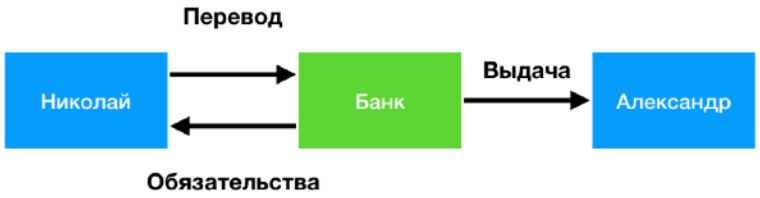
Консенсус - ложь

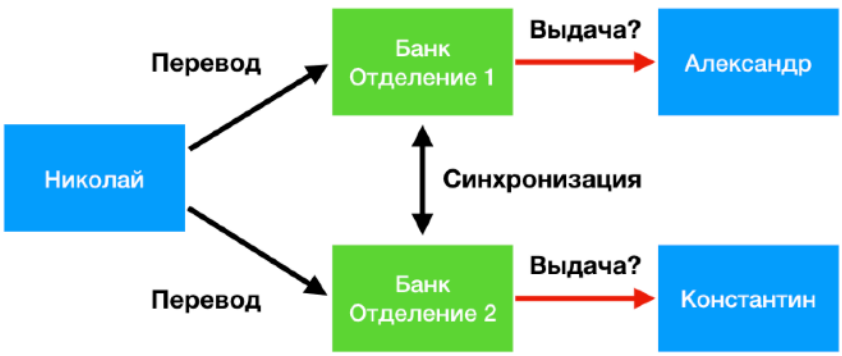
Многие знают что в блокчейне и системах на основе него одной из главнейших вещей является консенсус, договоренность машин и людей о чём либо по установленным правилам. Но... так ли это на самом деле? И не является ли это... обманом самого себя? В статье ниже мы в этом и разберёмся.

Для начала поймём а зачем вообще нужен консенсус и что это такое. Пусть у нас будет один банк и один вкладчик Николай, на счету которого числится 1000 рублей. Он отправляет письмо в банк с просьбой перевести все деньги на счёт своего друга Александра. И всё прекрасно - деньги списались с одного счета и записались на другой. В данном случае проблем никаких и нет, а новый владелец денег решил снять их в ту же минуту и всё хорошо.



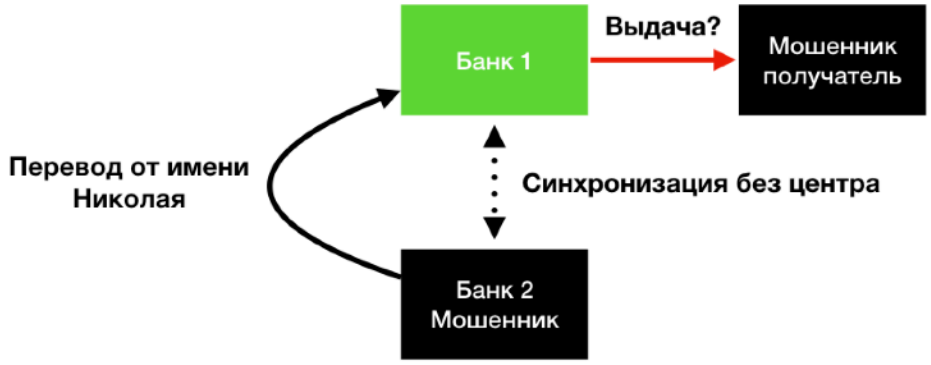
Но что если у банка сразу два отделения?

На счету Николая всё те же 1000 рублей, но теперь уже два друга, Александр и Константин, которые находятся в обоих отделениях и ждут когда деньги поступят на счёт чтобы взять их и уйти. И приходят два письма в оба отделения, но в одном из них 1000 рублей переходят Александру, а в другом Константину. И из 1000 рублей возникает 2000. И чтобы такое не могло произойти - каждое отделение банка должно оповестить остальные что деньги списаны и перечислены кому-либо, тогда вторая попытка их списать не выйдет - денег то на счету уже и нет. А кому достанется 1000 рублей? В идеальном мире тому на чьё имя письмо пришло первым, возможен вариант и с тем что отправителя попросили бы пояснить кому всё таки назначен был перевод. И всё ведь хорошо же, проблем нет.

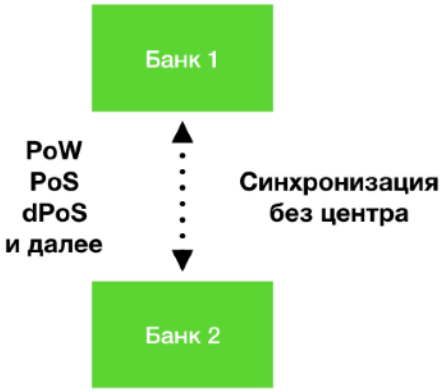


Но это всё ещё не тот консенсус что используется в современных криптовалютах.

А что если отделения банков на самом деле не являются отделениями, они просто мелкие частные банки, подключённые к единой системе платежей без центрального сервера? Почему бы и нет, вполне себе практика для разных сфер. Только система без лидера, просто договорились о партнёрских соглашениях и пересылают друг другу изменения на счетах общих клиентов, всё хорошо... или нет. Если произойдёт событие как в примере выше - кто решит кто был прав и кому достанутся деньги? А ведь время прихода этого письма даже в современном сверхбыстром интернете может оказаться одинаковым - ведь есть куча задержек, есть время обработки сервером - нельзя просто так взять и решить кто был первым, ведь не ясно какое из писем было отправлено первым в действительности, до определенного размера шкалы времени. И так вот оказалось что письмо по ней то и пришло в одно и тоже время, полностью идентичное, но с разными получателями средств. Какой из этих двух банков будет прав когда начнёт распространять всем другим банкам что теперь на счету указанного клиента такое вот количество средств? Как понять кто прав? А если один из банков вообще мошенник?



Собственно так и появились системы консенсуса. У самой популярной криптовалюты Bitcoin это PoW - доказательство мощности майнера, высчитывающего бесполезные для мира, но полезные для консенсуса хеши. Есть ещё PoS где прав тот «банк» у которого больше денег на его счету, а ещё есть dPoS где выбираются делегаты, которые решают кто прав, причём сила голоса избирателей равна количеству денег на счету, а вот делегаты уже решают просто большинством или по иным правилам. Есть множество других консенсусов разной степени равноправия и скорости работы. И вроде бы всё прекрасно.

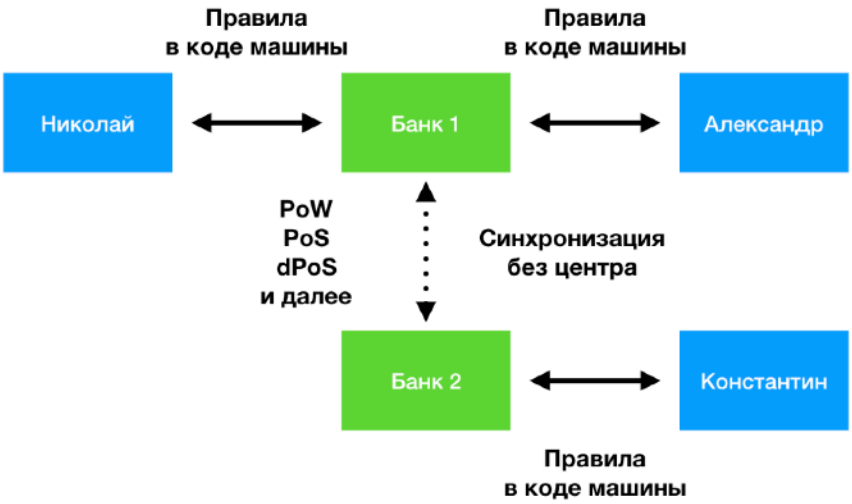


Но есть нюанс...

Приходя в магазин вы покупаете товар, а если товар оказался плохим, то обычно можно прийти и поменять его на новый, или на деньги обратно. Но может так что вы купили что-то с рук или в путешествии, вы можете никогда больше не встретить продавца который продал вам товар, так что по качеству претензий особо применить не получится. Ну а деньги - деньги на самом деле в современном мире всё чаще лежат не у вас в кармане, а в банке, а у вас есть лишь ключик в виде карточки или вообще записи в Apple Pay на вашем же телефоне. Одно прикосновение и «письмо» улетает через цепочку разных провайдеров и банков, списывая средства в одном банке и записывая их в другом, возможно в другой стране. И все всем доверяют. Но что пошло не так что появилась потребность в криптовалютах и консенсусах? Это пояснит вот эта микро-игра (только возвращайтесь потом назад, далее начнётся самое интересное):

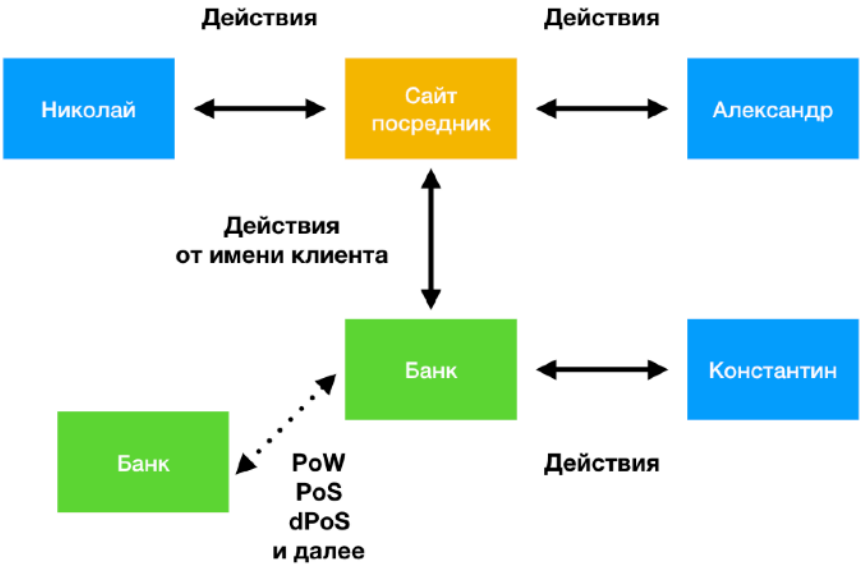
На русском: https://notdotteam.github.io/trust/
Оригинал: https://ncase.me/trust/

Дело в том что есть сферы где кейс взаимодействия состоит в том что раундов взаимодействия всего один, а анонимность даёт возможность и правда сделать его одним. В результате самым эффективным способом работы будет обман - обмануть партнера и получить больше, ведь больше вы никогда не встретитесь. Теория игр сурова, но справедлива. В итоге, в таком ключе необходима система, которая позволит обойти эту проблему, технически заставит соблюдать эти правила.

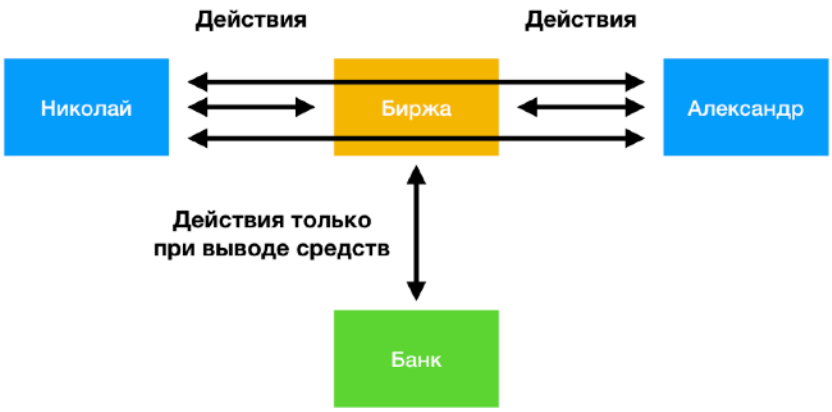


И всё бы хорошо, всё чудесно, но…

Те люди, которые взаимодействуют с криптовалютой сейчас, часто используют различные инструменты помимо обычных кошельков, ведь обычные кошельки предполагают полную синхронизацию, а так-то выкачивать и хранить терабайт данных такое себе удовольствие. В итоге люди выбирают легкие кошельки... или даже веб-кошельки, где нужно лишь ввести свой ключ или использовать плагин к браузеру и вуаля - всё работает, из любой точки мира, не хуже чем обычный кошелёк. Правда никаких технических гарантий... потому что гарантии находятся в другой плоскости. И тем не менее - это классический кейс использования криптовалют и прочих продуктов.

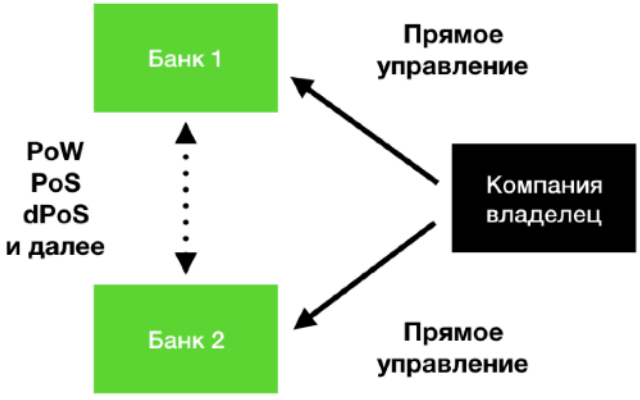


Есть люди, которые ни разу не держали на своих счетах криптовалюты, но вполне являются участниками экосистемы. Например трейдеры и некоторые инвесторы. Можно по разному относится к их деятельности, но так или иначе обыденность когда люди получают криптовалюту сразу на счёт биржи, отправляют средства на другие биржи, но, в конечном итоге, выводят деньги тоже через биржи, сразу в фиат или через обменники также в фиат - рубли, доллары или юани - уже не суть важно, но, участвуя в этой экосистеме, никак не касаются консенсуса.

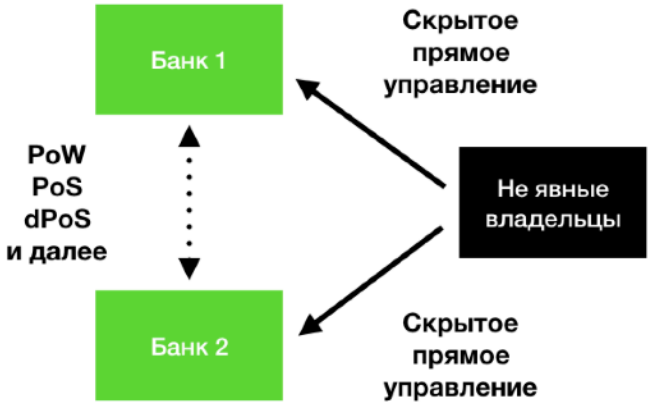


Обменники, которых достаточно много - нет никакого консенсуса что гарантирует тебе что когда ты перечислишь на счёт биткоины - тебе на карточку придут рубли. И вот ты программист криптостартапа или фрилансер, выводишь свои кровно заработанные биткоины или ещё какие-либо монетки или токены - и ты, скорее всего, получишь свои заработанные деньги, но по совсем другой причине, без консенсуса. Недвижимость за крипту, на смарт-контрактах. Или ещё что-либо из реального мира что записано в виртуальном. Никто и никогда не гарантирует вам исполнения обязательств в смарт-контракте, да ещё и по всей планете, что бы там ни было записано. Однако, как ни странно, оно может работать - только вот совсем по другим причинам и консенсус тут ни причём. Ну и конечно акции компаний - никакие гаранты не уберегли тех кто вкладывался в скам-ICO в 2017 году, кто-то ведь и машины и квартиры и бизнесы продавал ради токенов. И токены и правда остались на счету вкладчиков, консенсус помог. Но это ни в каком виде не уберегло их от потерь, от, по сути, украденных средств, это не принесло ожидаемых прибылей. Токены всё ещё на их счетах, а вот ценность - уже нет.

А как на счёт больших криптокомпаний? Интересный пример с проектом Ethereum, который сделал большой смарт-контракт по имени DAO, который собрал кучу средств... и который был ограблен хакером, потому что контракт не предусматривал некоторых нюансов, что позволило увести средства, и всё - по правилам системы. И... блокчейн просто форкнули, откатили изменения... в неизменяемом децентрализованном блокчейне... централизованным решением компании. Когда очень надо - любые правила вдруг отменяются, да и кто пойдёт против решения центральной компании, развивающей проект, верно? Кое-кто конечно пошёл, образовался форк Classic, который даже всё ещё жив, но на пару порядков слабже и почти никому не нужен, влияния за ним нет, ценности тоже, цена токенов на порядки ниже.



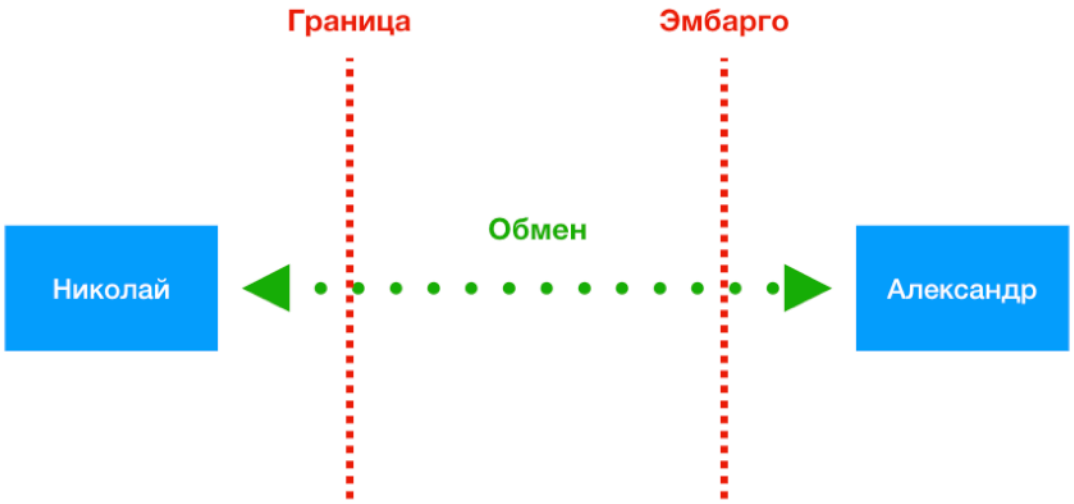
Ну и конечно даже если правила не меняются - всегда есть нюансы. В dPoS консенсусе всё стремится к олигополии, перетекающей в монопольную или близкую к такой власть, придумываются из воздуха делегаты, полностью подконтрольные кому нужно и проект рулится как нужно. В PoS достаточно купить на разные счета нужное количество монет, никто не знает что хозяин то один, а с PoW конечно сложно майнить всё самому, но если ты владелец пула и твои клиенты майнят по кусочкам за тебя - ты спокойно можешь делать нужные тебе дела от их имени и править системой как нужно именно тебе.



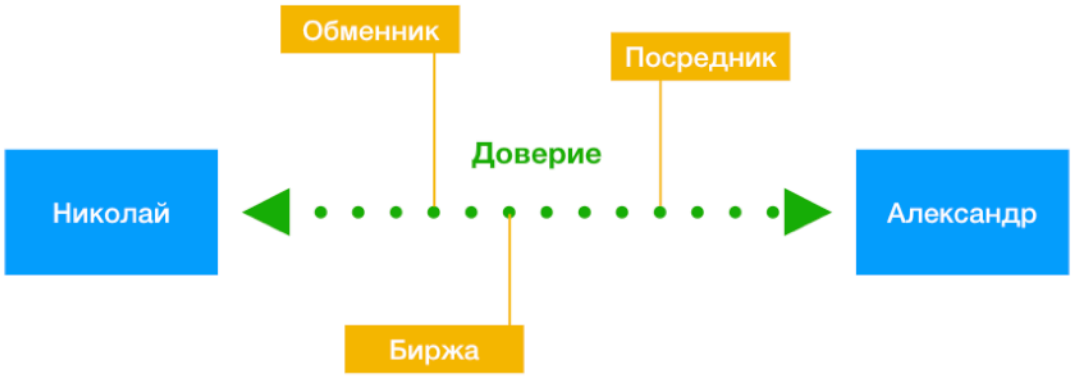
Есть конечно против этого всего веский аргумент, последняя линия обороны на случай если какая-либо из криптовалют или криптопроектов начинают контролироваться кем-либо в одного или в картеле. Дело в том что если ты владеешь блокчейном... тебе не выгодно обманывать. Ведь ты столько сил потратил на пути к вершине что брать и просто рушить систему, которая, обычно, приносит тебе токены через майнинг/стейкинг/делегатство... нет, тебе выгоднее продолжать держать её работоспособной, подтачивая напильником под себя, но тем не менее не вмешиваться на прямую. Но... чем это отличается от обычной корпорации?

И всё сводится к Теории Игр - когда тебе не выгодно обманывать если ты играешь в долгую игру, а сотрудничество приносит тебе блага.

Индустрия выросла. Но отнюдь не потому что консенсусные защищённые деньги и вот это вот всё. Нет. Причина роста в расширении финансовых инструментов для обычных людей. Например краудфандинг - раньше уже были проекты, которые позволяли собирать деньги на что либо. Но никогда не было на столько удобных международных инструментов, да ещё и без требований к верификации, объяснений откуда деньги, межграничного валютного контроля и вот этого вот всего. Границы были стёрты. Аналогично с платежами за границу. Нет, за счёт волатильности и комиссий это всё равно не всегда лучший вариант, но в некоторых кейсах - очень даже. На столько что некоторые государства таким образом обходят эмбарго со стороны других стран, особо примечательна история Венесуэлы.



Но везде, по большому счёту - работает принцип авторитетности. Когда ты отправляешь деньги кому-то через криптовалюту - ты доверяешь владельцам криптовалютной системы, будь там всё ещё множество хозяев или уже один. Когда в обменнике меняешь криптовалюту на карточку ты доверяешь обменнику и его авторитету, а ни чему-либо другому и не важно как устроена криптовалюта - главное исполнение обязательств обменником. Когда ты пользуешься криптобиржей ты доверяешь ей потому что у неё есть какой-никакой, но авторитет для тебя и ты пользуешься её услугами по её правилам. Когда ты что-либо вдруг покупаешь или продаёшь за криптовалюту - ты доверяешь человеку на той стороне и не важно как происходит процесс платежа, главное чтобы всё было в рамках условий здесь и сейчас. Чтобы не происходило, как бы оно ни работало - всё строится на доверии и авторитете. Доллар США очень авторитетен. Магазин напротив вашего дома может быть не на столько, но если вдруг там ненадлежащий товар - есть некоторая вероятность что товар можно будет вернуть, к тому же имеются законы, которые соблюдаются, в зависимости от страны, в разной степени, но если соблюдаются - то это перетекание части авторитета от государства, где оно является гарантом. Но вот в обменнике биткоинов на рубли на карточку нет никаких гарантов, кроме одного - Теории Игр, по которой вас не выгодно обманывать, особенно если обменник существует давно и комисси вполне окупают все расходы и удовлетворяют желаниям владельца. Только в этом всём консенсус совсем не нужен и на самом деле всё строится на доверии.



Сами же криптовалюты дали ещё один бонус - возможность сделать свой токен/ассет/поинт/коин/акцию в некоторое количество не сложных действий. Но можно ли предоставить возможность создавать свои ассеты чего-либо без необходимости тащить с собой консенсус, не быть частью децентрализованной (или нет) системы? Лет 10 назад это выглядело бы смешно, не доверительно... если это была бы небольшая компания. На самом деле рубли, доллары, или те же акции - те же токены по своей сути, долговые расписки, фьючерсы или что-либо иное, а должником вам выступает банк или иная организация, начиная с появления первых монет в замен физических кусков золота. Но мир поменялся, криптовалюты дали моральное право на печать своих монет, даже анонимных. И роль блокчейна тут лишь в первом шаге, в узких кейсах, но она принесла пользу. Всё остальное - построилось поверх самой Теории Игр со стратегией отсутствия выгоды в обмане, выгоды сотрудничества т.к. оно просто приносит больше выгоды, такова реальность на данный момент времени.

Продолжение следует…