rus.blockchain_prerequisites

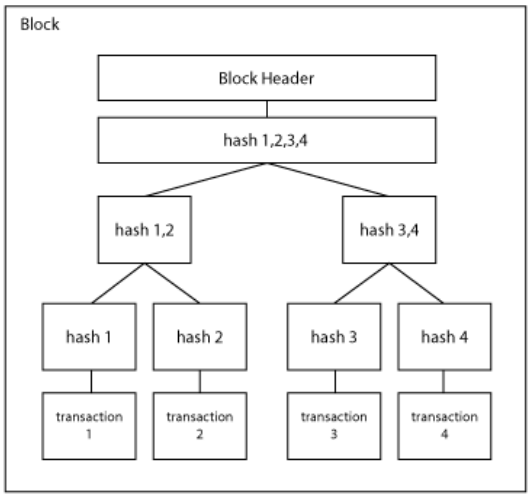
Alexandr Kirilov (https://github.com/alexandrkirilov)

Blockchain: Введение.

Для начала попробуем разобраться в том, что такое blockchain. Согласно открытым источникам, определение дано достаточно очевидное:

- en.wikipedia.org
- ru.wikipedia.org

Blockchain - технология хранения данных, при которой структура данных выстроена определенным способом, путем связывания элементов между собой при помощи специального алгоритма.



Многие связывают это только с финансами, потому что впервые широко этот термин был разрекламирован (стоит отметить, что был разрекламирован, но не использован впервые) при появлении в 2008 году Bitcoin, который для обеспечения безопасности транзакций начал это использовать. Впоследствии к данной технологии прибавили основы P2P сетей в простонародии - Torrent (скорей всего это была попытка сократить расходы на содержание серверов путем нахождения энтузиастов которые будут держать свои домашние компьютеры включенными для обеспечения доступности данных, точно так же как это в Torrent) и получилось нечто такое, представление о чем возникает в мозгу при упоминании blockchain.

Такое восприятие и понимание blockchain - неправильное. Это просто технология хранения данных обеспечивающая дополнительный (стоит сделать акцент на слове "дополнительный", подразумевается что не единственный) уровень целостности

данных, повышая тем самым уровень безопасности хранения данных. Именно по этой причине она получила высокий уровень распространения среди электронных систем платежей, где исторически сложившейся факт - высокий уровень возможности мошенничества.

Еще одно заблуждение, что это новая технология. Это не так! Наиболее яркий пример того, что это давно используется - это система контроля пробега у автомобилей. У многих автомобилей (Mercedes, Audi, Toyota и т.д), для избежания мошенничества с пробегом, особенно у топовых версий, используют распределенное хранение данных о пробеге на несколько частей (технически - это несколько датчиков расположенных внутри автомобиля) в которые определенным образом записывается информация о пробеге или её часть и компьютер, для примера, считывает значения с каждого, потом суммируя, выдает значение. Выглядит знакомо? Думаю да.

Так же это встречалось уже в разработке ПО при попытке защитить от несанкционированного копирования и использования приложений предоставляющих доступ к особо важной или ограниченной информации уже в начале 2000-х, а это больше 15 лет назад.

Теперь стоит обратить внимание на само слово blockchain (изначально это block chain, писалось раздельно):

- значение "block"
  - in Cambridge Dictionary
  - in Merriam Webster Dictionary
- значение "chain"
  - in Cambridge Dictionary
  - in Merriam Webster Dictionary

Перефразировав то, что написано словарях можно получить описание более расширенное в контексте применения в разработке баз данных и прикладного ПО:

Blockchain - это некая структура организованная таким образом, где элементы структуры связаны между собой таким образом, что изменение одного элемента невозможно без изменения связанных с ним. Иными словами нельзя изменить один элемент структуры не изменив связанные. Структура взаимосвязей элементов является block для работы с элементами chain, если можно так сказать.

Если посмотреть на пример с автомобильным пробегом, то для изменения значение нужно будет записать одновременно на все чипы часть значения и так чтоб это было корректно воспринято бортовым компьютером. Задача для мошенников усложнилась в

разы, а значит и увеличились затраты, и выгода получаемая от изменения пробега становится не так очевидна, либо проверка на наличие попытки "скрутить" становится более простой. Отсутсвие выгоды, либо легко определяемое мошенничество - основные типы защиты от любого вида мошенничества.