Roach motel protocols

Sometimes negotiations have to be undertaken where information will be disclosed that simply cannot be allowed to spread outside the negotiating table. An example might be someone selling an idea for a show to a group of buyers – they don't want their idea to be stolen, and the potential buyers may not want to reveal how much they are willing to bid for it. Thanks to transhuman technology there is a way for people who do not trust each other to reveal what they know in a negotiation and yet be certain it is not going to spread further. While non-disclosure agreement or memory editing drugs have their places, roach motel protocols guarantee total security.

Roach motel protocols (formally called "Blackbox Embedding Zero-Knowledge Smart Contracts") work by having the participants send forks of themselves into a closed simspace run by a trusted third party, perform their disclosure and negotiations inside, and then send a pre-arranged signal to the outside (usually handled by the trusted third party) about the outcome. The simspace and forks are then erased. No knowledge can escape, yet the participants know the outcome of the negotiations.

An example: Wideview Arbitration & Escrow is a corporation in Catseye Heights, one of the more upscale neighbourhoods of Extropia. Besides a number of notary, escrow and cryptographical services mainly aimed at the gambling and reputation markets the corporation offers roach motel negotiations in their "arbitration dice".

Before negotiations the participants agree with Wideview arbitrators on the terms of negotiation, in particular the possible outcome data. For an auction it might be who made the highest bid and the size of it. For a contract negotiation it might be a contract text or the terms for a smart contract AI.

Participants then are invited (physically or in an AR layer) to a sumptuous lounge where they download their forks into a cubical nanocomputer not linked to the mesh. While they wait the forks come online in a comfortable and speeded up negotiation simspace together with an AI representative of Wideview. They can negotiate in any way they want, their privacy guaranteed by the sealed-off simspace and tamperproofing of the computer. The design even has protections against fork-vs-fork hacking and can be set to self-destruct if it occurs. When an agreement has been reached (or the parts have decided to permanently break off negotiation) the AI encodes it in a write-only section of memory. This also triggers the nanocomputer self-destruct, erasing all information.

In the real lounge a Wideview representative removes the result sliver and ceremonially throws the die into the fireplace. The participants can then sign whatever contract or agreement their forks agreed to, knowing that this is what they would have agreed to knowing what their forks did.

Smart contracts

Smart contracts are contracts that are not just legal documents but actually active AI code. In the beginning smart contracts were just computer programs that facilitated, verified or enforced the performance of a contract. A simple example would be "digital repo", where access to certain

information or a machine would be granted or not depending on whether one party had paid the other. More advanced digital repo contracts would recognize if the seller went absent or bankrupt, and then allow access with no constraints. Over time the intelligence increased, allowing contracts to actually gather information, check that they are obeyed and even take action.

For example, two hypercorps decide to share research data on a quid pro quo basis. They create a smart contract that has access to both their research databanks. When both corps indicate a file each the contract copies them, after having checked that the contents fulfil whatever obligations are in the contract. If one of the corps breaks the rules the contract might have an arbitration clause, automatically calling in an arbitration company to deal with the disagreement, or possibly activate penalty clauses (such as debiting money placed in escrow or denying further access).

Smart contracts start out as elaborate legal documents, usually formulated in SCML, E!, DryXchnge or some other legal computer language. Once agreed on they are compiled into the contract AI, which is equipped with the necessary cryptographic signatures, budget and other information to do what it needs to do. Usually the contract resides in a bank, law or arbitration secure server, often with backup contracts in other servers.

Smart contracts are single-minded even for AIs; while some may have very advanced pattern recognition or legal thinking modules the *only* thing they care about is performing their contractual function. They might know major secrets, but if they are written to be quiet about them they will remain quiet no matter what.

Adventure possibilities: The PCs might be hired by a contract to check certain information. The contract has started to think one of the parts is doing advanced cheating that it cannot detect online.

The Fall destroyed many smart contracts; their servers, the parties they belonged to or the entire legal systems they acted in disappeared. But occasionally salvaging might unearth an old smart contract. It might have access to funds, data or legal obligations of a formerly minor company, today a major hypercorp. Played right by a very smart lawyer it might be a real treasure.

What do you do when your lease-buy contract acquires the Exurgent virus?

Microtorts

In extropian habitats microtort systems are sometimes used. This provides an expedited way of handling everyday interactions and disagreements. For example, if somebody trespasses into the space of somebody else, inflicts emotional distress or breaches confidence a microtort can be triggered – the claimant simply tells their muse to sue. The muse contacts the relevant law and arbitration companies. If the muse of the defendant agrees a microtort court is constructed virtually with AI representatives for the different parties. They decide on compensation and automatically debit it from the defendant if they lose. Since the results are also posted on the reputation blogs they affect rep. If the defendant and/or their muse decline to a micotort it is up to the claimant whether they want to escalate to a “real” tort case.

During an ordinary day a person can be in dozens of microtorts, each costing a small amount of credits. In many cases they just stabilize good behaviour: knowing that quarrelling with a neighbour will cost you a few credits or some rep can keep you from doing it. Sometimes it is worth paying a trivial fine for making a shortcut through someone's tunnel. There is a trade-off between being litigious and successful. While it is possible to amass money and rep by suing everybody, it tends to erode the overall rep strongly. Microtorts tend to earn more to the arbitration software than the people involved.

There is some discussion in the Titanian Commonwealth about using similar systems. The two microcorps Aarhus RapidStamning and Nanotort are currently demonstrating the possibility. Many Titanians think this is an inner system aberration that should be resisted, but some think a dose of flexible AI- and sousveillance-supported common law is just what Titan needs to become a more polite society.