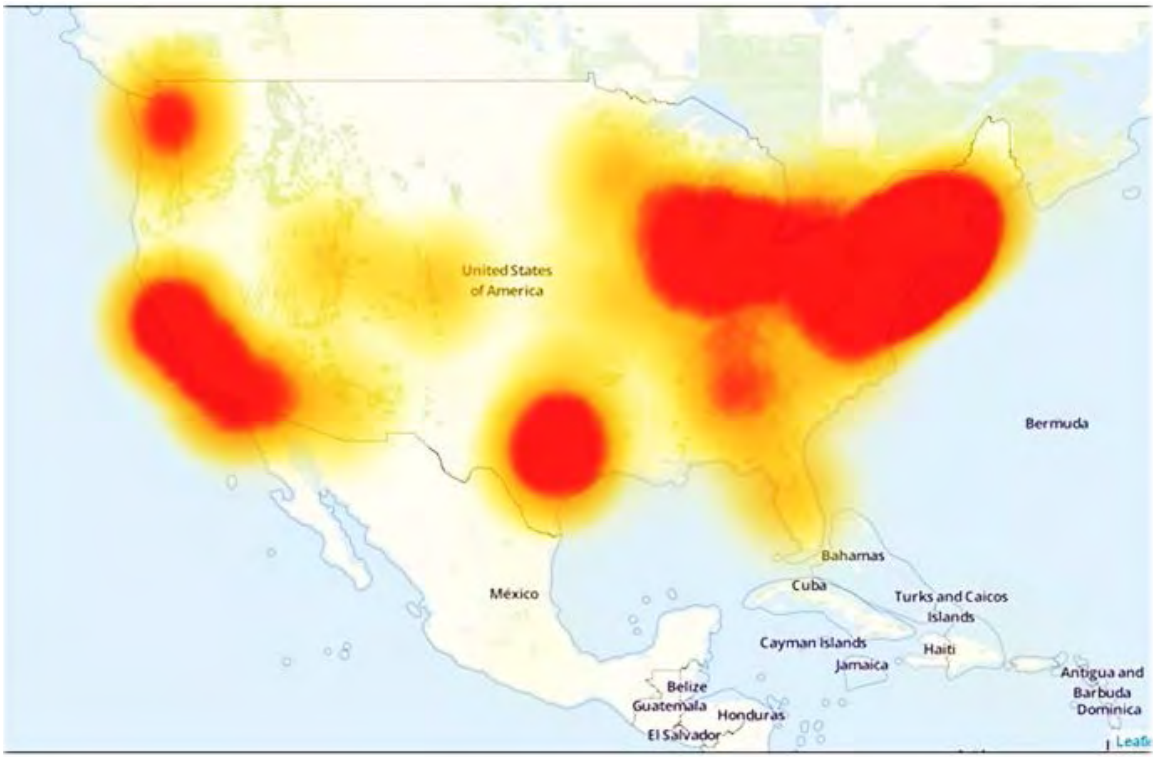

Рис. 4. Очаги DDOS атаки Mirai

личество пользователей на время лишились доступа в сеть. Некоторые исследователи утверждают, что мощность атаки могла достигать 1,2 Тб/с [1].

На самом деле, возможности применения технологии распределенного реестра в IoT гораздо шире и глубже, а потому сочетание этих двух технологий потенциально может иметь большой синергетический эффект [2, с. 40].

Так, по мнению Джона Уилмса из американской некоммерческой ассоциации компаний электросвязи TM Forum, есть ряд сфер применения, где блокчейн может поддерживать рост и развитие IoT. Среди них: противодействие мошенничеству, управление идентификацией, проведение транзакций, верификация состояния элементов различных систем, обеспечение целостности данных и т. д.

Решения на базе блокчейна и IoT в некоторых сферах подразумевают быстрое налаживание взаимодействия между несколькими экономическими агентами. Эти связи подразумевают возникновение юридических и финансовых последствий, и, что довольно часто, – необходимость формализации отношений посредством заключения договора между заказчиком услуги и ее поставщиком (Service Level Agreement, SLA). В этом документе, который можно поместить в блокчейн, указываются описание услуги, права и обязанности сторон, требования к качеству и другие существенные сведения. Использование смарт-контрактов может позволить системе получать объективные сведения о соблюдении экономическими агентами условий SLA с последующим установлением соответствующих поощрений или штрафных санкций для участников деловых отношений.

По мнению Джона Уилмса, блокчейн может оптимизировать многие процессы и создать новую систему отношений, построенную на доверии, в которой исключено любого рода мошенничество. Уилмс также считает, что стремительное развитие Интернета вещей создает управленческие проблемы, которые не существовали ранее.

Ярким примером сочетания этих технологий является Умный дом: умный дом состоит из следующих трех частей:

· Устройства: все интеллектуальные устройства, расположенные в доме.

· Local BC (BlockChain): безопасный и закрытый BC, который накапливает и хранит показатели измерений в одном (или более) устройстве, поддерживающие ресурсы, которые всегда находятся в сети. Примером может быть смарт-хаб или домашний компьютер. В отличие от Биткойн БК, управление которой децентрализовано, местный BC централизованно управляется его владельцем. Все транзакции, относящиеся к конкретному устройство соединены вместе. Владелец несет ответственность за добавление новых устройств создавая начальную транзакцию, которая похожа на создание новой монеты в биткойне. владелец также может удалить существующее устройство, удалив его книгу. Местный БК имеет заголовок политики, который является списком контроля доступа, который позволяет владельцу контролировать все транзакций, происходящих в ее доме. Устройства могут связываться друг с другом, только если владелец позволяет им сделать это, предоставив им общий ключ на основе обобщенного Диффи-Хеллмана [4]. Хотя все блоки в BC имеют заголовок политики, наиболее обновленный, помещенный в заголовок последнего блока, используется для проверки и изменения политики. Как и в биткойне, транзакции группируются вместе и добываются в единицах блоки. Однако, в отличие от Bitcoin, каждый блок добывается и добавляется к BC без POW или других головоломок, чтобы уменьшить

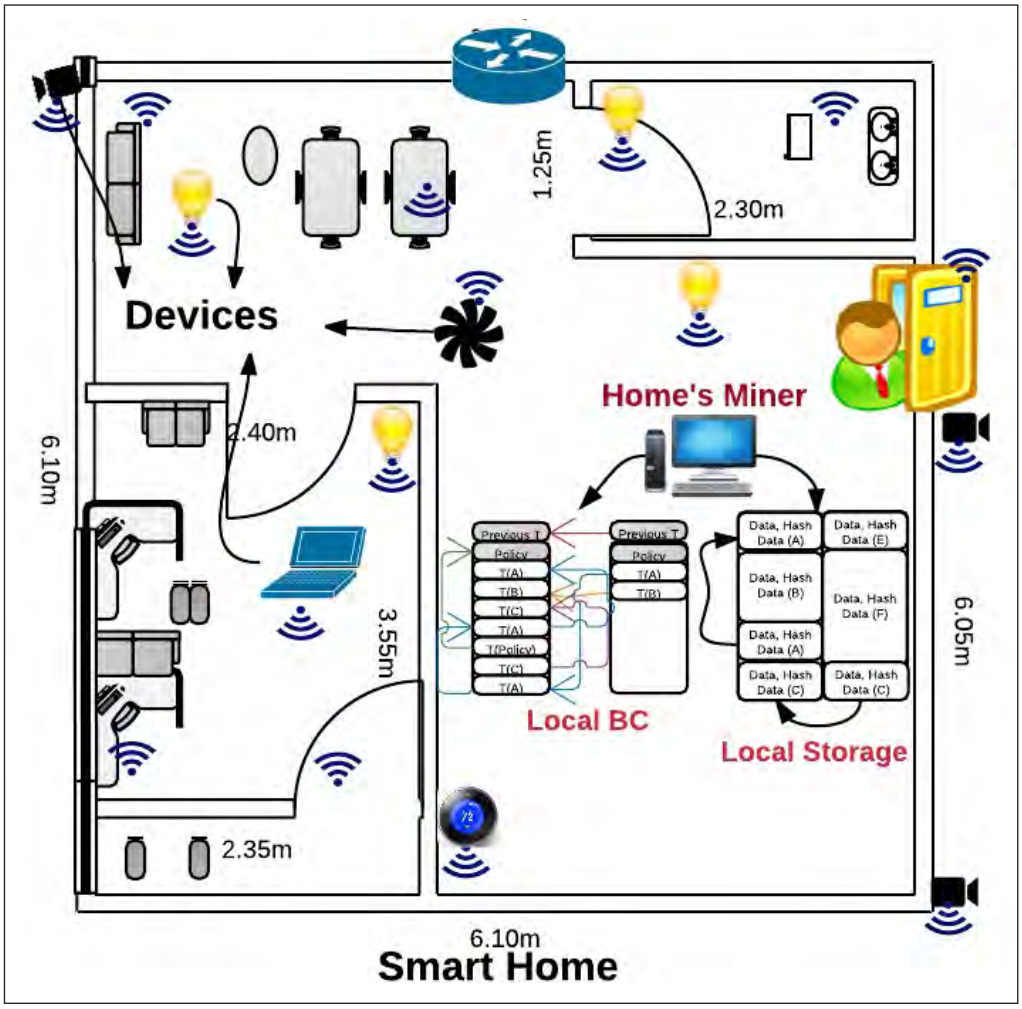

Рис. 5. Концепция технологии умный дом

связанные с этим накладные расходы. Шахтер добавляет указатель на предыдущий блок, копирует политику в предыдущем блочном заголовке в новый блоки соединяет блок с BC. Еще одна разница с Биткойном заключается в том, что когда транзакция была добавлена в блок, она рассматривается как истинная транзакция, независимо от того, блок заминирован или нет.

· Локальное хранилище. В каждом доме может быть дополнительное локальное хранилище для хранения данных локально, как показано в умном доме на рис. 1. Это может быть локальный резервный диск.

В дополнение к этим частям, у каждого домашнего шахтера есть список ПК, используемых для предоставления другим разрешение доступа к данным смарт-дома.

Выводы и предложения. Проанализированы основные проблемы технологий блокчейн и Интернет вещей.

Предложена концепция объединения технологий блокчейн и Интернет вещей для создания сети «Умный дом».

Предложена архитектура основные компоненты которой включают:

1. Умный дом (или в общем случае – локальная сеть);
2. Оверлейную сеть;
3. Облачное хранилище.

Выделены основные составляющие архитектуры локальной сети умного дома:

· Различные устройства;
· Локальный Блокчейн;
· Локальное хранилище.

Список литературы:

1. A. Ukil, S. Bandyopadhyay and A. Pal. "IoT-Privacy: To be private or not to be private" in Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on. Toronto, 2014.
2. Das, Manik Lal, "Privacy and Security Challenges in Internet of Things" Distributed Computing and Internet Technology, p. 33–48, 2015.
3. Yves-Alexandre de Montjoye et al. "Openpds: Protecting the privacy of metadata through safeanswers" PloS one 9.7 (2014).
4. Decker Christian, Jochen Seidel and Roger Wattenhofer. "Bitcoin Meets Strong Consistency".
5. H. Gross, M. Holbl, D. Slamanig and R. Spreitzer. "Privacy-Aware Authentication in the Internet of Things", Cryptology and Network Security. Springer International Publishing, p. 32–39, 2015.

6. Ho G., Leung D., Mishra P., Hosseini A., Song D. and Wagner D. "Smart locks: Lessons for securing commodity internet of things devices" in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security.
7. J. Buchmann. "Introduction to cryptography", Springer Science & Business Media, 2013.
8. Jøsang Audun and Jochen Haller. "Dirichlet reputation systems" in Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on., 2007.
9. Karl Aberer. Smart Earth: From Pervasive Observation to Trusted Information. MDM 2007: 3–7.
10. M. Amoozadeh et al. "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving" IEEE Communications Magazine, vol. 53, no. 6, p. 126–132, 2015.
11. Ninhui Sun, Zhiwei Xu, Guojie LI. Sea Computing: The new computing model of IOT. Communication of China Computer Federation. 2010, 6(7): 52–57.
12. S. Nakamoto. "Bitcoin: A peer-to-peer electronic cash system", 2008.
13. Skarmeta, Antonio F., Jose L. Hernandez-Ramos and M. Moreno. "A decentralized approach for security and privacy challenges in the internet of things" in nternet of Things (WF-IoT), 2014 IEEE World Forum on, 2014.
14. T. Project. [Online]. Available: https://www.torproject.org/.

Дуднік А.С.
Київський національний університет імені Тараса Шевченка
Чолишкіна О.Г., Луцький М.Г.
Міжрегіональна академія управління персоналом

АНАЛІЗ ТЕХНОЛОГІЇ ЗАСТОСУВАННЯ БЛОКЧЕЙН СПІЛЬНО З ТЕХНОЛОГІЄЮ ІНТЕРНЕТ РЕЧЕЙ ДЛЯ ОБРОБКИ ТА ЗБЕРІГАННЯ РЕЗУЛЬТАТІВ ВИМІРЮВАНЬ

Анотація
Світові відомо безліч цифрових валют, яких об'єднує технологія блокчейн. З кожним днем ця технологія набуває все більшого визнання, значно розширюючи межі і відкриваючи все нові сфери застосування. Зараз блокчейн використовується не тільки при здійсненні транзакцій між користувачами, але і в самих різних сферах людської діяльності, включаючи фінансовий ринок, ігрову індустрію, держуправління і т. Д. Різні рішення на базі блокчейна часто реалізуються в поєднанні з Інтернетом речей (IoT), технологією Big Data (великі дані), штучним інтелектом (Artificial intelligence, AI) і іншими сучасними технологіями.
Ключові слова: блокчейн, Інтернет речей, Big Data, штучний інтелект, безпеку, вимірювання.

Dudnik A.S.
Taras Shevchenko National University of Kyiv
Cholishkina O.G., Lutsky M.G.
Interregional Academy of Personnel Management

ANALYSIS OF THE TECHNOLOGY OF BLOCKING APPLICATION BETWEEN NETWORK INTERNET TECHNOLOGY FOR PROCESSING AND STORAGE OF RESULTS OF MEASUREMENTS

Summary
The world knows a lot of digital currencies, which is combined with the blockade technology. Every day, this technology gets more and more recognition, greatly expanding the boundaries and opening up new areas of application. Now BlockChein is used not only for transactions between users, but also in various fields of human activity, including financial market, gaming industry, state administration, etc. Different solutions based on blockade are often implemented in conjunction with the Internet of Things (IoT), technology Big Data (large data), artificial intelligence (Artificial intelligence, AI) and other advanced technologies.
Keywords: blockade, Internet of Things, Big Data, Artificial Intelligence, Safety, Measurement.