



Сергей
ГОЛУБИЦКИЙ
специально
для «Новой»

На выборах в Мосгордуму в трех округах провели экспериментальное «дистанционное электронное голосование» с использованием криптографии и технологии блокчейна. В процессе голосования система дважды ломалась и голоса избирателей-добровольцев в системе не регистрировались в течение 40 минут и часа. Представители избирательной комиссии успокоили общественность доходчивой фразой: «Сработала заглушка в грейлоке, данные пропали, потом появились».

Самые дотошные бросились шерстить «Гугл» в поиске объяснения того, что такое *грейлок*, но их мигом добили, чтобы не выпендривались: намекнули, что «пошла нулевая транзакция». Приставучая общественность сделала вид, что все поняла («А-а-а, нулевая транзакция! Так бы сразу и сказали»), и отстала.

После выборов эксперты-пятоколонщики нагло заявили, что в эксперименте с «блокчейн-голосованием» блокчейном даже не пахло, поэтому виновата не технология, а кривые руки. Эксперты-патриоты напомнили о первом блине. И вообще, нечего метать икру: ошибки учатут, систему доведут до ума и в следующий раз все замечательно срастется.

Одна только незадача: блокчейн — не блин, желанный в каждой хате. Блокчейн в глазах 99% населения — это мухомор. Причем не из соседнего леса, а заморский. И оттого — враждебный. Уровень понимания этой технологии в нашем обществе устойчиво полошется ниже плинтуса. Не потому, что люди глупые, а потому, что блокчейн — реально штука сложная. Не столько в техническом отношении (хотя и там — не подарок), сколько в психологическом.

Из непонимания рождается оправданное сомнение, которое рано или поздно превращается в энергичное отторжение. И вот уже широкая общественность усматривает в модном инородном веянии что-то вроде новаторского мошенничества.

Негатив в населении деловито распапляет пресса: «Кузминский суд Москвы заключил под стражу на месяц хоккеиста Игоря Мусатова, который обвиняется в мошенничестве с криптовалютой на 800 тыс. долларов» — фирменная новость осени 2019 года.

Как прикажете на таком информационном фоне оценивать блокчейн-голосование на выборах в Мосгордуму? Технология сама по себе мутная, не удивительно, что наблюдателям не дали каких-то там секретных ключей и доступ к блокчейну закрыли. Правда, журналиги из «Медузы» эти ключи где-то нарыли (вот же ушлые племя!) и голоса расшифровали. Что бы это ни значило.

Одним словом, патриотический обычай в очередной раз разжился сочным поводом ткнуть обличающим перстом в Запад, а вечно неудовлетворенный либерал получил новое неоспоримое доказательство мухлежа кровавого режима.

Все это очень печально, потому что технология блокчейна сама по себе потрясающая, и дискредитация ее кривым исполнением — трагедия.

Нужно ли вообще применять блокчейн в голосовании? Универсального ответа нет, потому что все зависит от конкретных обстоятельств. Теоретически технология блокчейна может дать неспоримые экономические и политические преимущества.

В экономическом отношении показателен опыт Эстонии, где возможность использовать альтернативное электронное голосование предоставляется с 2005 года. На парламентских выборах 2019 года через интернет проголосовало рекордное число избирателей — 43,8% от общего числа.

Мутная технология

УРОКИ МОСКОВСКИХ ВЫБОРОВ НА БЛОКЧЕЙНЕ



Считается, что каждый раунд электронного голосования позволяет стране экономить более 11 тысяч полных рабочих дней. Ежегодно блокчейн сберегает для Эстонии 800 лет человеческого труда (в эту цифру включено не только голосование, но и обширная блокчейн-инфраструктура, развернутая во всех областях — от здравоохранения до регистраций гражданских актов и ведения бизнеса).

Политические преимущества голосования на блокчейне обеспечиваются двумя ключевыми характеристиками технологии — устойчивостью к цензуре и безоткатностью транзакций. Применительно к процессу голосования это проявляется следующим образом.

В нашей стране уровень доверия к любой форме компьютерного вмешательства в процедуру голосования — нуль

Современные представления о демократичных и честных выборах предполагают выполнение ряда простых условий:

- участие в голосовании могут принимать только те граждане, которые имеют на это право;
- один гражданин может подать только один голос;
- все поданные голоса должны быть анонимны;
- после того как голос подан, он не может быть изменен ни на одном этапе, включая саму процедуру подсчета;

— результаты голосования должны легко проверяться.

Экосистема любого блокчейна строится на двух понятиях: монетах (токенах) и праве владения этими монетами. Единственная операция, возможная в блокчейне, — это передача монеты от одного собственника другому (это и называется транзакцией).

Технология блокчейна заточена на обеспечение трех правил, таких же элементарных, что и сами ключевые понятия (монеты и право владения):

— пользователь может совершать транзакции только тех монет, которыми владеет;

— пользователь не может перевести одну и ту же монету дважды (совершить т.н. двойную транзакцию);

— после совершения транзакции ее невозможно отыграть обратно.

Вот так вот все просто. Самое же потрясающее: на основании этих элементарных правил можно формализовать практически любую социальную активность человека.

Смотрите, как структура блокчейна ложится на процедуру идеальных выборов. То, что нам кажется таким сложным, в реальности сводится всего к двум транзакциям:

Транзакция № 1: Пользователь (=избиратель) подтверждает свое право владения (=право участвовать в голосовании) и в обмен на это право получает от системы 1 монету.

Транзакция № 2: Пользователь передает свою монету другому пользователю (=кандидату на выборах, за которого он хочет проголосовать).

Это и есть вся процедура голосования! Задача блокчейна — обеспечить уже знакомые нам стандартные условия: подтвердить право избирателя на голос (=владение монетой); проследить, чтобы не было двойной транзакции (=одна и та же монета не была переведена двум разным

кандидатам); устранить связь между пользователем и его транзакцией (=обеспечить анонимность); обеспечить невозможность внесения изменения в транзакцию (=акт подачи голоса за одного кандидата) после того, как эта транзакция попала в блокчейн (=систему голосования).

Как я уже говорил, все перечисленные условия реализуются в любом блокчейне нативно. То есть естественным образом и автоматически. Для этого эта технология и создавалась.

Остаются два условия из списка идеального голосования: полная проверяемость транзакций в блокчейне (=результатов голосования) и отсутствие связи между собственником монеты и совершенной им транзакцией (=анонимность голосования).

Современные блокчейны блестяще справляются и с тем, и с другим. Но существует ряд хитростей, которые, судя по всему, и помешали московскому эксперименту завершиться триумфом, а не мухомором.

Если кто-то не знает, то сегодня в мире существуют десятки различных типов блокчейнов, сотни вариаций каждого типа и тысячи конкретных реализаций. Все они выполняют разные задачи, соответственно, не каждый блокчейн обеспечивает открытость, прозрачность и проверяемость. И лишь немногие блокчейны реализуют подлинную анонимность.

Глобально блокчейны бывают инклузивными (то есть такими, которые не требуют ничего разрешения для подключения и участия) и эксклюзивными (в них к контролю допущены только официально уполномоченные участники системы).

Эксклюзивные блокчейны созданы специально для обслуживания корпоративных интересов, поэтому они закрыты для внешнего аудита. Инклузивные блокчейны — все известные нам криптовалюты.

Очевидно, что ни о какой прозрачности, открытости и проверяемости по первому требованию в эксклюзивных блокчейнах не может быть и речи. Проблема московского эксперимента с блокчейн-голосованием в том, что его провели на эксклюзивном закрытом блокчейне. Все ноды системы были развернуты где-то в недрах департамента информационных технологий, поэтому общественность была вынуждена клянчить какие-то ключи для расшифровки того, что принципиально не должно быть зашифровано.

Помимо экономического и политического аспекта у технологии блокчейн в контексте голосования есть еще и аспект психологический. Последний связан в первую очередь с уровнем технологического развития общества.

В нашей стране уровень доверия к любой форме компьютерного вмешательства в процедуру голосования (после близкого знакомства с работой системы ГАС «Выборы») — нуль. Уровень доверия к иноземному подрывному мухомору (блокчейну) — ниже нуля.

На таком психологическом фоне заикаться о политической (тем более — экономической) пользе блокчейн-голосований можно либо по недомыслию, либо ради освоения фондов.

Усилия государства и общества должны направляться на восстановление доверия к технологиям, дискредитированным кривыми имплементациями. Популяризировать, объяснять на пальцах, терпеливо развивать интерес и прививать доверие к блокчейну, с которым связывают свое будущее все технологически развитые государства, — вот задача-максимум на обозримое будущее.

Голосовать нужно в стеклянных урнах перед веб-камерами под присмотром не каких-то мистических комиссий, а любых желающих — предпочтительно рядовых граждан. Голоса считать надо открыто и в светлое время суток, а не при свечах на спиритическом сеансе. И будет тогда власти — доверие, а народу — счастье.