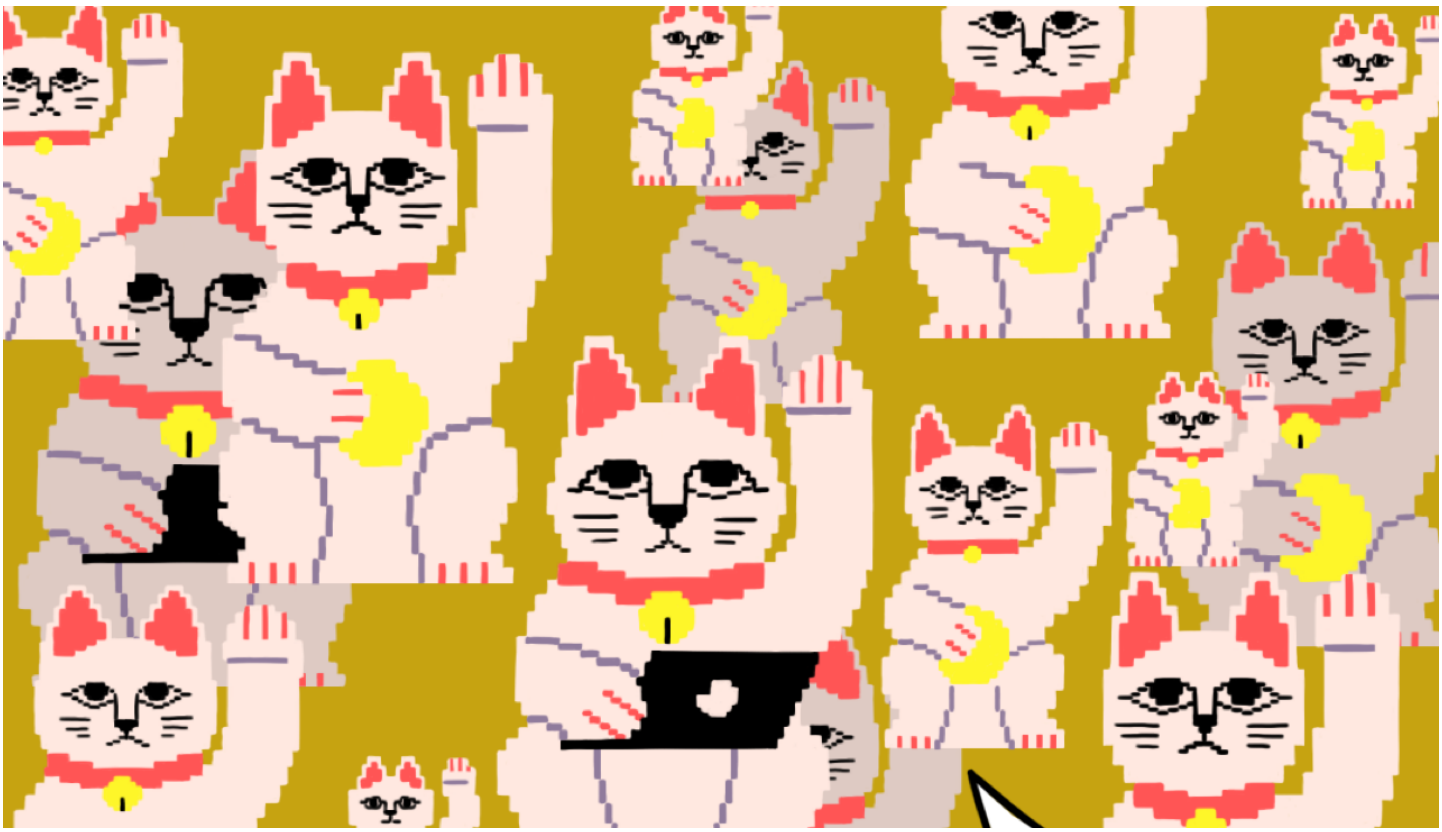
ИСТОРИИ

Блокчейн позволит провести по-настоящему честные выборы в интернете. И не только это Какое будущее ждет технологию, стоящую за криптовалютами

Meduza 16:04, 18 октября 2017



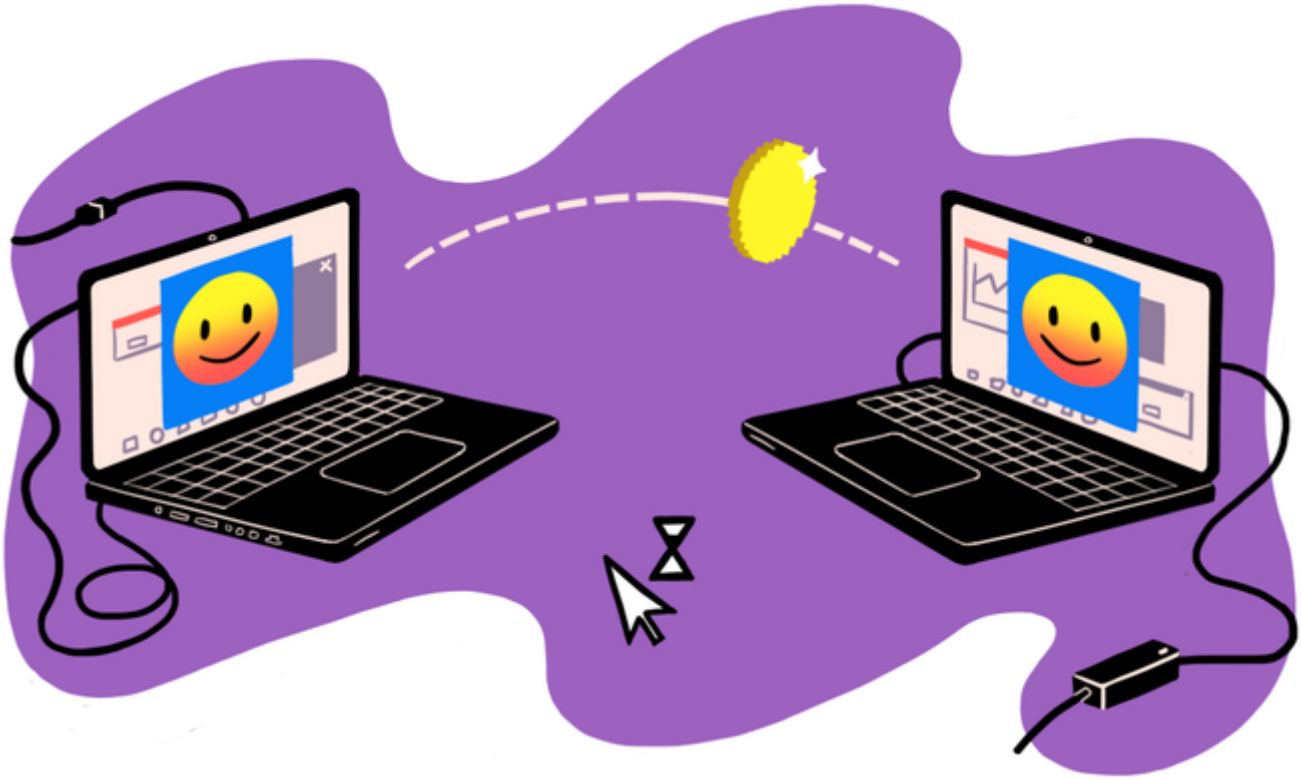
Саша Барановская для «Медузы»

Блокчейн сам по себе — технология как будто из будущего, описанного в научной фантастике, однако сейчас реализован далеко не весь возможный потенциал этой технологии. В будущем с помощью распределенных баз данных можно будет реализовывать самые смелые начинания — например, проводить гарантированно честные выборы в интернете. И это не просто фантазии: существует уже много проектов, по которым так или иначе можно угадать возможное будущее технологии. Редактор «Медузы» Денис Дмитриев рассказывает, по каким сценариям, скорее всего, будет развиваться блокчейн.

Этот материал — часть спецпроекта «Медузы» о блокчейне и криптовалютах; целиком его можно посмотреть здесь.

Отказ от майнинга

Проблема. Биткоин и большинство появившихся вслед за ним криптовалют для генерации новых блоков используют схему proof-of-work (доказательство выполнения работы). Ее главный недостаток заключается в трате впустую огромных ресурсов. Генерация новых блоков — конкурентный процесс. После того как одному из майнеров удается создать такой блок, всем приходится начинать работу с самого начала. Все предыдущие вычисления оказываются бессмысленными. По некоторым подсчетам, к 2020 году майнеры биткоина будут вместе тратить столько же электричества, сколько потребляют жители небольшой европейской страны вроде Дании; уже сейчас они тратят больше энергии, чем все исландцы.



Саша Барановская для «Медузы»

Решение. Чтобы избавиться от этой проблемы, разработчики блокчейнов предложили несколько альтернативных схем генерации новых блоков. Proof-of-stake (доказательство обладания долей): право сгенерировать новый блок получают пользователи, хранящие криптовалюту в виде депозита или вклада, который они не могут тратить какое-то время. Чем больше вы заблокируете собственных средств, тем выше ваш шанс заработать. Вторая по популярности криптовалюта Ethereum планирует начать использовать схему proof-of-stake в 2018 году. Proof-of-burn (доказательство уничтожения): тут вероятность продолжить цепочку зависит от того, сколько валюты вы уничтожили — перевели на адрес, к которому ни у кого нет доступа. Проще говоря, чтобы заработать криптовалюту, вам сначала придется расстаться со старой. Например, в 2014 году участники децентрализованного обменника CounterParty получили стартовый капитал в системе, сжигая свои биткоины. Proof-of-capacity (доказательство вместимости): валюта начисляется за использование места на жестком диске пользователя. В качестве примеров можно привести проекты SpaceMint и Permacoin.

Честные выборы

Проблема. Некоторые западные страны начинают использовать электронное голосование на выборах и референдумах. Теоретически этот шаг должен увеличить явку избирателей: проголосовать можно из дома в любое удобное время, потратив на весь процесс минимум времени. Но такую систему можно попытаться взломать. Из-за сложности протоколов электронного голосования, потенциальных компьютерных ошибок и хакерских атак избирательные комиссии в Казахстане (2011) и Нидерландах (2008, 2017) возвращались к бумажным бюллетеням, урнам и ручному подсчету голосов.

Саша Барановская для «Медузы»

Решение. Выборы с использованием блокчейна похожи на обычную сделку в криптовалюте. Граждане получают от избирательной комиссии специальные крашеные монеты, которые затем переводят на один из специальных счетов, связанных с тем или иным кандидатом. Для определения победителя достаточно проверить счета после окончания выборов. Так как публичный блокчейн может проанализировать любой желающий, каждый пользователь может отследить судьбу своего голоса. А для того чтобы члены избиркома не могли деанонимизировать избирателей, ученые предлагают распределять крашеные монеты с помощью технологии слепой подписи.

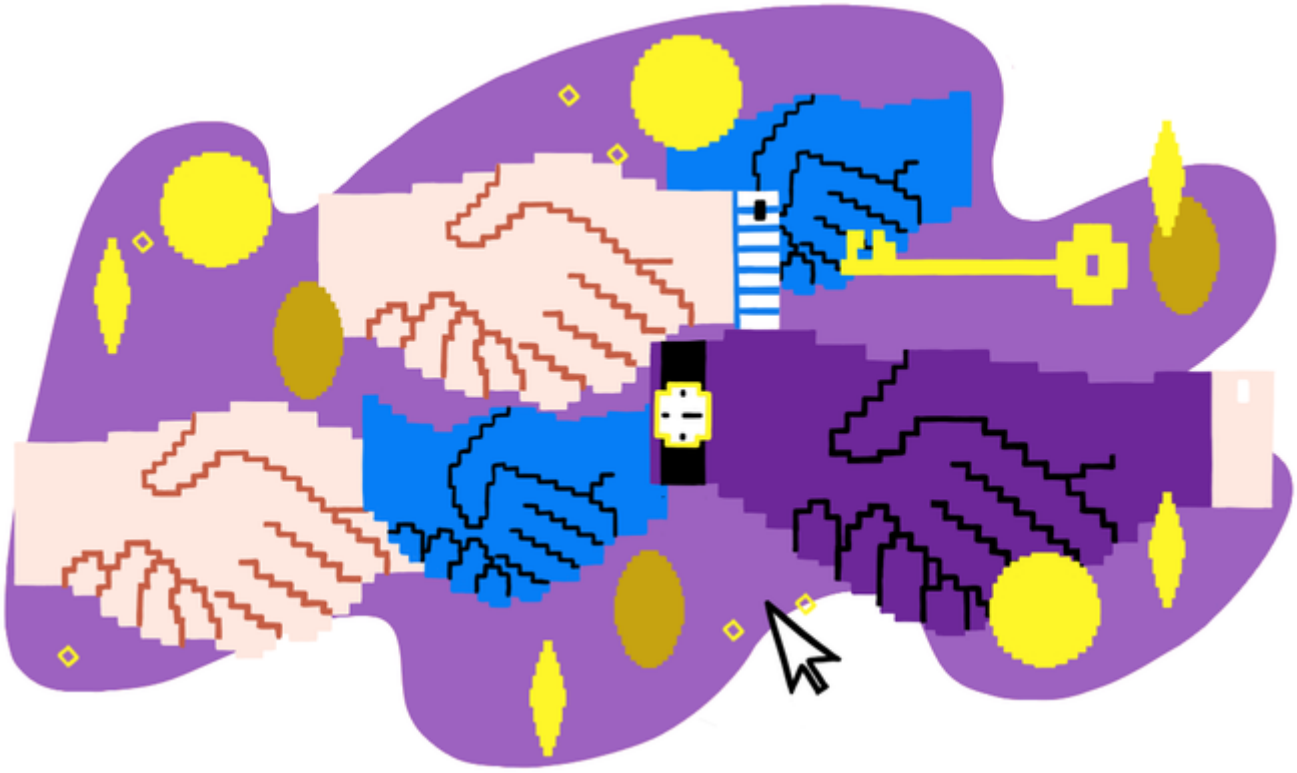
Безотзывное доменное имя

Проблема. Система доменных имен (DNS) позволяет пользователям посещать сайты, не зная их IP-адресов. Но сайты не владеют этими именами — доменное имя у сайта можно отобрать под самыми разными предлогами. Через такую процедуру в разное время проходили торрент-трекер The Pirate Bay, проект WikiLeaks, российская библиотека Flibusta.

Решение. С помощью блокчейна можно создать устойчивую к цензуре систему доменных имен. Пользователь может намайнить или купить специальную криптовалюту и потратить ее на регистрацию сайта в специальной доменной зоне (вроде.bit в Namecoin,.p2p в KeyID,.nxt в NXT). В транзакции конкретное имя будет привязано к его IP-адресу. Вместо IP-адреса можно использовать адрес в сети Tor (его, как правило, сложно запомнить), b32.ip-адрес в анонимной сети I2P или любой другой подобный. Поменять этот адрес сможет только его владелец. Забрать доменное имя в принудительном порядке никто не сможет — надо только не забывать продлевать регистрацию. Пока подобные проекты не получили широкой поддержки, поэтому для того, чтобы попасть на сайт с таким именем, нужно найти и подключиться к DNS-серверу, который умеет работать с конкретным блокчейном и которому вы доверяете. Или установить или настроить собственный (например, DNSChain).

Реанимация умерших торрентов

Проблема. Торренты — удобный способ распространения тяжелого и зачастую не вполне легального контента. Но шансы скачать редкий или давно выложенный альбом или фильм обычно невысоки. Все зависит от альтруизма сидеров — пользователей, раздающих контент. Они, как правило, не получают ничего взамен (кроме повышения коэффициента раздачи, который важно поддерживать на определенном уровне в закрытых торрент-трекерах).



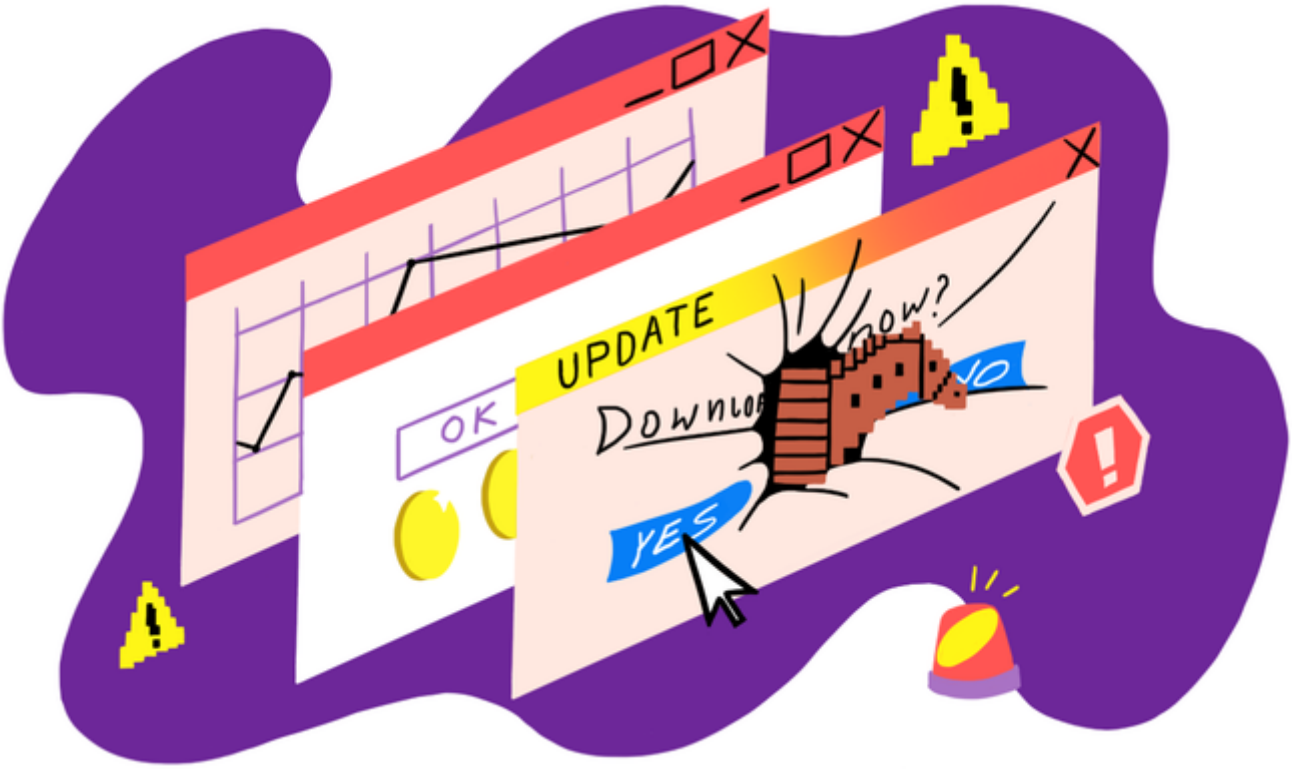
Саша Барановская для «Медузы»

Решение. Создатели торрент-клиента Tribler с помощью блокчейна решили построить репутационную систему для поощрения сидеров и наказания пользователей, которые закрывают раздачи сразу после скачивания файла. В основе такой системы лежит технология MultiChain. Вместо построения единой цепочки с общей историей обо всех переданных и полученных файлах (по аналогии с биткоином) для каждого пользователя строится своя, отдельная

цепочка. Каждый блок фиксирует взаимодействие двух пользователей — скачивающего и раздающего контент — и объем переданных данных. Такой блок записывается каждому из них в цепочку. Каждый узел сети, ориентируясь на эти данные, может принимать решение — отказать этому пользователю в раздаче или принять его запрос. Поддержка MultiChain появится в стабильном выпуске Tribler (пока можно установить тестовую версию).

Защита от таргетированной атаки

Проблема. Если хакеру интересна не любая потенциальная жертва, а конкретно вы (ваше устройство, данные, контакты), он может попытаться осуществить целенаправленную, таргетированную атаку. Даже если ваш компьютер надежно защищен, злоумышленник с хорошими связями может попытаться взломать ваш компьютер через установку обновлений. Вместе с новой версией программы будет установлен или просто запущен вредоносный код. Через систему обновления украинской бухгалтерской программы распространялся, например, вирус-вымогатель Petya. (Правда, эта атака не была таргетированной — зараженное обновление рассылалось всем клиентам.)



Саша Барановская для «Медузы»

Решение. Обнаружить такую атаку можно, сравнив загруженное по сети обновление с тем, что получили другие пользователи. Если окажется, что вы скачали другой файл, — это повод бить тревогу. В публичном блокчейне можно хранить информацию об установленных пользователями программах. Если хеш-сумма загруженного вами пакета совпадает с хеш-суммами других пользователей, все в порядке. Пока существует только прототип такой защиты пользовательского репозитория для дистрибутива Arch Linux.

Архивы, которые нельзя подделать

Проблема. Дату и время создания, модификации или последнего обращения к файлам, хранящимся в наших компьютерах, обычно легко сфальсифицировать. Для этого достаточно перевести назад системные часы на компьютере и проделать необходимые операции. Эта проблема существует даже для тех, кто думает о безопасности и пользуется системами шифрования информации. В асимметричном шифровании владелец приватного ключа (используемого для дешифровки сообщений или создания подписи) в случае его потери или кражи может отозвать свои ключи — так его собеседник понимает, что если сообщение подписано этим ключом, перед ним злоумышленник. Проблема в том, что хакер легко может обойти это ограничение — создать и подписать сообщение задним числом. Наконец, достоверно установить точное время бывает необходимо в ходе расследований или судебных разбирательств.

Решение. Проект OpenTimestamps предлагает использовать блокчейн для сохранения информации, которая позволит доказать, что тот или иной файл был создан не позже определенной даты. При осуществлении сделки в транзакцию можно записать строчку с хеш-суммой вашего файла — вычислить ее для несуществующего объекта невозможно. В каждом блоке записана дата его создания. Изменить или подделать эту временную отметку практически невозможно. Другой вопрос, что из-за низкой пропускной способности большинства блокчейнов (особенно биткоина) записывать хеш-сумму всего лишь одного файла в одну транзакцию очень неэффективно. Поэтому OpenTimestamps использует древовидное хеширование: информация об отдельных файлах хранится во внешней базе данных, а в блокчейн записывается лишь их общая хеш-сумма. Благодаря этой технологии весной 2017 года с помощью всего лишь одной транзакции в биткоине была зафиксирована информация о 750 миллионах файлов, хранящихся в веб-архиве archive.org.

Денис Дмитриев