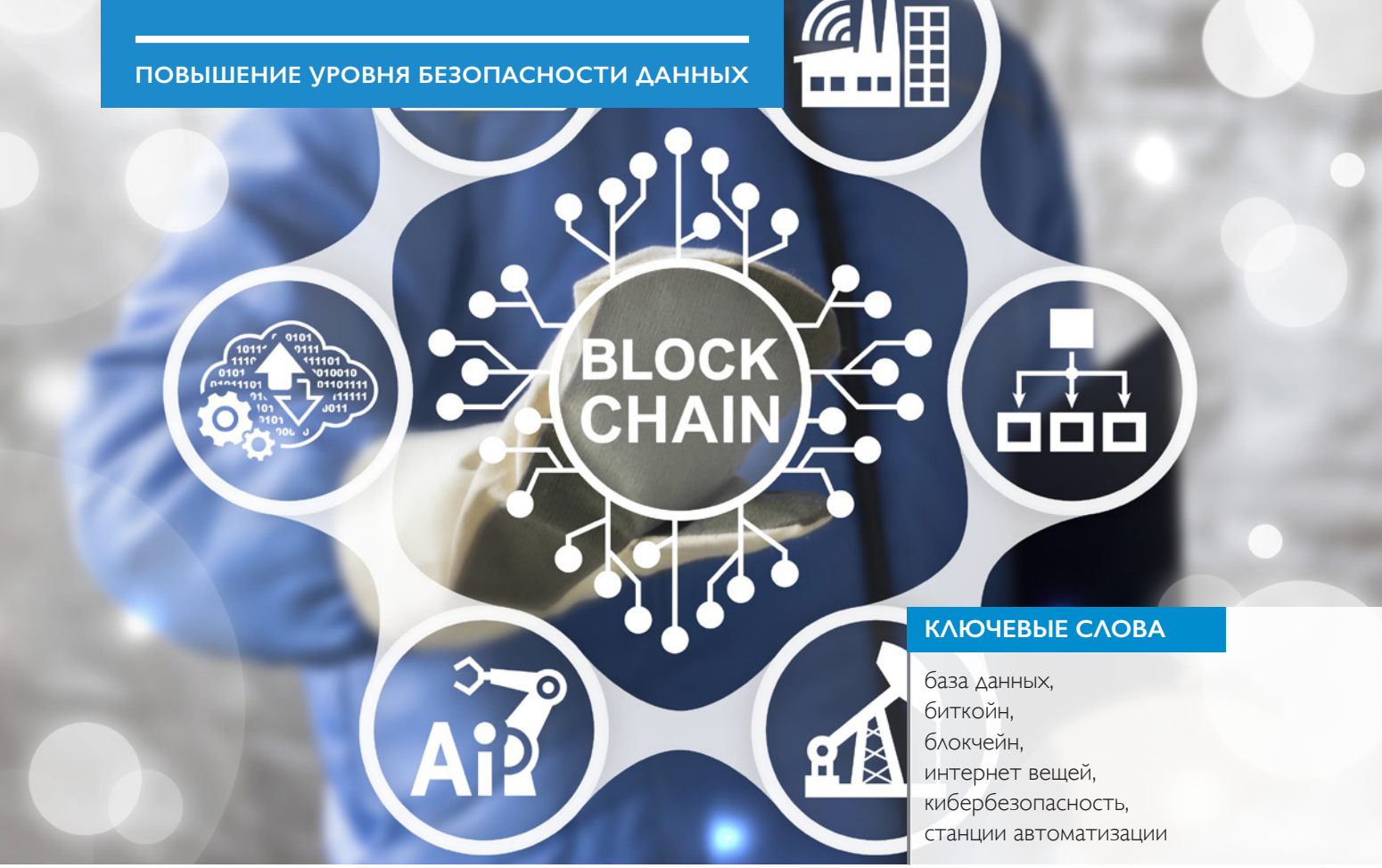



**КЛЮЧЕВЫЕ СЛОВА**

база данных,
биткойн,
блокчейн,
интернет вещей,
кибербезопасность,
станции автоматизации

# ТЕХНОЛОГИЯ БЛОКЧЕЙН ДЛЯ АВТОМАТИЗАЦИИ ЗДАНИЙ

**Феликс Гассман,** доктор, руководитель отдела технологий, Fr. Sauter AG

**С появлением биткойна, цифровой интернет-валюты, технология блокчейн неожиданно превратилась в нечто большее, чем просто реклама. Интернет-гиганты планируют ввести свои собственные цифровые криптовалюты, угрожая традиционному миру ключевых валют и банков. Но наряду с этими мегатрендами имеет место и другой подход, «мирное» использование технологии блокчейна – для защиты данных и процессов, используемых при автоматизации зданий.**

Блокчейн – это децентрализованная база данных, которая поддерживает постоянно растущий список записей. В операциях с биткойном эта база данных расширяется с каждой транзакцией, тем самым выстраивая цепочку, в которую постоянно добавляются новые элементы или блоки (отсюда и термин «блокчейн»). Когда блок завершен, создается новый, содержащий цифровой отпечаток предыдущего блока. Если кто-то удаляет только один элемент в этой цепочке блоков данных, отпечаток затрагиваемого блока изменяется и, таким образом, вся цепочка блоков распадается на отдельные звенья.

***#терминология***

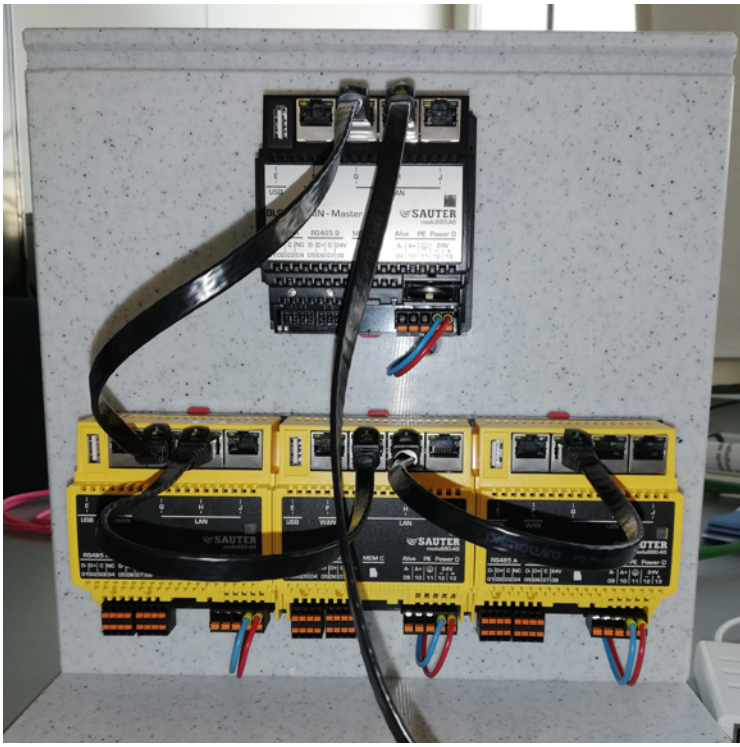
***Биткойн*** *(англ. bitcoin, образовано соединением слов bit – бит (единица измерения информации) и coin – монета) – новая цифровая валюта, созданная и работающая только во Всемирной паутине.*

***Всемирная паутиина*** *(англ. World Wide Web) – распределенная система, предоставляющая доступ к связанным между собой документам, расположенным на различных компьютерах, подключенных к сети Интернет.*

Особенностью биткойна является то, что каждая транзакция вновь проверяется, прежде чем записывается в блокчейн. Каждый компьютер в сети может видеть, что абонент А хочет перевести биткойны абоненту В. Затем компьютеры в сети проверяют, соответствует ли транзакция правилам и достаточно ли у А биткойнов. Только при условии согласия всех участвующих компьютеров с тем, что транзакция действительна, она затем вводится в блокчейн с цепью, постоянно защищающей ее от подделки.

Процесс проверки чрезвычайно загружает процессор. IPO[1] ряда крупных биткойн-компаний позволил определить их энергопотребление и экстраполировать его на всю сеть биткойнов. Был сделан вывод, что для работы сети сейчас требуется около 46 ТВт•ч (46 × 109 кВт•ч) электроэнергии в год. Эта потребность в энергии приводит к выбросу около 22 Мт диоксида углерода в год, что примерно соответствует выбросу $CO_2$ в Гамбурге или всей Шри-Ланке.

Уникально внедряет технологию блокчейн компания Sauter (далее – Компания) – она связывает свои станции автоматизации в сети зданий и создает кольцо блокчейна. При этом используемые вычислительные ресурсы и дополнительные коммуникационные данные более чем скромны. В результате получается повышение безопасности данных без чрезмерного энергопотребления.




## Кибербезопасность в эпоху Интернета вещей

Создание новой системы автоматизации зданий modulo 6 Sauter открыло двери в облачные технологии и технологии Интернета вещей (IoT). Однако поскольку здания подключены к Интернету вещей и облаку, безопасность системы и сети становится серьезной проблемой. Чтобы преодолеть эту проблему, в Компании была разработана концепция кибербезопасности для modulo 6 на базе нового международного стандарта промышленной автоматизации IEC 62443. Стандарт IEC определяет семь фундаментальных требований и четыре уровня безопасности для кибербезопасности (см. табл. 1 и 2).

Уровни безопасности, достигнутые по modulo 6 для сетей и компонентов системы, описаны в руководстве по modulo 6 для кибербезопасности. Эта спецификация позволяет определить текущий уровень безопасности для установок, которые могут требовать специальной защиты, и при необходимости усилить эти целевые меры.

## Блокчейн-кольцо, образованное станциями автоматизации

Modulo 6 имеет высокий уровень защиты, встроенный изначально. Станция автоматизации предлагает совершенно отдельный от сети здания сетевой интерфейс. Это создает межсетевой экран между Интернетом и локальной сетью здания. Шифрование, аутентификация и защита доступа гарантируются проверенными технологиями безопасности (TLS 1.3, IEC802.1X и т. д.), а сетевые интерфейсы уже

**Таблица 1 Семь фундаментальных требований согласно IEC 62443**

| |
|---|
| 1. Идентификация и аутентификац |
| 2. Контроль использования |
| 3. Системная целостность |
| 4. Конфиденциальность данных |
| 5. Ограниченный поток данных |
| 6. Оперативный ответ на события |
| 7. Наличие ресурсов |

**Таблица 2 Уровни безопасности согласно IEC 62443**

| | |
|---|---|
| Уровень безопасности 1: | Случайное неправильное использование |
| Уровень безопасности 2: | Умышленные попытки с основными ресурсами |
| Уровень безопасности 3: | Преднамеренные попытки, но с более продвинутыми знаниями и более обширными ресурсами (например, хакеры, специализирующиеся на автоматизации зданий с обширными финансовыми ресурсами, или контракт) |
| Уровень безопасности 4: | Целевые атаки, но с конкретными знаниями и значительными ресурсами (санкционированные правительством спецслужбы, например атака Моссада со Stuxnet на иранские урановые центрифуги) |

[1] IPO, от англ. Initial Public Offering, «первичное публичное предложение» – первая публичная продажа акций акционерного общества.

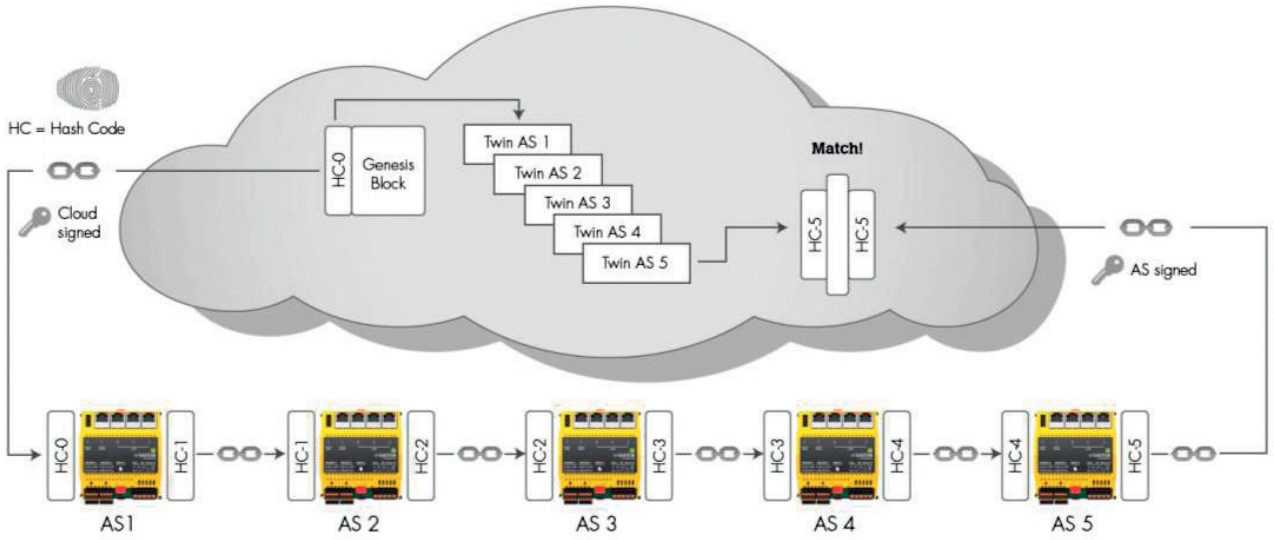



**Рис.** Sauter blockchain ring

хорошо защищены от DoS-атак на уровне автоматизации. Следовательно, процессы можно наблюдать, ограничивать, изолировать или даже при необходимости останавливать.

Modulo 6 также оснащен стандартом безопасности BACnet/SC (BACnet Secure Connect), запланированным на 2020 год. Это означает, что должным образом выполнены основные требования IEC 1, 2 и 4–7. Только для требования 3, то есть для обеспечения целостности системы, существующие меры представлялись все еще неудовлетворительными. Целостность системы также может быть описана как неповрежденность данных или защита от несанкционированного изменения данных. Примерами этого могут быть изменение проверенных данных измерений и обработки или помехи в программах автоматизации. Такие изменения данных могут быть вызваны даже собственным обслуживающим персоналом компании – по незнанию и совершенно случайно.

Представляя принципы функционирования технологий биткойна и блокчейна, мы изначально визуализируем безопасность транзакций данных или платежей. Однако ниже этого уровня динамических транзакций находится статическая распределенная база данных, защищенная цепочкой блоков, – своего рода «бухгалтерская книга, заложенная в основу всех существующих транзакций». В настоящее время Компания воплощает этот принцип в мир сетевой автоматизации зданий и разрабатывает собственный блокчейн-процесс.

Идея проста: статические данные станций автоматизации в сети образуют своего рода блокчейн-кольцо. Каждая станция автоматизации генерирует свой цифровой отпечаток. Он основан на ее собственных данных и «отпечатке пальца» предыдущей станции в кольце блокчейна. Данные блока обычно состоят из программ, встроенного программного обеспечения и параметров процесса и сети. Проще говоря, каждая станция использует свои собственные данные для формирования блока в блокчейне.

В случае нарушения целостности блокчейна ответы системы:

1. Только вызвать тревогу;
2. Активировать тревогу и изолировать затронутую станцию (и принять состояние аварийного сигнала, например);
3. Активировать тревогу, изолировать затронутую станцию и начать автоматическое самовосстановление.

Действие 3 требует создания цифрового «близнеца» для каждой станции во время ввода в эксплуатацию. Эти «близнецы» (копия всех статических данных) сохраняются в зашифрованной базе данных. Затем они могут храниться на выделенной станции автоматизации, локальном компьютере или в центре обработки данных / облаке.

## Преимущества решения

Усовершенствованная процедура для блокчейна позволяет случайным образом распределять «близнецов» между существующими станциями. Это полностью устраняет необходимость в дополнительном компьютере базы данных.

Процесс самовосстановления особенно полезен во время текущего обслуживания. При замене станции автоматизации данные, проверенные во время ввода в эксплуатацию, гарантированно будут переданы.

В настоящее время процедура была представлена в качестве патента и прошла международный патентный поиск. Таким образом, был достигнут уникальный уровень безопасности для важных требований целостности системы, предусмотренных IEC 62443.

***#терминология***

***Блокчейн*** *(blockchain, изначально block chain – дословно «цепочка блоков») – децентрализованная база данных, в которой все записи (блоки) связаны между собой с помощью средств криптографии.*

***Криптография*** *(от др.-греч.* Κρυπτός *«скрытый» +* γράφω *«пишу»)) — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации) и аутентификации (проверки подлинности авторства или иных свойств объекта).*