Трёхсторонняя проблема блокчейна

Наташа Храмцовская приводит и комментирует высказывания авторитетных специалистов о проблемах блокчейна.

"Многие инновации в технологии блокчейна были направлены на то, чтобы вырвать власть у централизованных властей и монополий. К сожалению, утопическое видение сообществом блокчейна децентрализованного мира не лишено значительных издержек."

"Децентрализация влечёт за собой три основных вида издержек: нерациональное расходование ресурсов, проблемы масштабируемости и неэффективность, связанная с внешними факторами сетевой среды.»

Мой комментарий (НХ): Эти три свойства – это корректность, децентрализация и экономическая эффективность. На рис. также отмечено, что если упор сделать на корректность и децентрализацию, то этим требованиям удовлетворяют блокчейн-системы, в которых консенсус основан на доказательстве выполнения работы (proof of work, POW). Если же главными являются корректность и экономическая эффективность, то наилучшим решением будет централизованный реестр.

"Экономических ограничения Биткойна и блокчейна» (см. http://www.nber.org/papers/w24717), высокая стоимость добавления блока в цепочку не является случайным негативным побочный эффектом, она важна для поддержания корректности блокчейн-цепочки, и ограничивает максимальную величину транзакции, которую можно безопасно включить в цепочку. Это подтверждает результаты анализа в [BA], согласно которым если система децентрализована и корректна, она должна быть неэффективной."

"Майнеры успешных блокчейнов реального мира, таких, как Биткойн и Эфириум, не являются независимыми; они объединились в несколько крупных групп-пулов для обеспечения разумно стабильного дохода. Два крупнейших пула Биткойн-майнеров, судя по всему, оба контролируются компанией Bitmain. Им достаточно сговориться ещё с одним пулом, чтобы у них появилась возможность провести «атаку 51%» (более половины майнеров, действуя согласованно, могут обеспечить регистрацию в блокчейне любого блока – Н.Х.).

"Майнеры менее успешных блокчейнов могут быть независимыми, но их не слишком много. Доступность «майнинга как услуги» означает, что «атаки 51%» на эти блокчейны становятся повальными."

"На практике одновременная децентрализация и безопасность является недостижимой целью. Безопасность успешного блокчейн-решения основывается на нежелании доминирующих пулов майнеров убивать курицу, несущую золотые яйца. Говоря иными словами, не выдерживается тезис об исключении доверенных посредников - пользователи успешных блокчейнов должны доверять людям, контролирующим доминирующие пулы майнеров, и это не говоря уже об основных разработчиках соответствующего программного обеспечения."

"Существующее разделение между осязаемым, узнаваемым базовым кодом, считающимся внутренним для экосистемы Биткойна, и разрушительными действиями участников, находящихся вне того, что составляет ядро, позволяет сети поддерживать «легенду» об алгоритмической децентрализации, несмотря на противоречащие этому доказательства. Почему пользователи продолжают доверять коду, особенно этому конкретному коду, несмотря на наличие таких сбоев?»

Если что-либо остается неизменным, так это вера в то, что бездоверительная система может быть спроектирована, убеждение в том, что элегантное видение Накамото уже почти в пределах досягаемости посредством незначительных технических корректировок. Участникам предлагается доверять если не данной версии кода, то следующей – и так до бесконечности. Не имеет значения, видны ли сегодня какие-либо решения, поскольку модель производства равноправных участников будет продолжать итерации до тех пор, пока они не появятся.»