BLOCKCHAIN - ЭТО НЕ ТОЛЬКО BITCOIN И КРИПТОВАЛЮТЫ

Николай Брадис
Complex Systems

Руководитель отдела исследований и разработок
В компании занимается техническим руководством всеми проектами, поиском решений для нестандартных задач, изучением и внедрением новых технологий в продукты компании.
Более 10 завершенных IT-проектов в области здравоохранения, образования, сейсморазведки, гидроакустики, гос. управления, text-mining

Блокчейн – что это?

Определения:

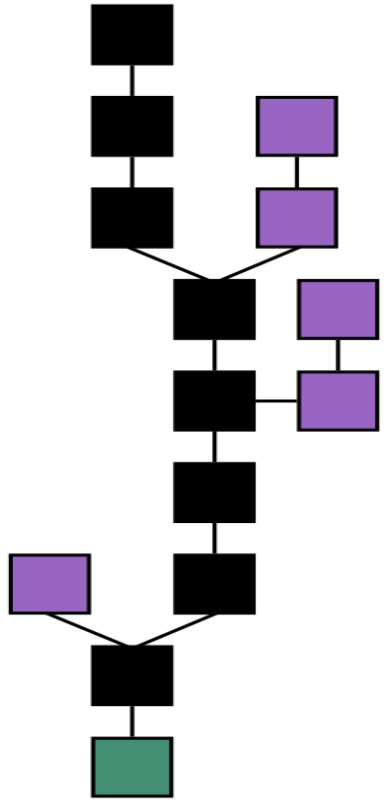
Блокчейн – выстроенная по определённым правилам непрерывная последовательнаяцепочка блоков, содержащих информацию.

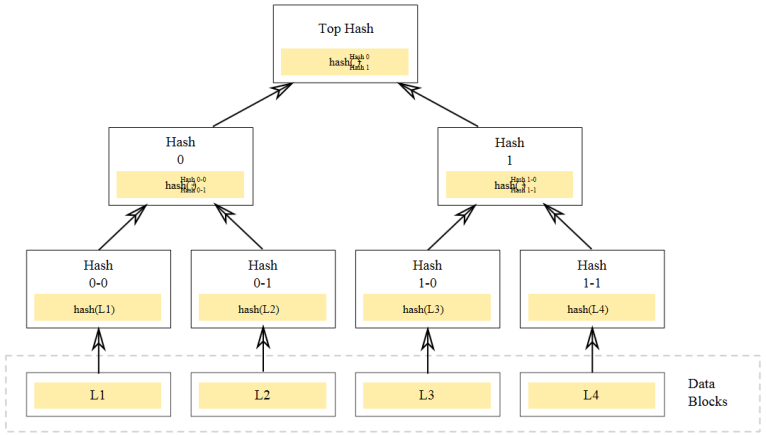
Хэш функция – функция, осуществляющая преобразование входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определенными алгоритмами.

Транзакция – любая операция в blockchain между адресатами. Транзакция считается завершённой и достоверной («подтверждённой»), когда проверены её формат и подписи, и когда сама транзакция объединена в группу с несколькими другими и записана в блок.

Блок транзакций – специальная структура для записи группы транзакций. Содержимое блоков может быть проверено, так как каждый блок содержит информацию (хэш) о предыдущем блоке. Все блоки выстроены в одну цепочку, которая содержит информацию обо всех совершённых когда-либо операциях.

nonce – соль, добавляемая к данным блока при расчете его хэша. Это как раз тот параметр, который перебирают майнеры для того, чтобы полученный ими хэш удовлетворял условиям блокчейн платформы (для биткоин – это определенное количество нулей в начале хэша) и сложности (значение, меньше которого должен быть найденный хэш).





Блок (на примере Bitcoin)

Блок #596830

Сводные данные	
Количество транзакций	1462
Всего выходов	1,276.86230719 BTC
Предполагаемый объем транзакций	175.67357168 BTC
Комиссия за транзакцию	0.08861178 BTC
Высота	596830 (Главная цепочка)
Временная отметка	2019-09-27 10:56:57
Время получения	2019-09-27 10:56:57
Передано по	Unknown
Сложность	12,759,819,404,408.79
Биты	387321636
Размер	622.909 kB
вес	1992.424 kWU
Версия	0x20000000
Nonce (случайно перебираемое число)	2239215633
Награда за блок	12.5 BTC

Хэши	
Хэш	00000000000000000001567d25210f8c3abaefe8b668cb408131ac69ac3fe9a67
Предыдущий блок	00000000000000000000af6f5a0ca421b0e8894f36237e83ea17168c4c42a8d72
Следующий(е) блок(и)	
Корень Меркле	d0aa4f8e8bf1f1e8775a70290254b7e100be17fb4895d4bbe65bd1d7afde3e2a

Майнеры. Кто они?

Майнер – основной ресурс блокчейн-платформы, обеспечивающий ее работоспособность и получающий за это вознаграждение.

Minig Pool – объединение майнеров, позволяющее получить гарантированное вознаграждение за свой вклад в расчет очередного блока. Вознаграждение делится между участниками пула пропорционально их вкладу в расчет блока.

Консенсус

Алгоритм консенсуса в блокчейне – это набор определенных математических правил и функций, регулирующих работу сети.

Функции механизма консенсуса:

Частота генерации новых блоков.

Благодаря данным алгоритмам исключаются ситуации, каждый узел генерирует свой блок и записывает его в блокчейн. К примеру, в сети Биткоин блоки генерируются каждые 10 минут. Однако иногда возникают ситуации, когда два или более узлов генерируют блок практически одновременно, с разницей в долях секунды. В этом случае возникает конфликт, который разрешается в пользу узла, раньше всех создавшего блок. Транзакции, которые входили в конкурентный блок или блоки, помещается в список неподтвержденных транзакций, и отрабатываются в следующем блоке.

Проверка информации в блоке.

Все участники должны подтвердить, что данные в сгенерированном блоке верны. Проверке подлежат хеши транзакций как текущего, так и предыдущего блока, а также корректность подбора числа nonce.

Размер вознаграждения.

Размер вознаграждения зависит от сложности сети, причем, как это ни парадоксально в обратной пропорции.

Алгоритмы консенсуса:

Алгоритм Proof-of-Work – доказательство выполнения работы.

Алгоритм Proof-of-Stake – Доказательство доли владения.

Алгоритм Proof-of-Importance – Доказательство важности.

Алгоритм Proof-of-Activity – Доказательство полномочий.

Smart-контракт

Смарт-контракт («умный контракт») – это компьютерная программа, которая отслеживает и обеспечивает исполнение обязательств. Стороны прописывают в нем условия сделки и санкции за их невыполнение, ставят цифровые подписи. Умный контракт самостоятельно определяет, все ли исполнено, и принимает решение: завершить сделку и выдать требуемое (деньги, акции, недвижимость), наложить на участников штраф или пеню, закрыть доступ к активам.

Сферы применения

Текущее состояние

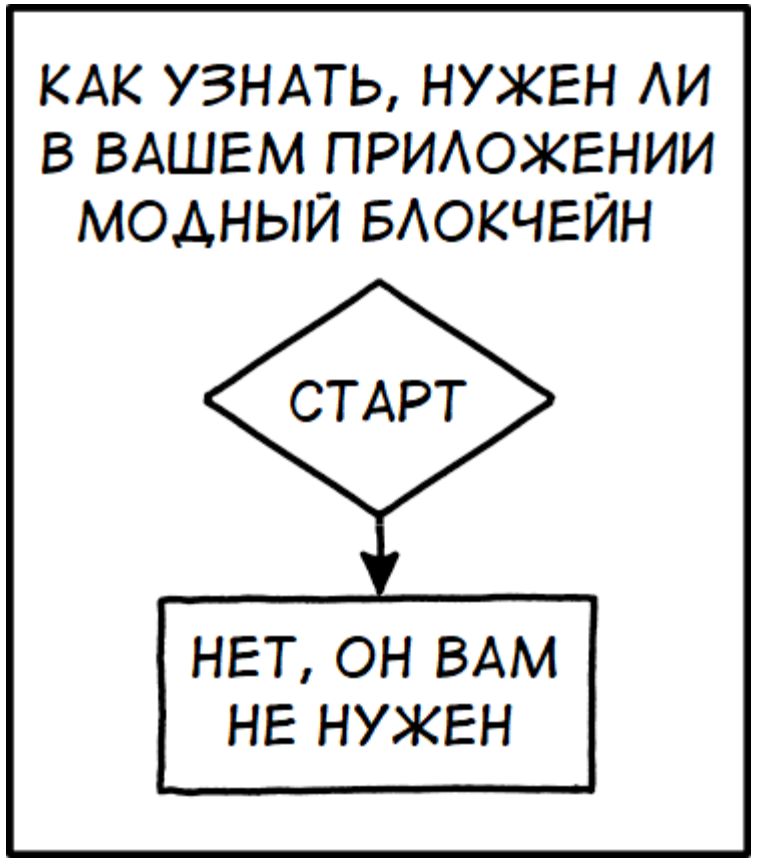
- Много пилотных проектов в страховании, недвижимости, транспорте, энергетике, ресурсных компаниях, судебном делопроизводстве, документообороте, банковском секторе.
- Бум ICO.

Причины отсутствия масштабных внедрений:

- Отсутствие экономического преимущества над традиционными решениями
- Ограничение производительности решений на основе блокчейн
- Неготовность на уровне государства и законодательства
- Ограниченность условий смарт-контрактов только средой блокчейн платформ

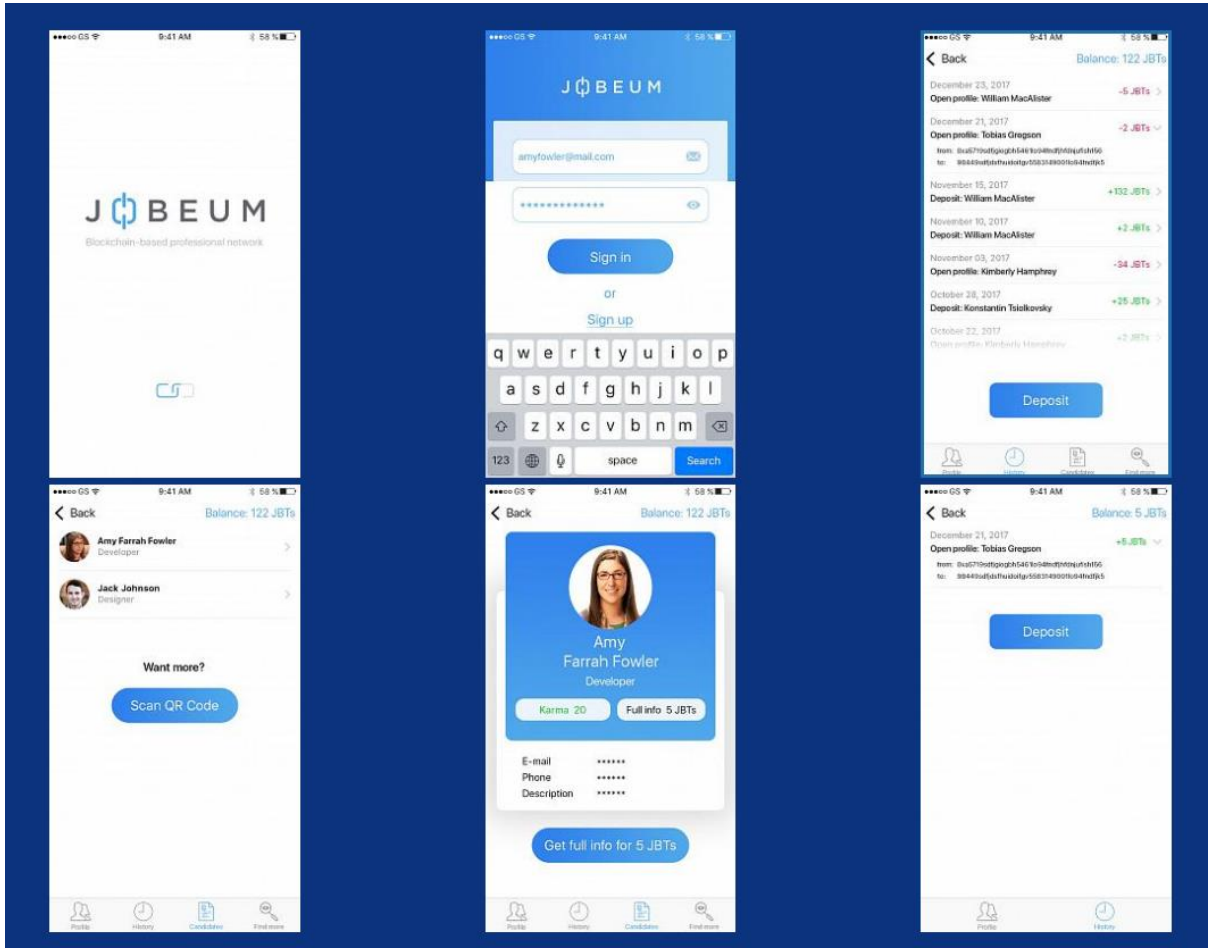
«Стрельнувшие» проекты:

- Humaniq (Alex Fork)
- CryptoKitties



Личный опыт

Jobeum – это децентрализованная социальная сеть для профессионалов, основанная на Ethereum.



Текущее состояние в РФ и выводы

- Технология блокчейн распределенного реестра в последнее время размежёвывается с криптовалютами.
- Растет число публикаций по технологии распределенного реестра
- Создан центр компетенций Национальной технологической инициативы (НТИ) по направлению «Технологии распределённых реестров» на базе Санкт-Петербургского государственного университета (СПбГУ)
- Более 10 проектов по развитию технологии на базе центра НТИ
- В среднесрочной перспективе следует ожидать развития технологии и появления реальных внедрений