

вартості до 20000\$ (17 грудня 2017р.) про перспективи біткойнів заговорили навіть найзапекліші скептики. Тисячі інвесторів вклали гроші в BTC в надії на майбутнє зростання курсу криптовалюти. Але вже в 2018 р. ситуація змінилася. Монета Bitcoin, яка показувала активне зростання, раптом почала різко знижуватись, і вже 5 лютого ціна BTC підбралася до позначки в 7000 доларів. На 19 серпня 2018 року ціна на біткойн становить 6402 долари. На тлі такої волатильності поки важко зробити висновок, куди саме піде ціна далі – вгору або вниз. На сьогоднішній день випущено трохи більше половини від запланованого. Сотні тисяч майнерів створюють біткойни по всьому світу, причому створення кожної монети сплачується цими ж біткойнами .

Карбованець – це перша українська криптовалюта, яка була запущена 30 травня 2016 р. В основі монети лежить технологія CryptoNote, яка дає високу ступінь анонімності, а завдяки алгоритму CryptoNight робить її захищеною від ASIC-пристроїв. Карбованець ідеально підходить для майнінгу, як на CPU, так і на GPU. Карбованець – це інтернет-гроші, криптовалюта, така як біткойн, тільки українська і конфіденційна завдяки технологіям Cryptonote. Карбованець – спроба відновити історичну грошову одиницю України в електронному вигляді в якості децентралізованої, анонімної розрахункової одиниці та платіжної системи. Це перспективна робота для багатьох програмістів в Україні. [4, 5]

ЛІТЕРАТУРА

1. Молчанов М. В. Криптовалюта: поняття і проблеми / М. В. Молчанов // Кіберленінка. – 2014. – № 10. – С.3-6.
2. Стригун Ю. І. Що таке біткойни та криптовалюта? / Ю. І. Стригун // Кіберленінка. – 2016. – № 1. – С.5-10.
3. Туров С. Альтернативні гроші: Чому все більше країн світу визнають криптовалюти – [Електронний ресурс]: <http://ua.112.ua/statji/alternatyvni-hroshi-chomu-vse-bilshe-krain-svitu-vyznaiut-kryptovaliuty-364338.html>
4. Перша українська криптовалюта. – [Електронний ресурс]: <http://www.earnua.com/elektronniy-karbovanec-ukrayinska-kriptoaluta-t7332.html>.
5. Карбованець. – [Електронний ресурс]: <http://karbowanec.com/>

РАЗВИТИЕ ПОНЯТИЯ БЛОКЧЕЙН В ИТ-ТЕХНОЛОГИИ

Водопьянов А.Д., Матвеева Т.В.

*Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
e-mail: tatiana_matveeva@ukr.net*

Термин Blockchain частично характеризует его задачи и назначение. Часть «Block» – это блоки, «chain» – это «цепочка». Получается, что Blockchain – это цепочка блоков доступ к которой может получить любой человек. Все блоки выстроены в цепочку, то есть связаны между собой. Для записи нового блока, необходимо последовательное считывание информации о старых блоках. Все данные в блокчейн накапливаются и формируют постоянно дополняемую базу данных. С этой базы данных невозможно ничего удалить или провести замену/подмену блока. Это одна из главных особенностей блокчейна, работу которого можно сравнить с Torrent. Все операции проводятся между субъектами

напрямую. А осуществляются они за счет того, что все участники подключены к одной сети – Blockchain [1].

Публичным лицом-создателем Blockchain, считают Сатоши Накамото в 2009-м году, но скорее всего это псевдоним, за которым стоит один или несколько человек, решивший(-шие) не разглашать свою личность. Очевидно, что на создание блокчейн они потратили тысячи часов.

Существует два вида цепочки: Публичный Blockchain – открытая, дополняемая база данных. Такой вид блокчейна используется в криптовалюте Bitcoin. Каждый участник может записывать и читать данные. Приватный или частный блокчейн имеет ограничения по записи/чтению данных. Могут устанавливаться приоритетные узлы. Подвид Private Blockchain – эксклюзивный блокчейн. В такой цепочке устанавливается группа лиц, занимающаяся обработкой транзакций [2].

Безопасность в технологии блокчейн обеспечивается через децентрализованный сервер, проставляющий метки времени, и одноранговые сетевые соединения. В результате формируется база данных, которая управляется автономно, без единого центра. Это делает цепочки блоков очень удобными для регистрации событий (например, внесения медицинских записей) и операций с данными, управления идентификацией и подтверждения подлинности источника [3].

Сеть blockchain представляет собой своеобразное хранилище цифровой информации, где все данные записываются последовательно в виде блоков. Представить это можно как дневник, хозяин которого четко записывает все свои действия одно за другим, или архив, в котором карточки с данными складываются последовательно, и следующая карточка не будет вложена до тех пор, пока своё место не займет предыдущая. Иначе её называют “технологией распределённого реестра”, так как не существует какого-либо централизованного органа или регулятора, который мог бы распоряжаться блокчейном по собственному усмотрению. Новые блоки в этой базе-цепочке создаются постоянно. Каждый вновь созданный блок содержит группу накопившихся за последнее время и упорядоченных записей (транзакций), а также заголовок. Транзакции – это любые действия, которые пользователи совершают в сети будь-то отправка средств, регистрация прав собственности и т.д. Когда транзакция сформирована пользователем, она отправляется в так называемый мемпул, где дожидается пока ее добавят в один из блоков и этим подтвердят. Когда блок сформирован, он проверяется другими участниками сети и затем, если все согласны, подсоединяется к концу цепочки. Как только это произошло, внести в него изменения уже невозможно. Помимо новой информации блок также хранит в зашифрованном виде данные о предыдущих блоках. База обновляется на всех подключенных к системе компьютерах, а майнеры (валидаторы) приступают к формированию следующего блока [3].

Основные принципы блокчейн: децентрализация и распределенность; безопасность и защищенность; открытость и прозрачность; неизменность уже записанного. Любая значимая информация, относящаяся к той или иной сфере жизни людей, где-то хранится. Покупка дома или машины, взятие кредита, регистрация брака, переводы денег – все данные об этих операциях фиксируются и размещаются централизованно на серверах госучреждений или частных компаний. Это часто приводит к криминальным действиям.

Технология блокчейн кардинально меняет такой подход. База данных хранится не в одном месте, а распределенно на тысячах, а то и десятках тысяч, а порой и миллионов компьютеров, разбросанных по всему миру. Вероятность, что все они будут выведены из строя, ничтожна мала и выглядит фантастической. А пока хотя бы один компьютер сети работает, система, основанная на блокчейн, существует. Взломать один из блоков и изменить информацию в нем смысла нет, поскольку ломать придется все блоки, а для этого нужны гигантские вычислительные мощности. Попытка взлома обязательно будет замечена другими участниками сети. К тому же препятствием к фальсификациям станет и мощный алгоритм шифрования с использованием хеш-функций, а также цифровой подписи. В подписи используется два ключа – открытый и закрытый. Первый необходим для проверки самой подписи, второй используется при ее создании и является секретным. Ключи обеспечивают доступ участникам к той или иной информации. Хеш-функция выглядит, на первый взгляд, как последовательность случайных цифр и букв. Именно она и обеспечивает неизменность всех записанных данных. Как видим, работа сети базируется не на мифическом доверии пользователей друг к другу, а на строгих математических вычислениях. Вся база находится в публичном доступе, а потому посмотреть данные того или иного блока может любой желающий. Например, один пользователь перевел другому 10 тысяч долларов – при желании узнать об этом может каждый. Вопрос в другом, кто и кому перевел деньги – остается тайной. Эта информация доступна непосредственным участникам обмена, если они сами не пожелают ее обнародовать [2].

Блокчейн позволяет напрямую обмениваться данными. Применение этой технологии не ограничивается только финансовой сферой. Блокчейн-технология очень перспективна и сулит очень большие преимущества как для бизнеса, так и для других сфер деятельности. Следует только запастись терпением и ждать, пока ситуация стабилизируется и станет абсолютно прогнозированной, а это рано или поздно непременно произойдет. Многие аналитики называют данную технологию самым большим техническим прорывом со времён изобретения интернета. И хотя некоторые люди настроены скептически, уже сейчас становится понятно, что прогресс не остановить, и технология блокчейна во многом изменит нашу жизнь [4].

ЛИТЕРАТУРА

1. Что такое блокчейн. [Электронный ресурс]: [prostocoin.com](https://prostocoin.com/blog/blockchain-guide). <https://prostocoin.com/blog/blockchain-guide>.
2. Что такое блокчейн простыми словами. [Электронный ресурс]: [paytopro.com](https://paytopro.com/blog/что-такое-блокчейн-простыми-словами). <https://paytopro.com/blog/что-такое-блокчейн-простыми-словами>.
3. Расскажем что такое блокчейн. [Электронный ресурс]: [Coinspot](https://coinspot.io/beginners/что-такое-блокчейн-расскажем-простыми-словами). <https://coinspot.io/beginners/что-такое-блокчейн-расскажем-простыми-словами>.
4. Технология распределенного реестра простыми словами. [Электронный ресурс]: информационно аналитический портал [Mining](https://mining-cryptocurrency.ru/blockchain/). <https://mining-cryptocurrency.ru/blockchain/>.