Криптовалюта : основные понятия, возможности использования, потенциальные риски и выгоды. Как отвечать на сложные вопросы детей по теме о криптовалютах.

Вагин Сергей Геннадьевич

д.э.н, профессор, DBA

Российская Ассоциация менеджмента знаний

Москва

11 марта, 2020

Вопросы.

Что такое цифровые деньги или виртуальные деньги ?

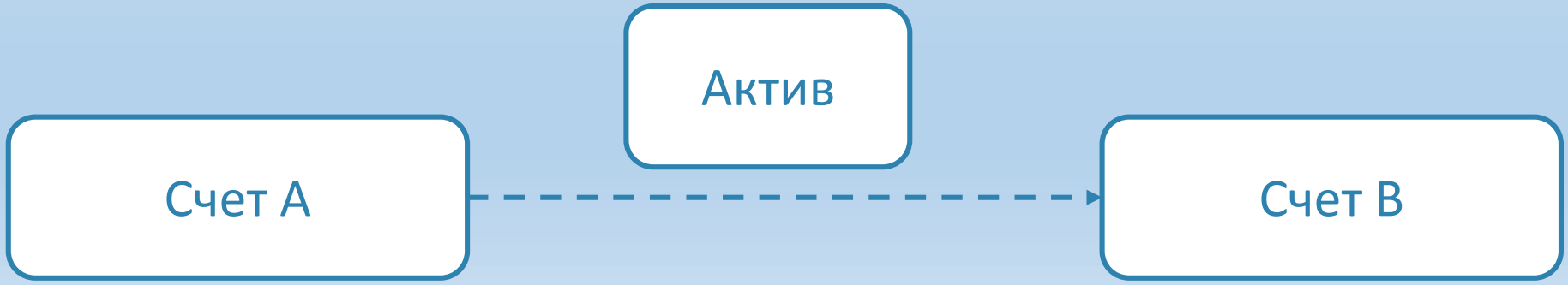

Цифровые валюты
Виртуальные валюты цифровое представление ценности, отличной от национальной валюты
Децентрализованные
Централизованные
Электронные деньги цифровое представление национальной валюты

Вопросы.

Что такое блокчейн, как он работает и зачем он нужен ?

Реестр (ledger)

- Реестр — форма систематизации, учёта; список, перечень, опись, система.
- Фактически представляет собой двойную бухгалтерскую запись



Различные типы реестров.

- Традиционные реестры
- Частные реестры
- Реестры с ограниченным доступом
- Публичные реестры
- Распределенные реестры

Распределенный реестр (Distributed Ledger).

Распределенный реестр — реестр данных, которые распределены и синхронизируются в сети.

Они распределяются по большому количеству узлов сети, а также географическим локациям.

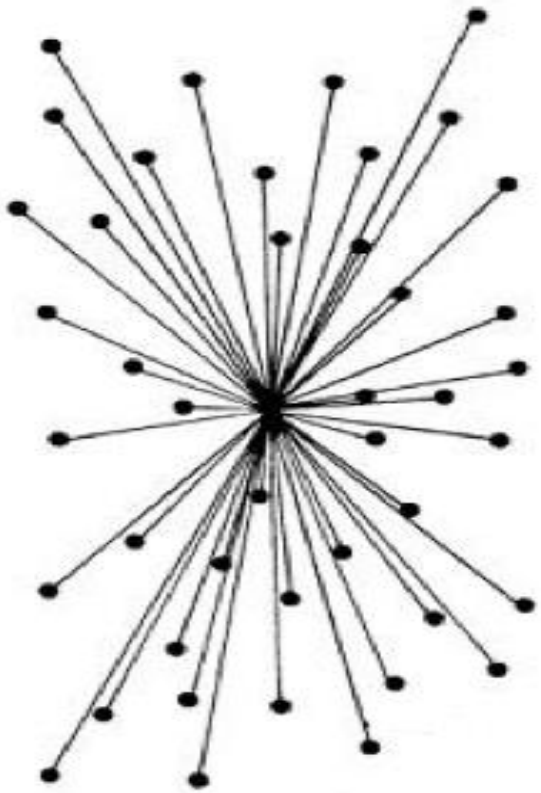
Распределенный реестр не имеет централизованных точек отказа.

Типы сетей.

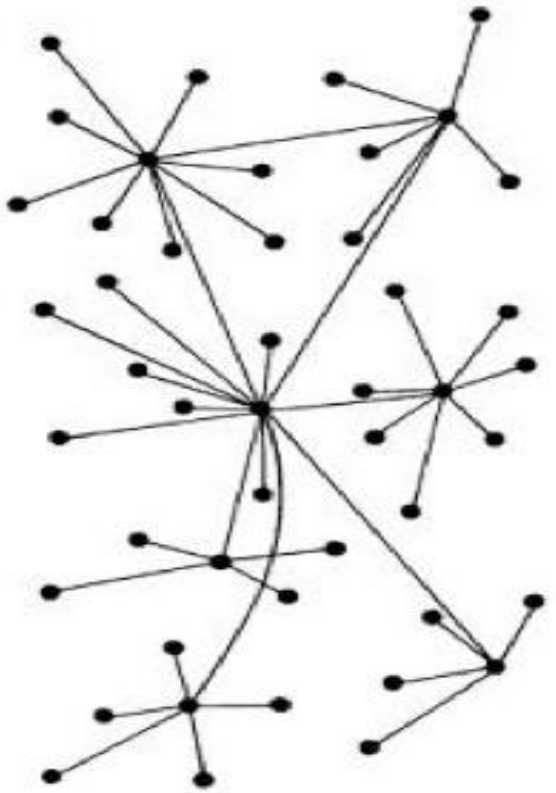
В общем случае, сети могут быть следующих топологий:

- Централизованные
- Децентрализованные
- Распределенные

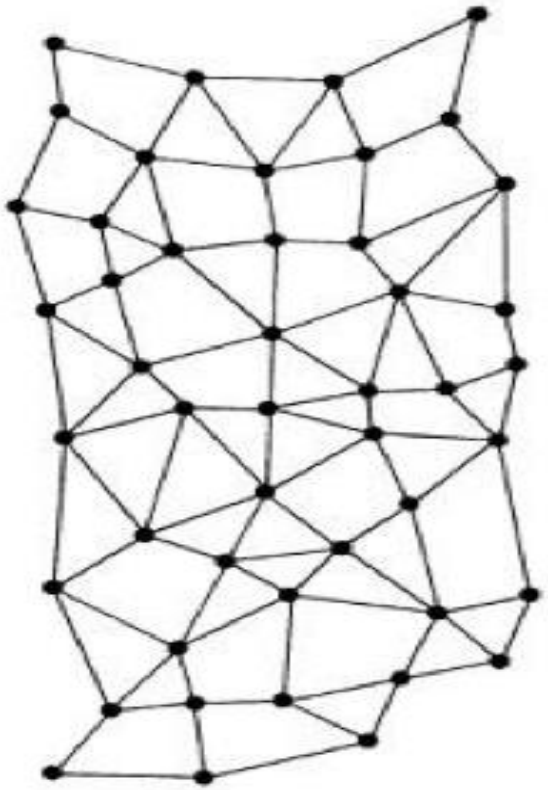
Типы сетей.



Централизованная модель



Децентрализованная модель



Распределенная модель

Blockchain: исторические предпосылки.

- 1991: описана криптографически защищенная цепочка блоков
- 1992: к работе 1991 года добавлено использование Деревьев Меркла
- 1999: Napster
- 2002: предложение об использовании доверенной сетевой файловой системы
- 2005: Ником Забо предложена блокчейн-подобная система
- 2008: Сатоши Накамото — представлена первая концепция блокчейна

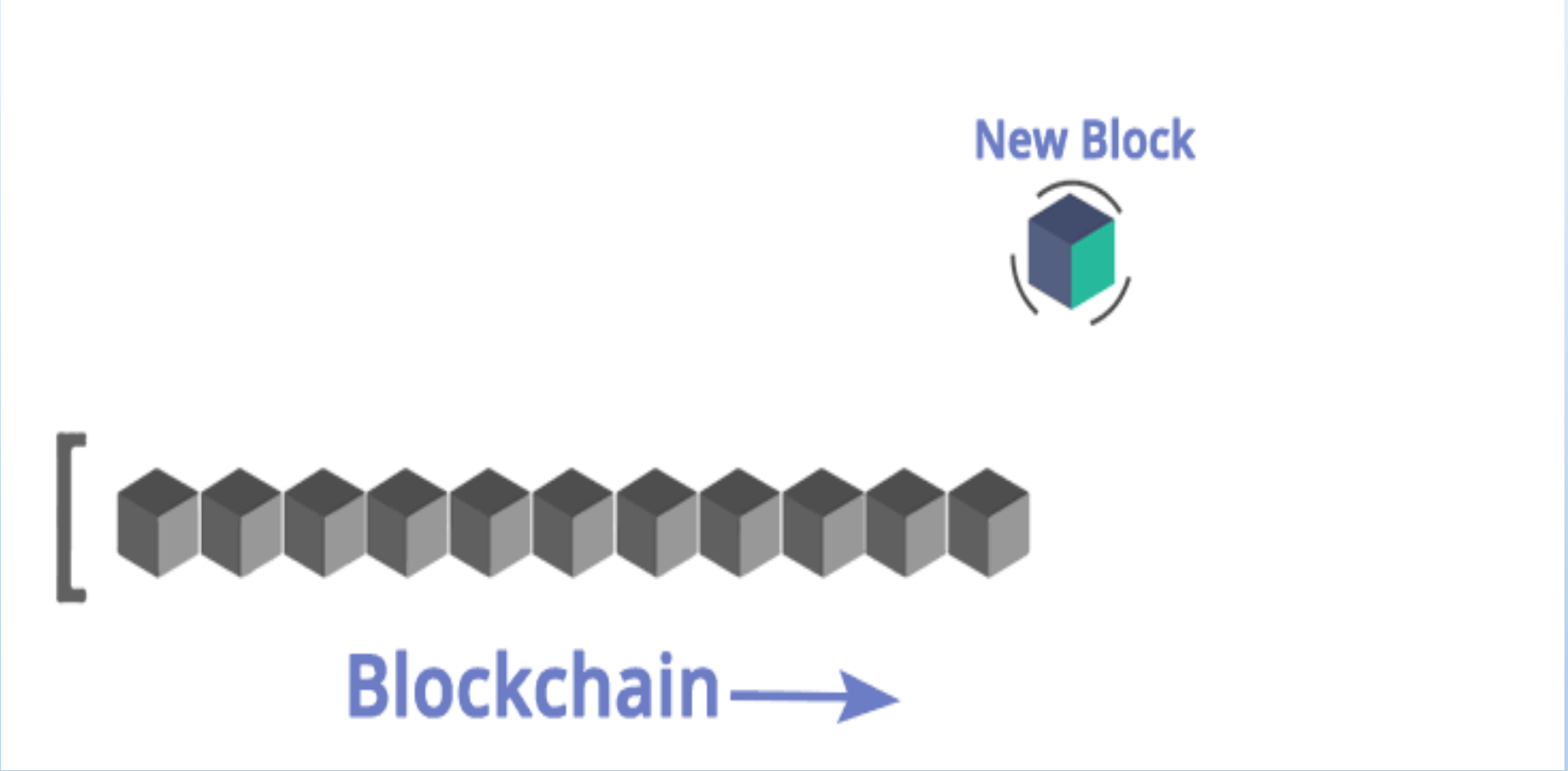
Блокчейн (**blockchain** или **block chain** – **"цепочка блоков"**) – распределённая публичная база всех транзакций, которая объединяет в себе множество блоков, каждый из которых представляет собой определённый тип информации об операциях, совершённых участниками сети.

Блокче́йн (англ. blockchain или block chain) — выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащих информацию.

*Wikipedia

Blockchain. Структура данных.

Blockchain обеспечивает распределенное, неизменяемое хранилище со встроенной проверкой целостности, но имеет максимальную емкость, основанную на стандартном размере блока и скорости блока. Чтобы обеспечить проверку целостности для больших объемов данных, данные хранятся вне сети, а хэш данные — в сети. Это гарантирует, что данные не изменяются, защищая blockchain от раздувания.



Blockchain.

Blockchain. Блок.

Каждый блок включает в себя след техническую информацию:

- Метку времени
- Хеш предыдущего блока
- Хеш корневого узла Дерева Меркла
- Хэш заголовка текущего блока
- Как минимум одну транзакцию

Хеш-функция.

Хеширование (англ. hashing) — преобразование массива входных данных произвольной длины в (выходную) битовую строку фиксированной длины, выполняемое определённым алгоритмом.

Функция, реализующая алгоритм и выполняющая преобразование, называется «хеш-функцией» или «функцией свёртки».

Хеш-функция.

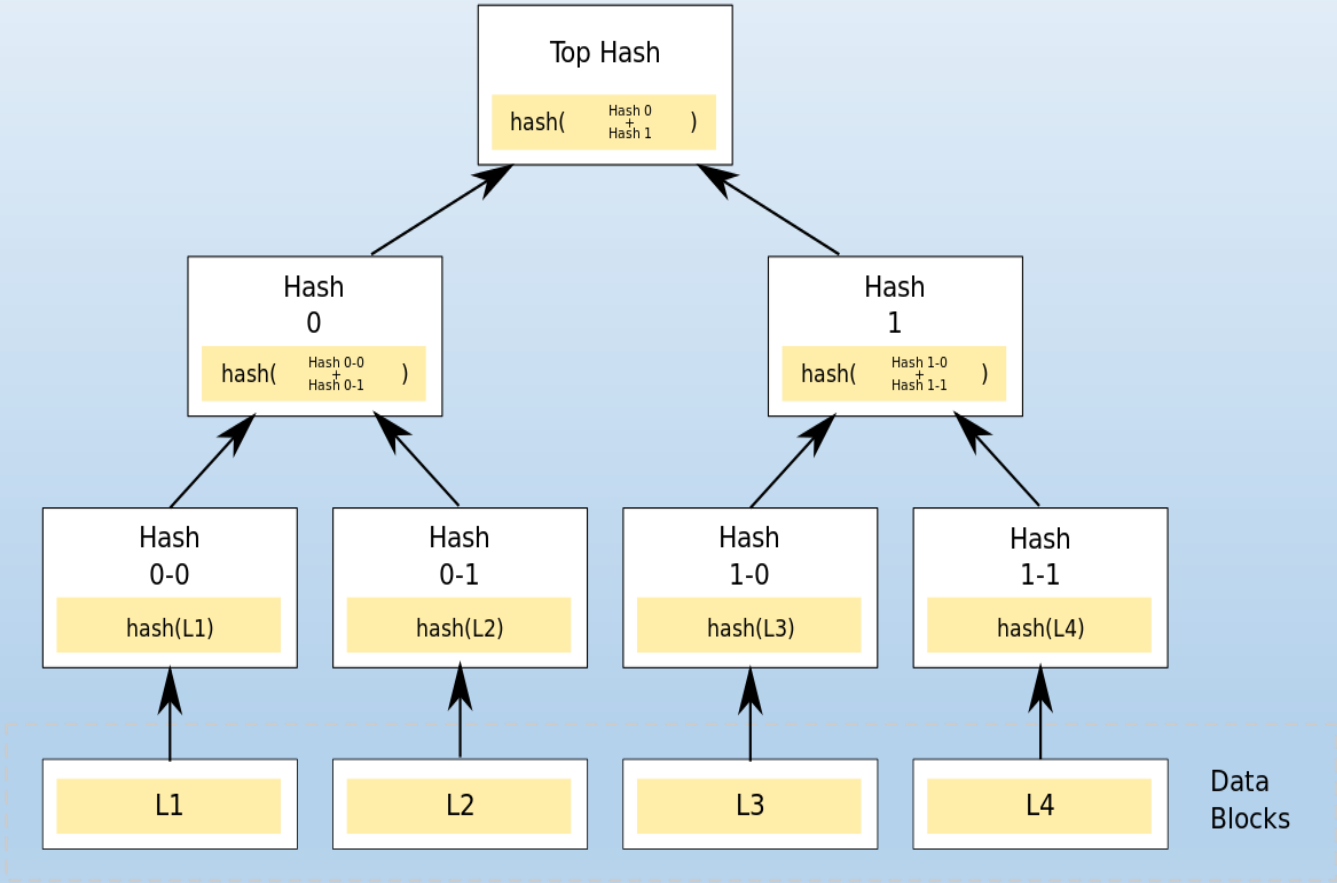
Хорошая хеш-функция должна удовлетворять двум свойствам:

- Обеспечивать быстрое вычисление;
- Иметь минимальное количество «коллизий».

Пример хеша: c4ca4238a0b923820dcc509a6f75849b

Дерево Меркла (хеш дерево) – Merkle tree.

Концепция была запатентована Ральфом Мерклом еще в 1979 году. Дерево Меркла представляет особую структуру данных, содержащую итоговую информацию о каком-то большом объёме данных. Используется для проверки целостности данных и эффективности верификации транзакций.



Заключение.

Blockchain это:

- Децентрализация данных
- Хеширование. Проверка неизменности данных
- Консенсус. Добавление данных

Восемь ключевых технологий.

- Blockchain
- Дроны
- Интернет вещей
- 3D-печать
- Роботы
- Виртуальная реальность
- Дополненная реальность
- Искусственный интеллект

37% российских компаний не используют ни одну из восьми ключевых технологий*

*PricewaterhouseCoopers, 2019

Вопросы.

Что такое майнинг и зачем для этого нужна ферма ?

Майнинг, также **добыча** (от англ. *mining — добыча полезных ископаемых*) — деятельность по созданию новых структур (обычно речь идёт о новых блоках в блокчейне) для обеспечения функционирования криптовалютных платформ. За создание очередной структурной единицы обычно предусмотрено вознаграждение за счёт новых (эмитированных) единиц криптовалюты.

Майнинг - процесс выпуска Биткоина или других криптовалют. Он основан на вычислении математических задач и является главным методом создания криптовалюты.

*Wikipedia

Виды майнинга.

- Любительский

- процессоры компьютера
- видеокарты

- Промышленный

- серверы
- фермы

- Облачный

Заниматься любительским майнингом в настоящее время экономически бессмысленно.

Blockchain. Преимущества.

- Хранение у всех членов системы одновременно, благодаря чему становится невозможным ее взлом и похищение;

- Прозрачность данных совершенных транзакций, благодаря чему любой пользователь может отследить информацию о переводе средств и удостовериться в том, что платеж в системе действительно был отправлен;

- Невозвратность всех транзакций: плательщик не может отозвать или заморозить отправленный денежный перевод «задним числом», обманув таким образом получателя;

- Передача кодов денежных единиц и других виртуальных ценностей от плательщика к получателю напрямую, без участия посредников и без оплаты комиссии.

Blockchain. Недостатки.

- Транзакции в сети блокчейн нельзя отменить или вернуть. Они невозвратные, поэтому, совершив ошибку, с ней придётся смириться;
- У системы блокчейн невысокая производительность, потому использовать её в глобальном масштабе не получится. Она уязвима, потому что обрабатывает слишком мало транзакций в секунду, существенно меньше, чем некоторые другие сети;
- В случае, если один пользователь будет владеть 51% всех блоков, уязвимость сети возрастет;
- У блокчейна нет официального статуса в мире;
- Блокчейн-разработчиков слишком мало, чтобы поддерживать глобальную сеть;
- Отрасль требует колоссальных инвестиций, которых сейчас катастрофически не хватает.

Технология блокчейн несет объективные выгоды и преимущества для пользователей, но является сложным инструментом, находящимся в самом начале своего жизненного цикла.

Развитие технологии блокчейн и сопутствующих ему криптоинструментов будет происходить по мере легитимизации данной технологии государствами и проникновением в общество.

Blockchain это не Bitcoin.

BLOCKCHAIN ≠ 

Вопросы.

Что такое биткоин

Что такое криптовалюты и какие они бывают ?

Биткóйн, или **биткóин** (от англ. *Bitcoin*, от *bit* — бит и *coin* — монета), —пиринговая платежная система, использующая одноимённую единицу для учёта операций. Для обеспечения функционирования и защиты системы используются криптографические методы, но при этом вся информация о транзакциях между адресами системдоступна в открытом виде.

Разные авторы по-разному классифицируют биткойны. Чаще всего встречаются варианты: криптовалюта, виртуальная валюта, цифровая валюта, электронная наличность.

*Wikipedia

Криптовалюта (cryptocurrency) - децентрализованная виртуальная валюта, основанная на математических алгоритмах и защищенная методами криптографии. Выпуск и обращение криптовалют осуществляется на основе технологии blockchain.

Виды криптовалют.

- Currencies Coin (монеты платежной системы)
- Platforms Coins (внутренние токены криптоплатформ)
- Cryptocurrency Exchanges (внутренние токены торговой площадки)
- Utility Tokens (служебные токены)
- Security Tokens (аппаратные токены, являются прямым аналогом ценных бумаг)
- Crypto Commodities (крипто-товар)
- Stable Coins (стейблкоины)

Криптовалюты. Статистика.

Существует **4090** различных криптовалют.

Общая рыночная капитализация виртуальных активов составляет **224 737 477 595$.**

Вопросы.

Преимущества и риски использования криптовалют ?

Криптовалюты. Преимущества.

- Отсутствие единого эмиссионного центра (чаще всего)
- Низкие комиссии за транзакции
- Анонимность переводов
- Круглосуточное функционирование
- Скорость проведения операций
- Гибкость в выборе вида монет
- Высокая защищенность от подделки
- Удобство инвестирования

Криптовалюты. Риски использования.

- Отсутствие единого эмиссионного центра
- Отсутствие гарантий защиты прав потребителей финансовых услуг
- Высокая волатильность криптовалют
- Невозвратность монет при утере ключей
- Отсутствие возможности отозвать платеж
- Если правительства развитых государств запретят хождение криптовалют, они станут атрибутом даркнета

Вопросы.

Зачем люди покупают криптовалюты ?

Объем капитализации рынка криптовалют.

Суммарная капитализация на 31 декабря :

- 2017 год: **$570 млрд.**
- 2018 год: **$140 млрд.**
- 2019 год: **$195 млрд.**
- 2020 год: **$224 млрд.** (текущая)

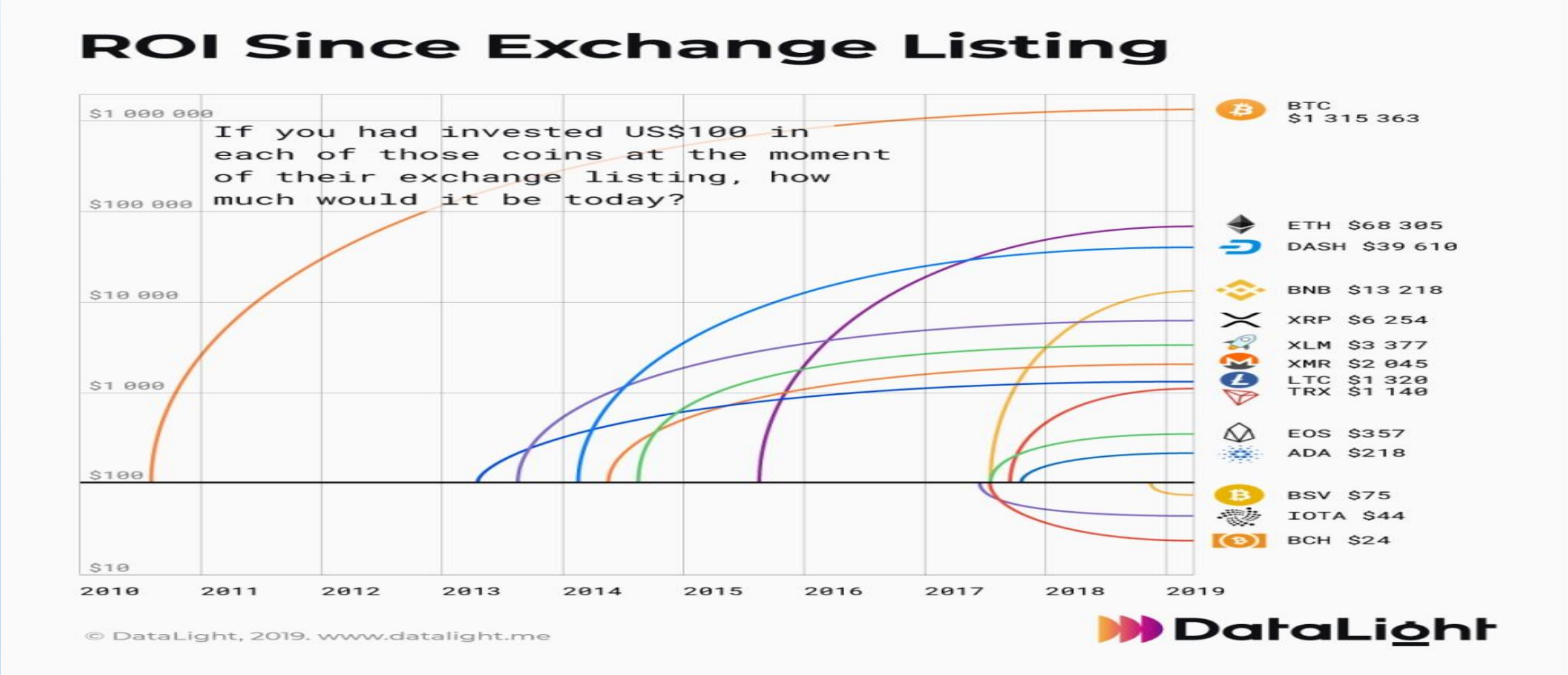
*CoinMarketCap на 8 марта 2020

Объем капитализации криптовалют.

1. Bitcoin (BTC) Монет: 18 195 800 BTC	**$171.96 млрд.** Доля: **64.27%**	**9450$** (↑1.18%) 1.0 btc
2. Ethereum (ETH) Монет: 109 533 945 ETH	**$20.96 млрд.** Доля: **7.83%**	**191.3$** (↑5.31%) 0.02022091 btc
3. XRP (XRP) Монет: 43 685 558 183 XRP	**$11.14 млрд.** Доля: **4.16%**	**0.25493$** (↑6.78%) 0.00002694 btc
4. Bitcoin Cash (BCH) Монет: 18 256 438 BCH	**$6.96 млрд.** Доля: **2.6%**	**381.1$** (↑0.45%) 0.04027678 btc
5. Bitcoin SV (BSV) Монет: 18 254 165 BSV	**$5.13 млрд.** Доля: **1.92%**	**281.2$** (↑0.91%) 0.02971714 btc
6. Tether (USDT) Монет: 4 642 367 414 USDT	**$4.65 млрд.** Доля: **1.74%**	**1.002$** (↑0.18%) 0.00010588 btc
7. Litecoin (LTC) Монет: 63 992 010 LTC	**$4.61 млрд.** Доля: **1.72%**	**72.01$** (↑2.66%) 0.00761014 btc

*CoinMarketCap на 8 марта 2020

Во что могли превратиться ваши 100 долларов, если бы вы инвестировали их «изначально»?



Сколько бы вы заработали, если бы вложили 1000 долларов в эти акции 10 лет назад?

На акциях Netflix:
50 696 $
Акция 10 лет назад:
6,98 $
Акция сегодня:
354,52 $
Доходность:
4979%

На акциях Starbucks:
12 394 $
Акция 10 лет назад:
6,03 $
Акция сегодня:
75,12 $
Доходность:
1146%

На акциях Visa:
10 909 $
Акция 10 лет назад:
14,5 $
Акция сегодня:
160,44 $
Доходность:
1006%

На акциях Facebook:
4 648 $
Акция 10 лет назад:
38,23 $
Акция сегодня:
178,78 $
Доходность:
368%

На акциях Amazon:
22 377 $
Акция 10 лет назад:
78,05 $
Акция сегодня:
1864,82 $
Доходность:
2289%

На акциях Apple:
11 375 $
Акция 10 лет назад:
17,63 $
Акция сегодня:
203,13 $
Доходность:
1052%

На акциях Nike:
6 477 $
Акция 10 лет назад:
13,65 $
Акция сегодня:
88,73 $
Доходность:
550%

На акциях Samsung:
4 136 $
Акция 10 лет назад:
227 $
Акция сегодня:
1034 $
Доходность:
356%

Вопросы.

Как получить криптовалюту ?

Криптовалюты. Способы получения.

- Майнинг
- Покупка за фиатную валюту
- Вознаграждение за работу в сети
- ICO, IEO.

Вопросы.

Как хранят криптовалюты ?

Горячее и холодное хранение кошельков.

Горячее хранение — это все онлайн кошельки, которые дают возможность в любой момент потратить криптовалюту. Горячий метод хранения отлично подходит для частого оперирования небольшими суммами.

Холодное хранение — оффлайн метод хранения, который предполагает сохранение приватного ключа где-то вне интернета. Такой метод хранения в основном используется для хранения больших сумм.

Оптимальные схемы хранения криптовалют.

Цель большинства атак – завладеть закрытым ключом, который позволит вывести средства с кошелька. Подобрать его невозможно, а вот украсть у неопытных пользователей – не сложно.

Ниже перечислено несколько простых, но очень действенных способов которые помогут уберечь криптоалюту от кражи и сохранить свои переводы в тайне:

- Создайте несколько кошельков;
- Остерегатесь любых сервисов, предлагающих хранение ваших средств онлайн;
- Используйте «холодное» хранилище;
- Используйте hardware кошельки.

Вопросы.

Разрешены ли криптовалюты в России ?

Нормативно-правовая база цифровой экономики в РФ.

1. Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей ГК РФ» («Закон о цифровых правах»)
2. Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» («Закон о краудфандинге»)
3. Проект Федерального закона № 419059-7 «О цифровых финансовых активах»

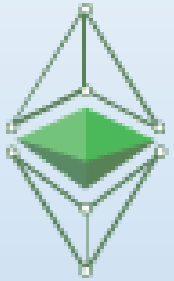
Вопросы.

Могут ли украсть криптовалюту ?

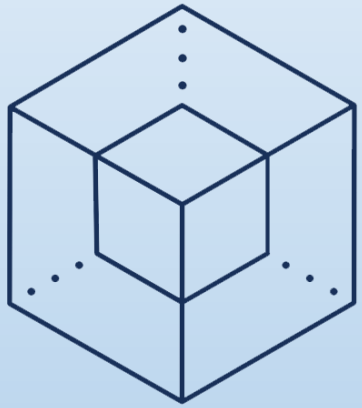
Наиболее распространенные способы кражи криптовалют.

- Программы-вымогатели
- Фальшивые кошельки
- Фишинг
- Финансовые пирамиды
- Фальшивые криптовалюты
- Мошеннические ICO
- Мошенничество на биржах P2P

Самые крупные взломы в блокчейн индустрии за 2019 год.



Classic Ether Wallet



Coincheck

COINDASH

Veritaseum™

Мошенничества на криптобиржах в 2019 году.

- Coincheck - более $ 656,5 млн
- Parity - более $ 30 млн
- Parity - $ 169 млн
- Coindash - $ 8,3 млн
- Veritaseum - $ 8,4 млн
- Etherparty - $ 300 000
- Classic Ether Wallet - $ 300 000
- Yapizon - более $ 5 млн
- Bithumb - $ 1 млн

Рост глобального кибермошенничества. Криптопирамиды.

- BigCoin – основана в 2019 году. Украдено 50 млн долларов.

- OneCoin – основана в 2014 году. Украдено 15 млрд долларов.

У компании было более 3 млн инвесторов.

Компания симулировала технологию blockchain и не выпускала криптомонеты.
С 2016 г. идут расследования в нескольких странах.
Основательница - Ружи Игнатова, скрывается предположительно в РФ.

Криптовалюты. Рост глобального кибермошенничества.

- Прокуроры США арестовали Мэтью Гетче, Джобадию Уикса и Джозефа Абеля по обвинению в организации мошеннической пирамиды BitClub.
- Гарантировали доходность 60 процентов годовых.
- Грозит тюремное наказание до 20 лет лишения за электронное мошенничество.
- С 2014 года 2019 года преступники собрали с участников пирамиды $722 млн.

Криптовалюты. Рост глобального кибермошенничества.

В 2018 г. хакеры украли более $2 млрд у держателей цифровых монет*

В 2019 году эта сумма может увеличиться в разы.

*аналитики Chainalysis

Вопросы.

Как используется технология блокчейн в бизнесе ?

ICO.

ICO (Initial Coin Offering) – форма привлечения инвестиций через выпуск и продажу инвесторам цифровых токенов за фиатные денежные средства или иные криптовалюты.
ICO содержит в себе элементы различных форм привлечения капитала:

- В большинстве случаев в результате вложений в проект инвестор получает актив, торгуемый на публичных торговых площадках, как при публичном размещении ценных бумаг (IPO);
- Как правило, продажа токенов связана с публичной PR-кампанией, свойственной краудфандингу;
- Проект находится на ранней стадии, типичной для венчурного инвестирования.

Smart Contract.

Smart contract - договор между двумя и более сторонами об установлении, изменении или прекращении юридических прав и обязанностей, в котором часть или все условия записываются, исполняются и/или обеспечиваются компьютерным алгоритмом автоматически в специализированной программной среде.

Впервые идея smart contract была предложена в 1994г. Ником Сабо (США) – ученым в сфере информатики, криптографии и права. Он описал smart contract как «цифровое представление набора обязательств между сторонами, включающее в себя протокол исполнения этих обязательств».

Smart Contract. Преимущества.

- Возможность отказа от доверенных посредников;
- Исполнение условий контракта происходит значительно быстрее за счет автоматизации процессов по сравнению со стандартным механизмом выполнения договора;
- Высокий уровень защищенности сторон соглашения друг от друга, так как условия контракта записываются в электронном виде и непосредственно сам contract хранится в распределенной сети. Это делает невозможным внесение изменений в его условия без согласования другой стороной;
- Применение инструментов smart contract дает импульс к появлению новых бизнес-моделей.

Smart Contract. Недостатки.

- Smart contract не обладает функциональной гибкостью;
- Отсутствие в мировой законодательной практике официально закрепленного статуса smart contract может затруднить решение спорных вопросов, возникающих при нарушении условий его исполнения;
- Smart contract в своей основе имеет программный код, который из-за допущенных ошибок на стадии его написания (программирования) может функционировать некорректно, что, в свою очередь, может привести к некорректному исполнению условий smart contract или возникновению условий для совершения мошеннических действий;
- Процесс создания smart contract является сложным, и чем больше условий и аспектов, которые должен отслеживать контракт (состояние товара в процессе транспортировки, таможенные действия и иное), тем сложнее их описать и учесть на момент заключения подобного договора.

Заключение.

Мы все сегодня находимся в динамично развивающемся цифровом пространстве. Криптовалюты являются неотделимым элементом цифровой финансовой экосистемы. Элементом на сегодняшний день технологически сложным, высокорискованным и юридически неопределенным.

Скорость вхождения криптовалют в нашу жизнь будет зависеть, в первую очередь, от позиции правительств и центральных банков.

И наилучшей стратегией поведения, применительно к криптовалютам, является получение необходимого объема знаний понимания происходящих процессов, здравый смысл и должная осмотрительность.

Мнения.

«Я могу рассчитать движения небесных тел, но не безумие людей»

Исаак Ньютон

Разрабатываем

сложные управленческие решения.

Российская Ассоциация
менеджмента знаний
http://km-alliance.ru/

Вагин Сергей Геннадьевич
д.э.н., профессор, DBA
+7 902 371 97 07
vsg63@hotmail.com