Грибов Андрей Юрьевич

Председатель Совета Директоров ООО КБ «ПЛАТИНА»

Генеральный Директор ООО «КИБЕРПЛАТ»

Риск-менеджмент криптовалют

Впервые вопрос о блокчейне встал передо мной, после того, как Герман Оскарович Греф выступил в 2014 году на Давосском форуме. Меня тогда спросили, что такое биткоин, а я им никогда не занимался, и ответить мне было нечего. Даже стало досадно: как это, Герман Оскарович Греф знает, а я нет? Тем более, что мы с ним в 2010-2011 годах весьма долго говорили о технологиях (он хотел купить “Киберплат”, но мы не договорились), и объем его познаний в цифровых технологиях я представляю очень хорошо.

Я занимаюсь компьютерами с 1983 года без перерывов и глубоко нахожусь в этой теме. А он, в общем-то, гуманитарий, и его взгляд в ИТ вряд ли может быть более глубоким. Чего, например, стоит идея в своем университете обучить сотрудников Сбербанка математическому инструменту искусственного интеллекта?! Я немножко занимался искусственным интеллектом в 1988-1989 годах и отлично знаю, что для этого надо сначала изучить математический анализ, линейную алгебру, теорию вероятностей, математическую статистику, методы моделирования, методы алгоритмизации… и только потом заняться только азами искусственного интеллекта! Не всякий отличник с крепким техническим образованием такое воспримет, а гуманитарий тем более: это приблизительно как революционного матроса обучать различиям в технике живописи импрессионистов.

Тем не менее, я начал разбираться в том, что такое биткоин, и пришел к печальному выводу. Почему печальному? Большинство радостно говорит нам: «Все туда идут, все там деньги зарабатывают!» Но в отличие от большинства, я знаю,

Что такое риск-менеджмент.

Попробую вам объяснить это понятие максимально популярно, без профильных тонкостей. Возьмем, например, страховой бизнес. Как формируются страховые премии по риску угона автомобиля? Страховщики смотрят статистику угонов определенной марки автомобилей за прошлый год. Допустим, угоняли 3% машин... Они предлагают ставку 4% и знают, что если застрахуют 100 машин, то три автомобиля угонят, а премия по четвертому останется им, и они все равно заработают себе на автомобиль. В этом и состоит оценка риска - знать величину риска максимально точно. А если после получения хороших премий еще и попробовать «уговорить» угонщиков не заниматься угонами – это уже риск-менеджмент.

В банковском бизнесе оценка риска обычно представлена в виде процентных ставок. Когда в банк приходит потенциальный заемщик, банкиры рассчитывают ему риски: страновой риск стоит столько-то, риск на правовую систему столько-то, риск на отрасль экономики, риск на собственника, риск на развитие технологий… Все это складывается в итоговую ставку по кредиту – например, 12,5% годовых. И клиенту показывают, почему именно столько, а не, например, 10% и не 15%.

Так же надо считать риски и в новых технологиях. Когда финансисты и/или айтишники профессионально «заходят» в новую область, они обязательно создают риск-менеджмент новой области: эдакую условную книгу, где оглавление - это перечень рисков, и каждая глава - это описание риска как такового, его граничные величины и методы его минимизации.

Давайте посмотрим, как подобные ситуации решались раньше. Например, для управления кредитными рисками банкиры привлекали юристов, разрабатывали длинные кредитные договоры, потом понимали, что нужно иметь какое-то обеспечение этих кредитных рисков… Кредитование в том виде, в каком есть сейчас, началось совсем не сразу! Банкам как институции всего 400-500 лет, и за эти 500 лет были придуманы такие инструменты, как юридическое сопровождение кредитных договоров, варианты обеспечения, гарантии, поручительства, залоги и т.д. и т.п

Существуют расчетные риски. Для их преодоления лицензируют предприятия, занимающиеся расчетами. Не все подряд занимаются расчетами массово, а только те, за кем Центральный Банк регулярно приглядывает. Когда придумали чеки, по ним со временем сделали целое законодательство. По аккредитивам - тоже, по счетам эскроу – тоже.

История создания риск-менеджмента кредитных и расчетных рисков показывает, что решать вопросы риск-менеджмента блокчейна, биткоина и различных криптовалют вполне возможно. А решение, как обычно, трехэтапное: перечисление рисков, описание рисков (модель угрозы), работа по нахождению методов минимизации рисков.

Где мы сейчас находимся в риск-менеджменте криптовалют

Прежде всего, пока в России, да и в мире, наблюдается *низкое понимание происхождения этой технологии и целей ее создателей*. Наталья Касперская начала немного рассказывать про американское происхождение биткойна, но большинство людей в принципе не понимает, кто и зачем это создал. Каково было техническое задание на разработку, если получился такой результат? Почему из огромного многообразия вариантов создатели выбрали именно такие технологические принципы?

Беда неграмотной оценки влияния технологии на жизнь часто состоит в максималистских оценках, проистекающих из того, что такой неграмотный оценщик даже приблизительно не представляет, о чем рассуждает. Есть одна оценка: вся наша жизнь глобально изменится, потому что пришел блокчейн. И есть другая: трогать это не надо, потому что криптовалюты - организованное мошенничество. Представляете, какой разрыв? Это даже не ситуация, когда вы заходите в темную комнату и не знаете, слон там или кошка. Это ситуация, когда вы не уверены, в комнате ли вы вообще.

В какой плоскости находятся риски криптовалют?

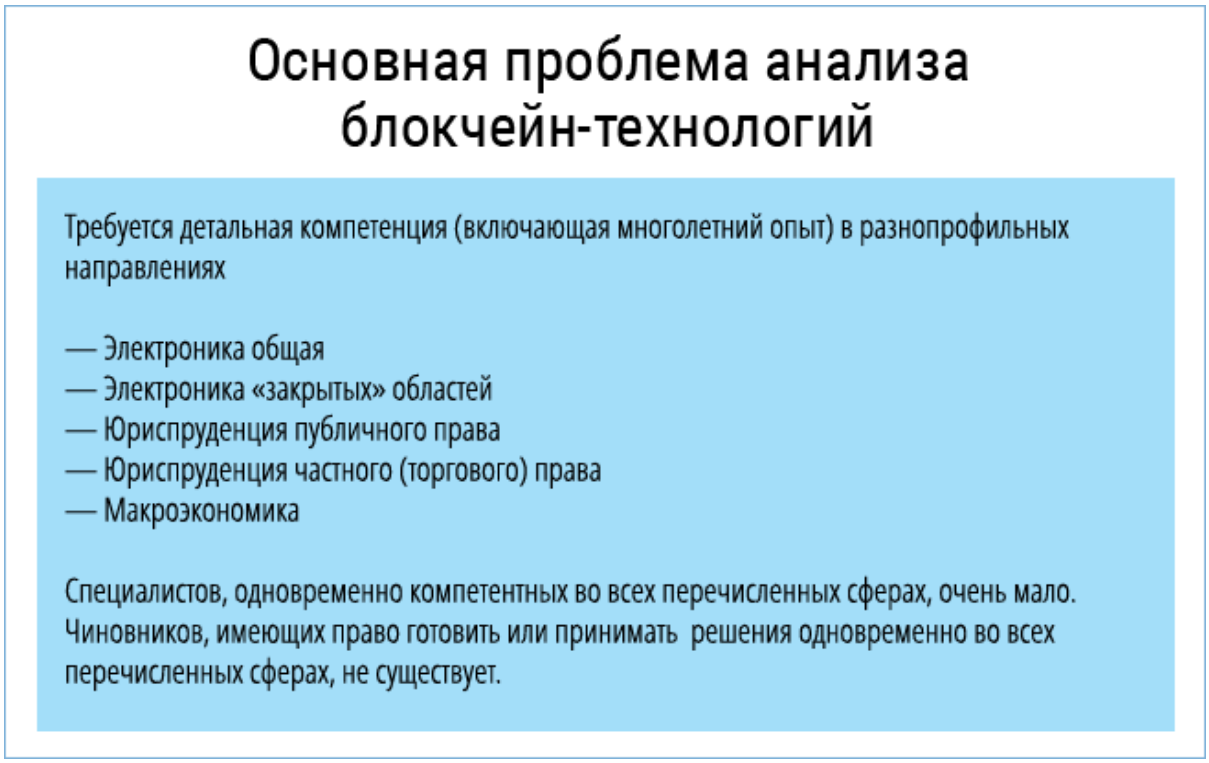
Поэтому, когда я начал изучать криптовалюты, я начал смотреть именно на перечень рисков... И обнаружил, что их не только много, а они

еще и находятся в трех больших и разных плоскостях: риски айтишные, риски экономические, риски юридические. И найти одного универсального специалиста, который разобрался бы сразу во всех этих направлениях, практически невозможно. Таких людей - десяток на страну, и вряд ли они работают чиновниками.

Поэтому, по большому счету, прежде чем заниматься криптовалютой, нужно составить список всех рисков, какие только возможны, и разделить их на профессионально-ориентированные группы рисков, где каждую разберет соответствующий специалист. Юридическую группу рисков - юрист, экономическую группу рисков - экономист и так далее. Потому что когда экономист начинает рассуждать об айтишных рисках, ничего хорошего не выходит. В этом самая главная проблема всех цифровых валют: каждый говорит о своем, и никому не пришло в голову, что нужно всем, кто хочет этим заниматься, собраться вместе, создать общество, состоящее из отделов по профилям, которое каждый риск относило бы к компетенции того или иного отдела.

Первый вывод заключается в том, что основная проблема анализ блокчейн-технологий, а правильнее было бы сказать технологий распределенного реестра, требует детальной компетенции в разных областях.

Что это за области?



Во-первых, это *общая электроника*, или понимание того, как вообще работают компьютеры. Надо понимать, почему она основана на

двоичной системе счисления (именно единичках и ноликах), а не на, условно говоря, двоечках или троечках.

Далее, очень важна *новейшая электроника, она же электроника так называемых "закрытых" областей*, прежде всего - военная электроника, в которой применяются специальные алгоритмы. Ведь сугубо мирных технологий изначально не бывает. Если человек что-то изобретает, обычно это изобретение сначала используется для того, чтобы всех соперников поубивать. Когда человечеству удалось осуществить расщепление атомного ядра, для начала убили 300 тысяч человек в Хиросиме и Нагасаки. Думаю, что и обезьяна взяла палку в первый раз не для того, чтобы фрукт сбить с дерева, а чтобы настучать по голове другой обезьяне.

То же самое в электронике - все, что мы видим в мирной области, будьте уверены, сначала использовалось в военной. Например, сотовая связь - это полевая опорная сеть связи, разработанная еще в середине XX века для военного применения. Часть этой технологии рассекретили, и она стала доступна обычным абонентам. Интернет изначально назывался ARPANET и связывал между собой несколько сотен военных учреждений и предприятий в США. Его рассекретили, передали в открытое пользование – теперь мы шлем друг другу электронные письма, смотрим новостные и прочие сайты.

Итак, для анализа технологий распределенного реестра нужны как минимум базовые знания в электронике двух видов.

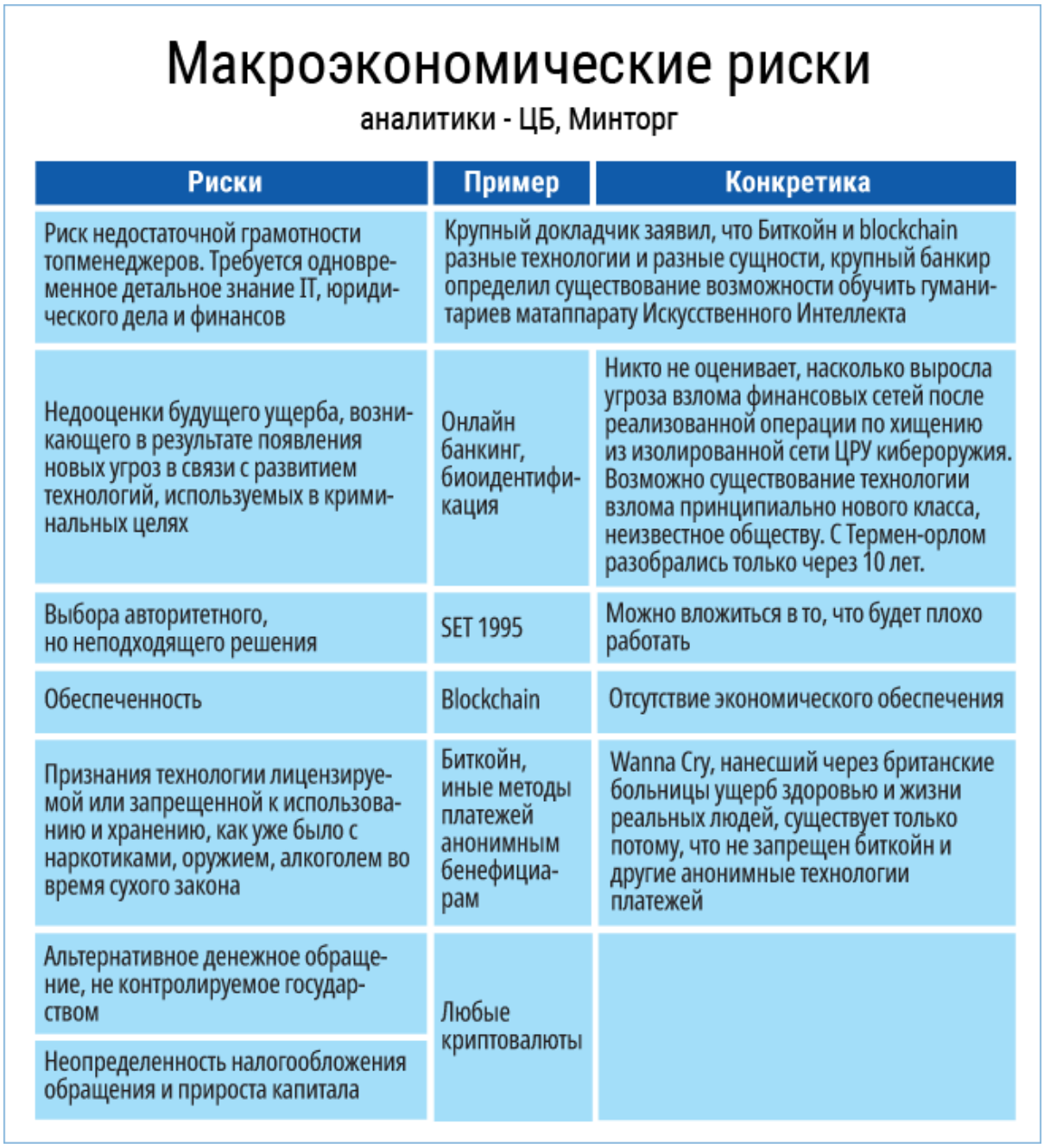
Далее - *юриспруденция*. Юриспруденцию нужно знать: и публичного права – каким образом криптовалюты, деньги, расчеты регулируются государством, и частного (торгового) права, то есть как два равноправных лица (юридических или физических) могут ими обмениваться.

И, конечно же, знать *макроэкономику*.

Попробуйте представить, как много найдется людей, которые знали бы достаточно хорошо все эти отрасли? Лично мне, к счастью, повезло, у меня есть как раз эти три образования: электронное (Московский институт электронного машиностроения), финансовое (Финансовая Академия [1]) и юридическое (юрфак МГУ).

И верхнеуровневая проблема даже не в том, чтобы найти многопрофильных универсальных специалистов. Проблема в том, чтобы найти таких универсальных чиновников, потому что ведь именно они должны регулировать процессы на государственном уровне, в области публичного права, но в макроэкономических интересах, и опираясь на знания в области электроники.

Разберем сначала макроэкономические риски.



Макроэкономические риски

аналитики - ЦБ, Минторг

Риски	Пример	Конкретика
Риск недостаточной грамотности топменеджеров. Требуется одновременное детальное знание IT, юридического дела и финансов	Крупный докладчик заявил, что Биткойн и blockchain разные технологии и разные сущности, крупный банкир определил существование возможности обучить гуманитариев матаппарату Искусственного Интеллекта	
Недооценки будущего ущерба, возникающего в результате появления новых угроз в связи с развитием технологий, используемых в криминальных целях	Онлайн банкинг, биоидентификация	Никто не оценивает, насколько выросла угроза взлома финансовых сетей после реализованной операции по хищению из изолированной сети ЦРУ кибероружия. Возможно существование технологии взлома принципиально нового класса, неизвестное обществу. С Термен-орлом разобрались только через 10 лет.
Выбора авторитетного, но неподходящего решения	SET 1995	Можно вложиться в то, что будет плохо работать
Обеспеченность	Blockchain	Отсутствие экономического обеспечения
Признания технологии лицензируемой или запрещенной к использованию и хранению, как уже было с наркотиками, оружием, алкоголем во время сухого закона	Биткойн, иные методы платежей анонимным бенефициарам	Wanna Cry, нанесший через британские больницы ущерб здоровью и жизни реальных людей, существует только потому, что не запрещен биткойн и другие анонимные технологии платежей
Альтернативное денежное обращение, не контролируемое государством	Любые криптовалюты	
Неопределенность налогообложения обращения и прироста капитала		

Первый риск - это *риск недостаточной грамотности топ-менеджеров*. Пример. На одной из профильных конференций выступил докладчик, занимающий весьма ответственную должность, который заявил, что блокчейн и биткоин - это совершенно разные вещи, к которым надо по-разному подходить. А вообще-то биткоин создан на технологии блокчейн. И ведь что интересно, никто не возразил, не возмутился, никто не зашикал…

Другой риск - *недооценка будущего ущерба, возникающего в результате появления новых угроз в связи с развитием технологий, используемых в криминальных целях*. То, насколько мы не понимаем будущие риски, можно проиллюстрировать таким примером. Лет пять назад все громко кричали: “Система «банк-клиент» изменит жизнь, люди из дома по сотовому телефону будут высылать в банк платежки, и все будет хорошо”. И никто не предупредил, что одновременно возникнут хакеры, которые будут взламывать счета, заходить туда вместо клиента, делать куда-то переводы. Это описывает Нассим Николас Талеб в книге “Антихрупкость”: “люди всегда говорят про высоту гор, исходя из знания той самой высокой горы, которую они видели. Но это не значит, что они не найдут гору еще выше.» Никто не оценивает грамотно и квалифицированно вероятность риска того, что эти криптовалюты, не дай Бог, украдут. Недавно мне попалась информация о том, что 10% денег, собранных при ICO, украдены хакерами. И это еще только начало. Процент похищенных средств будет расти, потому что хакеры быстро совершенствуются.

Другой пример. США - высокоразвитая страна, которая создает кибернетическое оружие для защиты своих интересов. И, чтобы заниматься этим оружием, ЦРУ разработало отдельную сверхсекретную сеть, физически не соединенную с остальным интернетом. И у них из этой сети это оружие украли! Возникает резонный вопрос: если хакеры смогли взломать изолированную сверхсекретную сеть ЦРУ в высокотехнологических США, неужели они не смогут взломать Центробанк? А ведь у криптовалют даже единого реестродержателя нет!

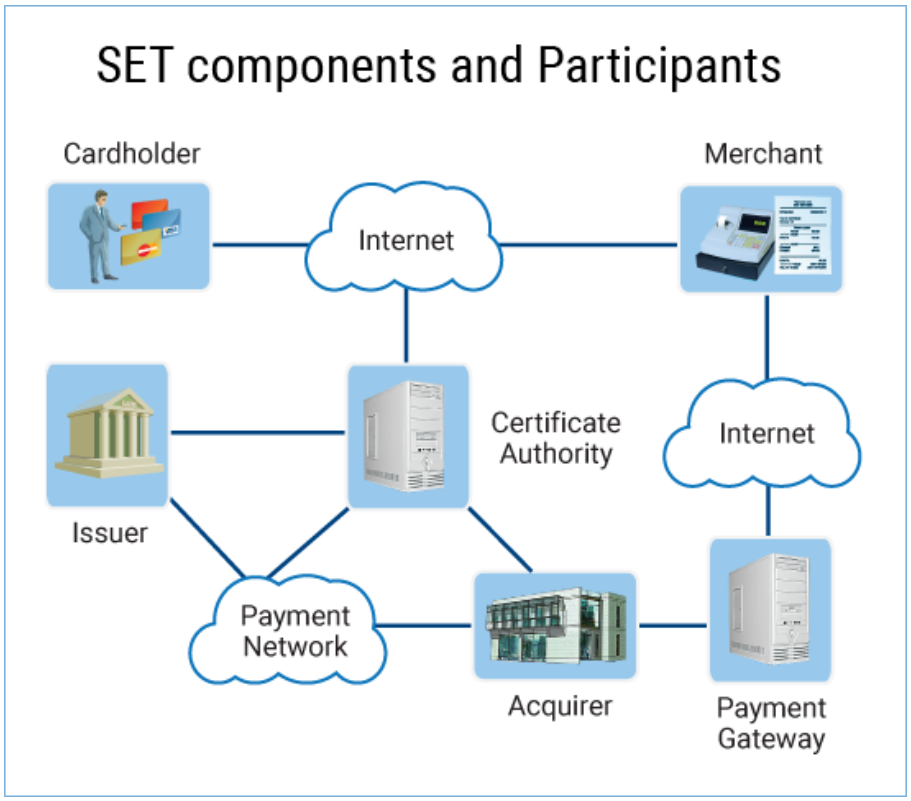
Есть очень показательная история о том, к чему приводит недооценка рисков технологий, про которые пока никто не знает. Российский изобретатель Лев Термен изобрел в свое время подслушивающую систему “Златоуст”, которая потом 10 лет работала на Россию против американцев [2] .


Поехал как то американский посол в Артек, посмотреть на пионеров, и те подарили ему вырезанного из дерева орла. «Красивый орел, - подумал посол. - повешу у себя в кабинете, это же символ Америки. И потом, он абсолютно деревянный, никаких проводочков из него не торчит,

электрическое питание не подведено, - там не может быть подслушивающих устройств!». Так орел 10 лет провисел у него в кабинете. И когда уже точно знали, что где-то у него в кабинете есть подслушивающее устройство, и разобрали всё по деталям, все-таки решили и этого орла посмотреть. Его разобрали и нашли некие проволочки. И оказалось, что если этого орла направленно облучать определенной радиочастотой, то проволочки выступают голосовым модулятором, которые берут звук и накладывают на эту частоту. А в другом месте эту модулированную частоту снимают с эфира и слышат, что говорится в кабинете.

Эта технология не была никому известна первые десять лет своего существования и использования. А вы представляете, сколько сейчас технологий, о которых мы не знаем, а они есть, и они работают! Хорошо, если их когда-то вскроют и разрешат ими пользоваться. Вот, например, вы думаете, что купили мобильный телефон, и он ваш. А Наталья Касперская, говорит совершенно открыто [3]: “Смартфон - уже не ваше устройство. Вам его дают, чтобы вы побаловаться могли. А на самом деле это устройство совершенно других людей, которым мы передаем большой и теплый привет”. Соответственно, мы совершенно не понимаем риски новых секретных технологий, именно в силу их секретности, а нам говорят - берите и пользуйтесь вовсю. А не прошло не только 10 лет, вообще почти нисколько не прошло.

Следующий макроэкономический риск - это *риск выбора авторитетного, но неподходящего решения*.

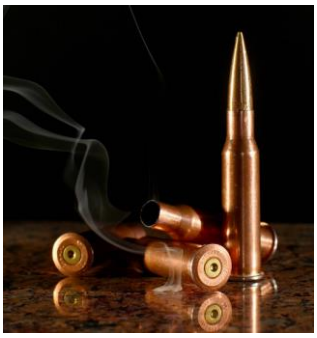


В 1996 году собрались монстры экономики - Microsoft, IBM, Visa, Mastercard и решили разработать единое для всех решение по электронным платежам. Разработали, называлось оно SET (Secure Electronic Transaction). Visa сказала: отлично, будем жить с этим решением. А грамотные люди, которые разбирались в ИТ, сразу поняли, что оно очень тяжелое, неудобное, и никто, условно говоря, не будет ездить в булочную на БЕЛАЗе. А те, кто не разбирались в ИТ (и в тот момент это был, в частности, Альфа-Банк), взяли и купили решение SET за сумму около миллиона долларов [4]. Но уже через год поняли, что на БЕЛАЗе действительно неудобно ездить в булочную, да и Visa вдруг вышла из этой ассоциации, и IBM сказала - извините, мы ошиблись…

Получилась ситуация, когда все выбрали, кто-то один вложился, а потом остальные дружно сказали - ой, это будет не так. Альфа-Банк после этого долго ругался с Visa. Кончилось все тем, что их в утешение взяли в какой-то наблюдательный совет.

Что в этой истории важно - выбрать неправильное решение могут и самые опытные люди. И кто нам доказал, что именно биткоин - правильное решение, если сейчас на рынке уже несколько тысяч криптовалют? И биткоин даже контрольный пакет уже не держит среди них!

Все это - макроэкономические риски, оценивать которые должен кто? Центробанк, Минэкономразвития, Минпромторг и иные государственные органы.



Еще один макроэкономический риск - *признание технологии лицензируемой или запрещенной к использованию и хранению*, как уже было с наркотиками, оружием, алкоголем во время сухого закона. В свое время я задался вопросом, какая валюта самая лучшая. Набрал в «Яндексе» запрос “самая лучшая валюта”... и знаете, что он мне выдал? Первой же ссылкой? «Самая лучшая валюта - это патроны. Один патрон - одна жизнь».

В ряде мест, где идет война, так и есть. И наши спецназовцы, кто в Чечне воевал, тоже это понимают. Там, где закона нет, оружие - лучшая валюта. Но как только появляется закон – свободное обращение оружия запрещают. Есть список вещей, запрещенных в цивилизованном мире к свободному обращению: наркотики, оружие, ракеты, определенные химические вещества… Бывает так, что долгое время что-то было легальным, а потом вдруг становится нелегальным. Достаточно

вспомнить историю компании Bayer: она начинала с легального производства и продажи кокаина. Были даже кокаиновые капли в нос - народный комиссар здравоохранения Николай Семашко прописывал их членам Совнаркома. Bayer процветал, а потом кокаин запретили к легальной продаже. Тогда они начали производить героин [5], пока его тоже не запретили.

В такой сфере, как обращение денег, на которую государство смотрит очень внимательно, ситуация, когда что-то из легального может стать нелегальным, крайне вероятна. Очевидно, что криптовалюта в каких-то странах будет признана легальной, а в каких-то нет. В каких-то странах её уже запретили. И даже если у нас пока может существовать целый Telegram-канал, где висят объявления о продаже квартир, машин и даже титановых месторождений за биткоины и иные криптовалюты, то остается открытым вопрос юридического оформления такой сделки. Как признать, что сделка состоялась, что деньги перешли от покупателя к продавцу? И начинаются чисто юридические риски - признание сделки незаконной, нелегальной, несостоявшейся, или еще хуже - притворной.

Не так давно по миру прокатился вирус-шифратор WannaCry, который привел к реальным человеческим жертвам, потому что он в том числе зашифровал компьютеры, отвечавшие за жизнеобеспечение людей в британских клиниках. А откуда он взялся? Первые дешифраторы работали на отмене этого шифра при условии оплаты через SMS. И когда этот канал оплаты вымогателям перекрыли, хакеры перестали их рассылать эти вирусы, перестали использовать этот инструмент. Можно сказать, что WannaCry основан на существовании анонимных криптовалют: если бы не было биткоина, не было бы экономического смысла запускать вирус-шифратор. Поэтому если человечество захочет защититься от вирусов-шифраторов, то придется отменить анонимные криптовалюты. Ведь сколько можно заразить электроники этими вирусами-дешифраторами, начиная от смартфонов и заканчивая системой вентиляции! И если, не дай Бог, кто-то будет пугать весь мир такими вирусами, вопрос о запрете криптовалют встанет моментально. А принимают эти решения люди, которым выгодно принять политически выгодное популистское решение.

Еще один макроэкономический риск - *альтернативное денежное обращение, не контролируемое государством*. Об этом уже говорила и Председатель Центрального банка РФ Эльвира Набиуллина, и замминистра финансов Алексей Моисеев: ни одно нормальное

государство не допустит на своей территории обращения валюты, которое оно не контролирует. До каких-то пределов на это не обращают внимания, но, как только объемы обращения вырастут - ситуация изменится.

Неопределенность налогообложения обращения криптовалют и прироста капитала. Буквально завтра государство может ввести любые налоги на криптовалюту, и такой риск тоже нужно предусмотреть.

Криминальные риски.

Криминальные риски

аналитики - МВД, ФСБ, Росфинмониторинг, ЦБ

Риски	Пример	Конкретика
Использования для неисполнения законодательства по ПОД/ФТ	Любые криптовалюты	Нет единого эмиссионного центра, не идентифицированы плательщик и бенефициар
Антигосударственной социальной инженерии	Любые криптовалюты	Оплата цветных революций
Использование несоответствия текущему законодательству в мошеннических целях	Blockchain	Смарт-контракты не соответствуют понятию АСП в ГК РФ
Воровства или публичности коммерчески значимой информации и коммерческой тайны или персональных данных	Blockchain	По определению вся информация о всех сделках и сторонах известна
Хищения	С бирж были украдены криптовалюты на сотни миллионов	Необходимы гарантии правоохранительных органов сохранности средств, а также ЦБ, ответственного за денежное обращение в стране
При этом мы не сможем обеспечить абсолютную надежность транзакций в силу того что если по какой-то причине 50% + 1 валидатор криптовалюты скажут, что транзакция была, а на самом деле ее не было, у нас не будет никакой возможности это опровергнуть", - пояснил Моисеев.		

Таких рисков немало.

Любая криптовалюта находится под риском *использования для неисполнения законодательства по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ)*.

Еще один риск - *антигосударственная социальная инженерия*. Что это такое? Допустим, люди получают анонимный email, призывающий: «Приди на Болотную площадь в такое-то время, получишь 1/10 биткоина». Сколько людей придет? Можно собрать очень большую толпу. И представим себе - эти люди пришли и получают новое сообщение: «А теперь перейдите через мостик и дойдите до Красной площади». Или до Манежной. Любой, у кого в руках есть эта технология, может манипулировать большим количеством жадных и глупых людей дистанционно.

Третий риск - *использование несоответствия текущему законодательству в мошеннических целях*. Например, смарт-контракты, на которых все основано, в Гражданском кодексе вообще не описаны. Электронная цифровая подпись описана, она там называется АСП. А что такое смарт-контракты, с юридической точки зрения не знает никто, и если прийти с этим в суд, у суда нет никакой законодательной базы, а тем более практики, по которой надо принимать судебное решение. Вы обменялись криптовалютами, да, но судебной поддержки этого решения нет по определению. Чему равен этот риск? Надо оценивать, взвешивать его. Потому что правила игры могут изобрести такие, что ваши вложения в криптовалюту обесценятся мгновенно.

Еще один риск: *воровство или публичность коммерчески значимой информации и коммерческой тайны или персональных данных*. Здесь кроется беда всей технологии блокчейн. Все знают про все сделки сразу. Вы знаете персональные данные всех. Это напрямую противоречит закону «О персональных данных».

Риск хищения мы выше несколько обсудили - те самые 10%. Пока. Как сказал господин Моисеев: «Мы не можем обеспечить абсолютную надежность транзакций в силу того, что если по какой-то причине 50% + 1 валидаторов криптовалюты скажут, что транзакция была, а на самом деле ее не было, у нас не будет никакой возможности это опровергнуть». А если эти валидаторы еще и анонимны, то риск возрастает существенно.

Риск нахождения запрещенной информации в сети криптовалюты. Любой валидатор криптовалюты является хранителем всего архива данных сразу. Поскольку подавляющее число валидаторов не является профессионалами в области создания и контроля криптографического ПО, то они не могут даже понимать, что внутри архива может находиться что-либо постороннее. При этом Исследователи из университетов Аахена и Франкфурта обнаружили, что в сети биткоина помимо финансовой информации хранится около 1 600 других файлов. Среди обнаруженных файлов семь нарушают авторские права: в них содержатся отрывки из разных whitepapers, приватный

ключ RSA, секретный ключ ПО и ключ к взлому защиты от копирования DVD. Также блокчейн биткоина хранит свадебные фотографии и снимок людей с указанием их онлайн-псевдонимов. Среди файлов обнаружены копии дипломатических телеграмм США, утечка которых произошла через WikiLeaks в 2010 году, и новость о демонстрации в Гонконге в 2014 году, некоторые файлы в блокчейне биткоина содержат противозаконную информацию и 274 ссылки на подобные ресурсы, 142 из которых ведут на сервисы в Dark web [6].

Из существования данного факта вытекают весьма несложные выводы:

- Существует неизвестный широкой публике метод помещения в архив посторонних файлов.
- Таким образом в архив можно поместить (если они там уже не находятся) вирусы и иное зловредное программное обеспечение.
- А если существует неизвестный широкой публике метод помещения в архив посторонних файлов, то логично предположить, что существует и неизвестный широкой публике метод считывания из архива этих посторонних файлов, в том числе вирусов и зловредного программного обеспечения.
- Также логично предположить, что существует и неизвестный широкой публике метод самораспаковывания и самоустановки таких посторонних вирусов и зловредного программного обеспечения на компьютер пользователя, эксплуатирующие скрытые возможности ПО майнинга криптовалюты или их операционных систем.

Риск контейнерности криптовалюты. Таким образом, архив криптовалюты является криптоконтейнером. Получив его, пользователь может знать лишь информацию, написанную на «стенке контейнера», его название и видимое для широких слоев содержимое. В некоторых типах блокчейнов знать, что еще находится внутри архива - криптовалютного криптоконтейнера, пользователь не может именно в силу зашифрованности (если понимать под зашифрованностью криптопреобразование), а также в силу того, что не знает алгоритма поиска и идентификации «добавленной» информации (не знает что и где искать), то есть стеганографии. А внутри может находиться все что угодно: инструкции по терроризму или совершенно секретная информация. Или вредоносный код.

Например, в публичный блокчейн может писать неограниченный круг лиц, контроль доступа не производится и нет совершенно никаких шансов, что валидатору не поступит какая-либо запрещенная информация или вирус. И нет никаких сертифицированных или хотя бы доверенных средств, чтобы проверить, что именно находится в архиве-

криптоконтейнере. Кроме того, многие криптовалюты предоставляют разработчикам открытый API для разработки своих токенов на основе «основной валюты». У разработчиков имеются все возможности добавлять в криптоконтейнер нелегальный контент и его вряд ли кто-нибудь контролирует, помимо самих разработчиков.

Был ли в истории прецедент реализации рисков в «непроверенном контейнере»? Да, был. В XIII веке хан Хубилай запустил относительно «скоростные» караваны по «Шелковому пути». Кто возражал тогда против этой новой, явно революционной технологии доставки грузов? Все были «за» и очень рады. Просто никто тогда не понимал, что вирус чумы, являющийся природным в Монголии, не стал успевать убивать караваны в пустыне Гоби, и эти самые караваны за счет увеличения скорости стали разносчиками чумы в Европе и Китае. Цена реализации риска тогда составила смерть половины населения Европы и двух третей населения Китая.

Какая «зараза» сейчас может находиться в этих криптовалютных криптоконтейнерах, мы не знаем. Очень несложно поместить туда зловредное ПО, похищающее информацию или инфицирующее критическую информационную инфраструктуру. Какова величина остановки критической инфраструктуры, мы сейчас понимаем?

Технологические риски.

Технологические риски

аналитики - Крупнейшие существующие интеграторы с большим опытом внедрения, производители банковского софта, Минсвязь

Риски	Пример	Конкретика
Непредназначенности для данного использования	Blockchain	Технология распределенных реестров необходима для АСУ войсками
Несоответствия поставленным задачам (излишняя публичность, низкая скорость)	Blockchain	Все видят все транзакции, скорость – 3 (максимум 5) транзакции в секунду существенно увеличена быть не может
Непрозрачного создания	Биткойн	Автора никто никогда не видел, неясен источник финансирования в 20 млн. долл
Первоначального использования технологии	Биткойн	Родился внутри Tor'a, тесно связанным с ФБР (http://www.cnews.ru/news/top/anonimnaya_set_tor_na_60_finansiruetsya), в магазине Silk Road, называемым Amazon или Ebay для нелегальных товаров

Откуда взялась технология блокчейн? Никто об этом не говорит. А ведь технология распределенного реестра известна не последние лет пять, которые о ней говорят, а лет 35-40. И использовалась она обычно для автоматизированных систем управления войсками, прежде всего для обмена тактической информацией. Представьте себе, что у вас 50 боевых юнитов, которые ведут боевые действия. И какой-то юнит - например, вертолет, который поднялся в воздух, что-то важное увидел, получил информацию. Эту информацию надо передать всем юнитам подразделения и командованию, чтобы каждый из них имел полную картину боя. Либо напрямую, либо по цепочке. Транзакция считается законченной, только когда эта информация доехала до каждого разрешенного абонента. Не с того момента, когда каждый узнал, а именно когда дал отклик, что получил. Если у вас 50 абонентов, передача данных происходит достаточно быстро. Но как только их становится тысяча, начинаются проблемы… До этого не дозвонился, с этим связь потеряна… А блокчейн изначально рассчитан на многие тысячи узлов валидации. Поэтому быстродействие этой технологии составляет максимум 7 транзакций в секунду. Что это значит в сравнении? У нас в «Киберплате» штатная «скорострельность» 100 транзакций в секунду, пиковая - 500. В Сбербанке, предположу, штатная где-то 400, пиковая - 1500 транзакций в секунду. Это сколько нужно блокчейнов? Когда Герман Греф говорит о пользе блокчейна, я сразу начинаю прикидывать - сколько же ему их понадобится?

Риск несоответствия поставленным задачам. Что такое 7 транзакций в секунду? Это около 220 миллионов транзакций в год. А у нас население 140 миллионов! Это значит, что каждый из нас может сделать меньше ДВУХ транзакций в год! А если надо три, то третью надо еще год ждать. Если же вам нужно, к примеру, 300 транзакций, то извините, вы не доживете до их выполнения. Поэтому внедрение такой технологии в больших сообществах в принципе невозможно. А большие сообщества как раз и обслуживают банкиры, им это интересно. Когда компанией IBM была собрана первая серийная сотня компьютеров, один купил Пентагон, один – метеорологи, а остальные 98 - банки.

Был кейс один, когда группа разработчиков, услышав, что быстродействие 7 транзакций в секунду - это несерьезно, собрала в одной комнате тысячу компьютеров, соединила их оптикой и добилась 200-300 транзакций в секунду. Но распределенность реестра, если весь этот реестр находится в одной комнате, становится никакой. Потому что если ты хочешь распределить по земному шару этот реестр, то надо пользоваться всей системой связи: медь, воздух, и так далее. А на распределенной, по-настоящему распределенной, сети такой производительности быть не может. Для военных 7 транзакций в секунду приемлемы. А банкиров такое быстродействие не будет

устраивать. Эта технология изначально делалась не под это и не подходит под нынешнюю форму финансового рынка.

Потихоньку подходим к главному. *Риск непрозрачного создания*. Кто писал техзадание на создание этого софтвера? Кто принимал в работу? Кто писал структурный алгоритм? Кто принимал в эксплуатацию код? Кто проводил отладку?

Фото: Хакер.ru

Наталья Касперская первая публично заявила об этом, что нет никакого Сатоши Накамото, а за блокчейном стоит группа американских криптологов. Мы уже знаем, что технология распределенного реестра изначально использовалась в АСУ войсками довольно давно, и именно поэтому про нее ничего не писали в научных и научно-популярных журналах. А теперь мы узнаем, что кто-то где-то эту технологию уже использует. И явно он в ней разбирался в ней раньше. А в каком месте есть люди, которые разбираются в таких вещах? Очевидно, что это - Пентагон.

Теперь давайте вспомним, где впервые был использован биткоин? Есть такая анонимная сеть Tor, и в ней был онлайн-магазин Silk Road, который торговал наркотиками. Сеть Tor существует на анонимные пожертвования, но как ни странно, известно, кто является главным донором. Это Федеральное бюро расследований США. И понятно, что взломать эту сеть нельзя, потому что нужно взломать пять серверов подряд… Если, конечно, все эти пять серверов не твои. А если они твои, все пять, ты читаешь всю эту переписку и принимаешь решения: вот этих мы посадим - обеспечим статистику, этих мы не сажаем, а смотрим, кто на них клюнет, этих не сажаем - они нам платят. Злые люди говорят, что так и была создана сеть Tor - определенными людьми для определенных людей.

А про Интернет-магазин Silk Road злые языки говорят, что когда ФБР ловит кого-то с наркотиками, оно что-то там сдает государству, а остальное, конфискат, продает налево, а где самый удобный магазин, где продать конфискат налево? Очень удобный инструмент для этого - Интернет-магазин. Если еще знать, что в США все сотрудники ФБР официально освобождены от ответственности за операции с наркотиками под предлогом «им приходится это делать, чтобы в ОПГ внедряться», то картинка вообще становится законченной. Сразу становится ясно, кто и как контролирует данный рынок. Но, сделав несколько оборотов “наркотики/оружие - биткоин”, эти люди начали сбрасывать криптовалюту или менять ее на квартиры, машины,

титановые месторождения и так далее. А поскольку у этих людей есть в арсенале множество журналистов, раздуть историю вокруг всего этого не стоило никакого труда.

Прямым следствием всего вышеперечисленного является *Риск нечаянной утраты*.

Доступ к кошельку с криптовалютой может быть утерян в результате потери пароля, сбоя на носителе данных, потере самого носителя данных.

Из-за принципа функционирования криптовалют и лежащей в его основе технологии блокчейна пароли пользователей нигде не сохраняются, кроме их памяти или личных записей. Нет соответствующего бизнес-процесса, при помощи которого можно в личном присутствии заменить пароли, удостоверить личность владельца и вернуть права на эти криптовалюты или иные криптоактивы.

Как сообщает New York Times, около 20% от существующих в мире 18,5 млн биткоинов находится на кошельках, которые были по какой-то причине заблокированы, либо чьи пароли были безвозвратно утеряны. Общая стоимость валюты, которой нельзя воспользоваться, оценивается в $140 млрд.[7]

Подводя итоги. Перед тем, как куда то войти, давайте подумаем - а как выходить будем? И если окажется, что это было отмывание в особо крупных размерах, то по сути вы оказываетесь соучастником отмывания операций с наркотиками и оружием.

Что надо делать.

Надо заняться менеджированием рисков. Описывается риск, описывается его максимальная величина, формируется так называемая стратегия угроз, описывается величина этой угрозы, и каким образом ей надо противодействовать.

Как известно, наиболее эффективными борцами с террористами являются сами террористы - те, которые контртеррористы. Они знают, каким образом осуществлять теракт, и легко догадываются, каким образом их можно нейтрализовывать. Любой хороший изготовитель брони прекрасно знает, как устроен снаряд, иначе он не сделает броню. Почему, когда бандиты навязывают свою крышу, они называют это страховкой? Потому что это все единое целое.

Не так давно появилась теория государства как стационарного бандита, за нее чуть ли не Нобелевскую премию дали экономисту, который ее написал. Формулируя всю теорию в одной фразе - “у кого самая большая дубинка, тот и главный на этой территории”. В случае с криптовалютами - то же самое. Чтобы заниматься макроэкономикой, нужно идти к крупнейшим жуликам в макроэкономике - в Центробанк, в Правительство. Чтобы заниматься криминалом, надо идти… понятно куда. Только тогда, когда им станет это выгодно и интересно, они начнут управлять этим процессом.

Мое глубочайшее убеждение, что настоящая Америка - та, которую мы знаем - началась с созданием в 1920-х годах Murder Incorporated. Когда крупнейшие мафиозные кланы собрались и решили, что убивать человека можно только с разрешения руководителей всех мафиозных кланов одновременно. Тогда кончился беспредел, и они своим внутренним судом приговаривали, кого можно убить, а кого нет. С этого момента страна стала цивилизованной. До этого ковбои стреляли по шерифам, а шерифы по ковбоям, и они друг от друга отличались только наличием или отсутствием значка. Но с того момента, когда в нелегальном пространстве появилось свое судопроизводство, с того момента началась цивилизация в США. Любой риск должен рассматриваться профессиональными риск-менеджерами. А вот кто они… Писать не будем, но понимать будем.

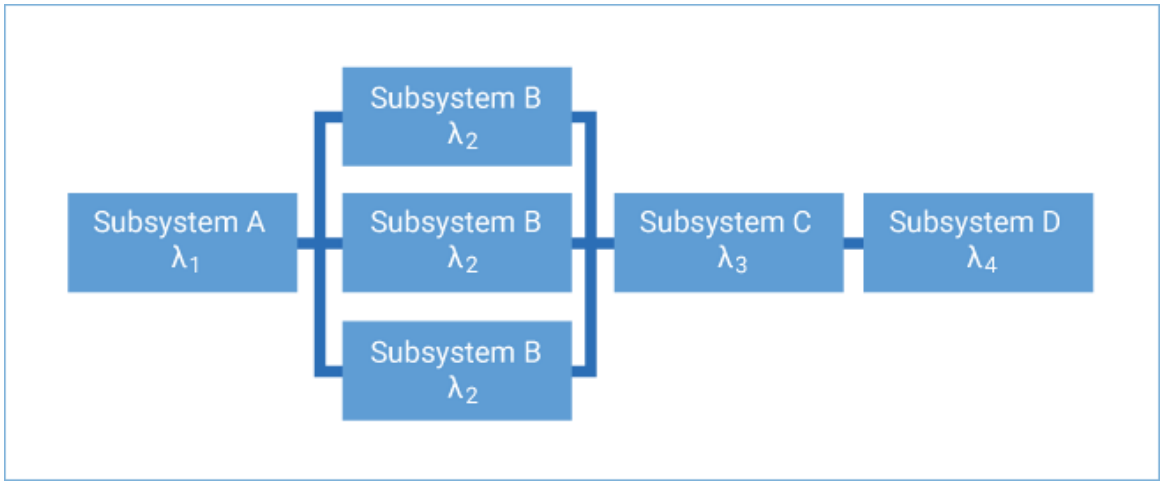
Поэтому для определения рисков криптовалют и создания риск-менеджмента криптовалют надо поделить все риски на группы, и каждую группу рисков должны изучить те, кто в этом разбирается.

- Например, IT риски стоит поручить Министерству связи и Академии Наук.
- Экономические риски – Центробанку, Минэкономразвитию, Минфину.

- Криминальные риски – Министерству юстиции, МВД, Прокуратуре, спецслужбам.

И только собрав профессиональные мнения всех групп воедино, можно принимать объединенное фундаментальное решение.

Катастрофоустойчивость и живучесть.



Теория вероятности учит нас, что двукратное дублирование информационной инфраструктуры в мирное время, например, на гражданских самолетах, или в процессинговых системах, является вполне достаточным, а трехкратное уже и несколько избыточным. Называется этот параметр – катастрофоустойчивость. А вот в боевых самолетах и АСУ войсками, например, дублирование критической информационной инфраструктуры должно составлять 4-7 раз. По той простой причине, что во время использования этого устройства в боевых целях противник предпринимает меры для уничтожения такового. Поэтому при умышленном поражении 2-3-4 уровней боевой информационной инфраструктуры самолет или система управления все равно должны выполнять свои боевые задачи. Поэтому и уровень дублирования четырех-семикратный. И называется это – живучесть. Термин этот используется при проектировании и тестировании оружия. Можно услышать словосочетания «живучесть корабля», «живучесть танка», «живучесть самолета». Но такого словосочетания для мирных систем нет. Потому что такой уровень живучести в мирное время не нужен. Не нужен для мирного пассажирского самолета семикратный уровень дублирования бортовой электроники. И для мирных процессинговых систем семикратный уровень дублирования тоже не нужен. Если, конечно, не ставить перед собой задач по финансированию терроризма, разведывательных сетей в тылу противника или

осуществления заведомо противоправных деяний типа реализации наркотиков.

В блокчейне же каждый «добытчик» - «майнер» в идеале дублирует практически всю сеть. Это какая-то супермегаживучесть. Даже при уничтожении 99% резервирования блокчейн не перестает функционировать. Но разве возможно в мирное время потерять 99% инфраструктуры резервирования? Конечно, нет. Тогда зачем все время платить за такой явно избыточный ресурс?

За мегаживучесть криптовалют приходится платить дополнительной работой процессоров всех участников, а главное – временем транзакции. **Именно явно избыточная мегаживучесть и является причиной низкой производительности и высокой ценой использования криптовалют**.

Бывший генеральный директор PayPal Уильям Х. Харрис пишет «Требуется около часа для подтверждения транзакции биткойнов, а система биткойнов ограничена пятью транзакциями в секунду. MasterCard может обрабатывать 38 000 в секунду. Перевод 100 долларов США от одного человека другому стоит около 6 долларов США с использованием криптовалют и менее 1 доллара с помощью электронного чека…… На создание одного Биткоина (процесс, называется «добыча») требуется столько же электроэнергии, сколько хватило бы средней американской семье на два года. Если бы биткойн использовался для значительной части мировой торговли (чего не произойдет), он потреблял бы очень большую часть мирового электричества, отвлекая дефицитную энергию от полезных целей.» [8]

Для мирного применения блокчейна вполне достаточно сократить число узлов верификации до 10, максимум до 20. А если передать эти функции верификации игрокам, ответственным за риск-менеджмент данной криптовалюты, то все встанет на свои места. Получим сверхнадежную по катастрофоустойчивости (и даже живучести) платежную инфраструктуру, где верификаторами являются министерства и ведомства, уполномоченные государством. Риски использования такой криптовалюты будут минимальными.

Таким образом, наиболее рациональным развитием технологии распределенного реестра для создания криптовалют является создание криптовалюты с сильно ограниченным количеством верификаторов-реестродержателей, число которых, состав и обязанности (прежде всего по снижению рисков использования) будут определены Правительством. В их число обязательно будут входить Минсвязи, Академия Наук, Центробанк, Минэкономразвития, Минфин, Минюст, МВД, Прокуратура, спецслужбы.

Все остальные пользователи будут пользоваться этим реестром и не будут держать у себя «архивы» чужих транзакций.

11.04.2018

PS

В результате размышления и обсуждения систем распределенного реестра для систем автоматического управления войсками удалось понять, что число не только узлов дублирования, а даже абонентов у них, весьма ограничено. Во-первых, подразделение, грубо говоря, воюющее в районе Мурманска не нуждается в тактических данных на Кавказе. А во-вторых, при попадании в плен одного боевого юнита противник не должен получить доступ к большому объему секретных данных. Что самое интересное, у диверсантов та же картина. При попадании в плен одного диверсанта местная контрразведка не должна получить много информации о диверсионной сети. Число узлов дублирования, таким образом, даже в самых рискованных зонах не превышает 10.

То есть эмпирические данные дают нам возможность сделать вывод, что дублирование более 10 раз не нужно нигде и никому ни при каких условиях. Ни одному пользователю в мире. Закрытый интервал от 1 до 10. Не существует такого риска в природе, требующего более чем 10-кратного резервирования.

Тогда кому же нужны криптовалюты с многотысячекратным дублированием всего реестра?

При длительном размышлении удалось выявить только один тип организаций, которым надо знать все обо всех. Нет, конечно, есть еще и журналисты, но высокоуровневая криптография с элементами технологий систем автоматического управления войсками – это «не их почерк». Понятно, что для спецслужб, если они являются организаторами внедрения криптовалют, такой инструмент удобен. Каждый сам дает на себя весь объем приватных данных, свято веря, что система анонимна, и не желая думать, что любой криптософт, созданный спецслужбами, просто обязан иметь «бэкдор» [9].

Это нормальная работа спецслужб, им именно за это зарплату платят. Но пользователям-то это зачем? Даже если у них есть такая большая любовь к спецслужбе своей страны, то можно, наверное, найти менее затратный и сложный метод передачи им информации. Если же речь идет о спецслужбе другой страны, то можно попасть в весьма щекотливую ситуацию, незамысловато описанную Уголовным Кодексом. Как писал поэт «там просто без соли едят, там штемпель ставят наугад, кладут в конверт и посылают за можай». И если домохозяйка сможет доказать твердое незнание основ теории надежности как части теории вероятности, то любому айтишнику, который наверняка должен был ходить на лекции по терверу (теории вероятностей), да еще и экзамены сдавал, о чем осталось документальное подтверждение, отвертеться будет нелегко. Аргумент «все так делают» может и не сработать, поскольку гносеология – наука о познании, являющаяся частью философии, прямо говорит нам, что «мнение большинства не является критерием истины».

03.05.2018

Последняя редакция 31.03.2021

Ссылки

1. Ныне Университет
2. https://geektimes.ru/company/pult/blog/281704/
3. https://www.computerworld.ru/news/Natalya-Kasperskaya-zayavila-chto-bitkoin-razrabotan-amerikanskimi-spetssluzhbami
4. https://alfabank.ru/press/news/2002/2/5/1.html
5. https://ru.wikipedia.org/wiki/Героин
6. http://bankir.ru/novosti/20180321/issledovanie-v-seti-bitkoina-obnaruzhen-zapreshchennyi-kontent-10137403/
7. https://www.gazeta.ru/tech/2021/01/13/13434218/bitcoin_lost.shtml
8. https://www.recode.net/2018/4/24/17275202/bitcoin-scam-cryptocurrency-mining-pump-dump-fraud-ico-value
9. https://vz.ru/news/2018/7/15/932555.html

Юмор про криптовалюты:

При майнинге бульбы осуществляется тот же процесс - самозарождение ликвидной стоимости в результате многократной дубликации и репликации генетического кода картофеля.

Процесс майнинга картофеля сейчас более выгодный, чем майнинг биткоина. "Ферма" и участок 10 "соток" стоят одинаково, около 3000 у.е. С десяти соток хороший трейдер намайнит форк в восемь тонн бульбы, что по нынешнему биржевому курсу к доллару эквивалентно 2400 долларов США. Окупаемость проекта составит 15 месяцев. А если ферму подразогнать на навозе, то можно и все десять тонн собрать.

И при этом процесс майнинга бульбы идёт без расходов на электричество, а сама майнинговая бульбо-ферма не теряет в цене.

Более того, у бульбы имеется побочный форк под названием "самогон". Перемайненные на самогон восемь тонн бульбы дадут полторы тысячи пол-литров, или 7500 долларов США. Биткоин столько не принесёт.