Блокчейн и криптовалюты. Что это даёт экономике?

Дробышевский С.М.

Институт экономической политики им. Е.Т. Гайдара

Гайдаровские чтения, Архангельск
28.04.2018

Распределённый реестр

Распределённый реестр (Distributed Ledger Technology, DLT) – одноранговая (peer-to-peer, p2p) сетевая база данных, в которой

- "каждый" участник может иметь копию базы данных,
- "каждый" участник может регистрировать изменения,
- использование механизмов криптографии (ключи, подписи).

Алгоритм консенсуса – набор правил (алгоритмов), по которым производится регистрация изменений в базе данных и определение узлов-лидеров для проведения определённых операций.

Алгоритмы консенсуса

- **Proof-of-Work** – доказательство работы; решение задачи нахождения хеш-функций заголовков блоков заданной сложности для наиболее длинной цепи (майнинг)
- **Proof-of-Stake** – доказательство владения; вероятность сгенерировать следующий блок прямо пропорционально зависит от кол-ва токенов на счету узла (нода)
- **Proof-of-Authority** – доказательство авторитета; блоки генерирует заранее определённый круг лиц

Blockchain

Blockchain – один из вариантов реализации DLT.

Основные характеристики:

- **Общедоступный** дневник записи чего угодно.
- формирование блоков, содержащих некоторый набор транзакций (изменений в базе данных), через хеширование заголовков предыдущих блоков
- Защищён от подделывания. Содержит всю историю. Любую транзакцию/запись легко восстановить/извлечь.
- **Mining** – решение криптографической задачки с использованием компьютерных мощностей. Кто первый решил - тот записывает блок со сделками в блокчейн и получает награду.

Примеры использования блокчейн

- Биткоин и другие криптовалюты.
- Смарт-контракты.
- Системы электронного голосования. Уже использовалось в Эстонии.
- Проведение банковских аккредитивов. Упрощение и ускорение аккредитивных сделок, оцифровка необходимой для сделок информации. Реализуется Альфа-банком в качестве пилотного проекта.
- Ведение кадастрового реестра. Использовалось в Грузии.
- Банковские гарантии. Потенциальные пользователи – банки, имеющие право на выдачу гарантий, торговые площадки (смогут получать из реестра информацию о гарантиях по сделкам), юридические и физические лица, госорганы.

Криптовалюта – разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах.

- Как правило, учёт криптовалют децентрализирован.
- Функционирование данных систем основано на таких технологиях как блокчейн, направленный ациклический граф, консенсусный реестр (ledger) и др.
- Информация о транзакциях обычно не шифруется и доступна в открытом виде.
- Для обеспечения неизменности базы цепочки блоков транзакций используются элементы криптографии (цифровая подпись на основе системы с открытым ключом, последовательное хеширование).

Историческая справка

- Август 2008: зарегистрирован адрес bitcoin.org. Октябрь 2018: опубликована white paper – документ, описивающий схему работы протокола Биткоин.
- Январь 2009: зарегистрирован первый блок, через 9 дней проведена первая транзакция. 5 октября: На бирже New Liberty Standard опубликован первый курс биткоина к доллару: $1=1,309.03 BTC.
- 2011 год. Появились новые криптовалюты-конкуренты. Курс достиг $31 за 1 BTC.
- 2013 год. Цена на короткое время поднялась до $1000 за 1 BTC.
- Январь 2014 года: первая крупная кража 850 000 BTC с биржы Mt Gox, что на тот момент составляло $450 млн.
- В 2016 году существенную нишу занял конкурент биткоина – Ethereum. Это способствовало появлению ICO (первичное размещение монет).
- 17 декабря 2017 году цена BTC достигает максимальной отметки в $20 000. Рыночная капитализация рынка всех криптовалют за год выросла с $11 млрд до $374 млрд.

Динамика цены BTC

Криптовалюты: деньги или актив?

- Средство платежа, но не мера стоимости или средство сбережения.
- Не являются «частными деньгами».
- Не имеют фундаментальной стоимости.
- Не являются финансовой пирамидой.
- Подвержены риску образования ценовых «пузырей».

Выводы

- Новая технология с широким спектром применения.
- Снижение пользовательских издержек.
- Смарт-контракты.
- Парадокс регулирования.
- Анонимность.

Спасибо за внимание!