Intelligence MEMOS

From: Thorsten Koeppl

To: Office of the Privacy Commissioner of Canada

Date: May 18, 2017

Re: WHAT THE "TERMINATOR" TELLS US ABOUT BLOCKCHAIN AND YOUR PRIVACY

The Blockchain revolution is here. And, in many ways, it is like the Internet was when it started 20 years ago. We did not know how we would be affected, but we all had a feeling that this is going to be big. After watching a movie classic — the "Terminator" — I realized that three questions stand out when gauging the potential of Blockchain and Distributed Ledger Technology more broadly.

First, how big are the cost savings?

The financial industry has jumped on the technology because distributed ledgers allow for supplanting crucial intermediaries that form the infrastructure on which financial markets run. Payment systems, record-keeping, even mortgage lending could be performed without the use of specialized intermediaries and traditional front-line institutions such as banks. So, big profit stakes are up for grabs and the question is only how cost effective distributed ledger technology can become.

Second, is there a need for privacy?

Big data has already pushed many enterprises towards customer monitoring, targeted advertising and unbundling of services. Consequently, it has become near impossible for people to hide sensitive information. New developments in Blockchain have made it possible, however, to effectively hide one's identity in online payments transactions. It thus seems possible to go further and design systems that protect one's privacy entirely without a designated third party having access to such information.

Third, can we rely on independent, safe and smart communication between IT systems?

A future where machines control other machines and robots produce robots depends on one crucial element: guaranteed self-execution. Smart contracts are often heralded as the future of Blockchain. Such contracts are precisely designed to "enforce" themselves without faults. Seems like SkyNet is not that far off a reality after all.

Blockchain applications seem to have little merit unless one can answer such questions convincingly. Reflecting on the three questions above, however, one intriguing area where a Blockchain could help has recently gained a lot of traction: universal ID systems that give people (i) a unique, online identity — something like an official universal passport; and (ii) privacy at the same time.

With Blockchains that ensure privacy, computers in a network compete for maintaining and updating the information contained in the ID system without having access to this information per se. Hence, no third party is necessary. The downside of this model is that it is quite costly to implement since the security of such a Blockchain increases with the computer power sunk into it and such an ID system needs to be super safe.

Maybe after all then a simple, universally available distributed ledger where only the government has permission to change entries is a better option for such an ID system as it could help reduce costs. But would you really trust the government with running this chain and protecting your privacy? So an independent network of computers protecting your privacy — even if costly — is not such a bad idea after all ... well, if there weren't those cyborgs.

Thorsten Koeppl is a Fellow-in-Residence, and Scholar in Financial Services and Monetary Policy, at the C.D. Howe Institute.