Тимоти Мэй

Манифест криптоанархизма

Призрак бродит по современному миру, призрак криптоанархии. Компьютерные технологии стоят на пороге того, чтобы дать возможность отдельным людям и группам общаться и взаимодействовать абсолютно анонимно. Два человека смогут обмениваться сообщениями, заниматься бизнесом, заключать электронные контракты, не имея возможности установить Подлинные Имена, личности друг друга. Взаимодействие в Сети невозможно будет отследить из-за многократных изменений маршрутов зашифрованных пакетов и предупреждающих от несанкционированного вмешательства блоков, которые наделяют криптографические протоколы практически идеальной защитой.

Репутация будет иметь первостепенную важность при заключении сделок, гораздо большую, чем сейчас имеет оценка кредитоспособности. Эти нововведения полностью изменят характер государственного регулирования, возможность взимать налоги и контролировать отношения в экономике, возможность хранить информацию в секрете; изменят свою сущность даже понятия доверия и репутации.

Технология для такой революции — а революция эта определённо будет и социальной, и экономической — теоретически разработана в прошлом десятилетии. Её методы основаны на использовании открытых ключей, систем аутентификации на основе доказательств с нулевым разглашением и разнообразных программных протоколов, предназначенных для взаимодействия, аутентификации и верификации.

До сегодняшнего дня в центре внимания были академические конференции в Европе и США, конференции, за которыми пристально наблюдало Агентство национальной безопасности. Но лишь недавно компьютерные сети и персональные компьютеры приобрели быстродействие, достаточное для практической реализации этих идей. И в следующее десятилетие быстродействие возрастёт ещё более, для того чтобы сделать эти идеи экономически осуществимыми и необратимыми.

Государство, очевидно, боясь социальной дезинтеграции, попытается замедлить или приостановить распространение таких технологий, ссылаясь на соображения национальной безопасности, использование этих технологий наркоторговцами и неплательщиками налогов. Любое из этих соображений будет обоснованным: криптоанархия позволит свободно торговать национальными секретами, а также незаконными препаратами и краденым. Анонимный компьютеризированный рынок сделает возможным даже создание отвратительного рынка заказных убийств и вымогательств. Криминальные элементы и иностранцы станут активными пользователями CryptoNet'a. Но это не остановит криптоанархию.

Точно так же, как технология книгопечатания изменила социальный строй и уменьшила могущество средневековых гильдий, криптографические методы принципиально изменят корпорации и роль государства в экономических транзакциях. В сочетании с возникающими рынками информации криптоанархия создаст ликвидный рынок любых материалов, которые можно представить в виде слов или изображений. Подобно кажущемуся второстепенным изобретению колючей проволоки, позволившей огораживать огромные ранчо и фермы и тем самым навсегда изменившей представления о земле и правах собственности в западных штатах, «второстепенное» открытие «тёмной стороны» математики стало кусачками, разрезающими колючую проволоку вокруг интеллектуальной собственности.

Действуйте, ибо вам нечего терять, кроме этих изгородей из колючей проволоки!