Outsmarting Smart Contracts – or Does Man Always Win?*

Blanka Kovács

Ari Juels:
The Oracle
Talos Press, 2024, p. 288
ISBN: 978-1-945863-86-8

Since the publication of Satoshi Nakamoto's Bitcoin whitepaper, a number of books and studies have been published on blockchain technology, the crypto market, the technological and financial innovations based on it, including speculation and fraud, and the impact of such on society. The development of the technology is followed with great interest not only by professionals but also by the media. Thus, it is not surprising that literary minds and imaginative people have also been inspired by the topic, and browsing Amazon, you can find many books in the crypto sci-fi genre.

The Oracle, published in February 2024, stands out for being written by an academic with considerable expertise in the world of blockchain. *Ari Juels* is a Professor in the Department of Computer Science at Cornell University, co-founder of IC3 (Initiative for CryptoCurrencies and Contracts) and Chief Scientist at Chainlink Labs. This is not his first foray into literature: he is also co-author of the 2010 techno-thriller *Tetraktys*. Juels is the author of more than a hundred widely-cited studies, his h-index[1] is high. His key areas of research include security, smart contracts cryptography and blockchain technology.

The novel's inspiration comes from three sources: Juels' passion for ancient culture and mathematics, a place that is special to him, and a study published in 2016. The author studied Mathematics and Latin, and this provides the historical thread of the story. The bridge motif recurs several times in the book. According to the main character's definition, blockchain oracles form a bridge between the real world

* The papers in this issue contain the views of the authors which are not necessarily the same as the official views of the Magyar Nemzeti Bank.

Blanka Kovács: Magyar Nemzeti Bank, Analyst. Email: kovacsbl@mnb.hu

[1] H-index, a measure of a researcher's scientific performance. The more citations to a researcher's publication, the higher the h-index. An h-index of 20–30 indicates an internationally recognised performance. Ari Juels has an h-index of 100. https://scholar.google.com/citations?user=uf0D-uoAAAAJ&hl=en

and closed blockchain systems. The protagonist works in a Manhattan skybridge office, a setting inspired by the writer's fascination with skybridges and his previous office. The central idea of the novel was inspired by a publication that explored the potential use of smart contracts and blockchain oracles for criminal purposes. The thriller aims to entertain and raise awareness of the stories that blockchain solutions combined with artificial intelligence can tell.

The plot of the book starts when a software developer working for a blockchain company becomes the target of "rogue smart contracts". The open source code is published on the internet by an organisation called Delphian. There was a contract out on the protagonist for allegedly disrespecting and "desecrating" the ancient Greek god Apollo. Given the vast amount of information on the internet, this could even be a bad joke. But when the first target is actually murdered, the contract is activated, and somebody actually gets the reward, it arouses the FBI's attention.

The blockchain technology, according to the protagonist, is conceptually not complicated, and is like a digital bulletin board that is accessible to all. Its main features: transactions are immutable and verifiable by third parties, i.e. transparent. The radical change is that you can run smart contracts on it. These smart contracts are also unalterable and are not controlled by a central body. The code is available to and can be run by anyone. The blockchain oracle is the secret ingredient, as these systems are closed, the challenge is to load authentic and correct data into the smart contracts (blockchain oracle problem). The Oracle of Delphi was one of the most important sites in ancient Greece, where rulers and commoners could turn to the Greek god of truth, Apollo, for advice and guidance. The original meaning of the word oracle is also mediator. Oracles served as a kind of bridge in Greek mythology. In Juels' novel, the modern analogue of the oracle of Delphi is the blockchain oracle, a source of information for smart contracts, allowing them to perform transactions based on authenticated data.

Juels' characters reflect a variety of subcultures. We meet the protagonist as an anonymous person who, as a technical expert, is also interested in history. In his spare time, he blogs about technology with an educational purpose. As a snub to the academic world, he says: "I don't read this Cornell professor's papers, because I can predict what he will write about". Among others, an FBI detective character we know from American films, a researcher with a passion for ancient Greek mythology, a Generation Z cryptocurrency native and the manager of a leading investment bank, also join the story. These characters represent a broad spectrum of people who (also) operate in the world of blockchain and cryptocurrency.

In addition to the twists and turns, the story also includes technical details, e.g. about a new financial product, the multi-block flash loan. A flash loan is a decentralised financial product, and a multi-block flash loan is a variant of this.

The idea behind a flash loan is that the loan is taken out and repaid in a single block, which means the whole process can take a few seconds depending on the speed of the blockchain. Flash loans are often used for various financial strategies, such as arbitrage, without the user having to use his or her own funds. Since the loan and the repayment are made in one transaction, the loan will only be successful if the loan amount is repaid in full by the end of the transaction. If the repayment is not made, the transaction is reversed as if it had never taken place. This minimises risk for the lender, but requires a high level of technical knowledge and market expertise from the user. Multi-block flash loans allow transactions to be spread over several blocks. This means that the user is given more time to use and repay the amount borrowed, which allows for more complex financial transactions, such as complex arbitrage strategies or other more time-consuming transactions. With multi-block flash loans, the user must ensure that the loan and associated fees are repaid over several blocks, which offers greater flexibility and opportunity, but also entails the challenges of ensuring successful repayment.

The story also explores ethical dilemmas, highlighting that combining blockchain technology with artificial intelligence can have unexpected consequences. The protagonist, whose faith in the integrity of smart contracts is unquestioned, is faced with a dilemma when the FBI asks him to hack the blockchain oracle. It also raises the question of whether open source code and publicly available smart contracts require profound knowledge, are safe for everyone to use, or whether they are only safe for skilled professionals.

Smart contracts are essentially computer code, with the advantage that they are unambiguous and can be used to enforce precise “contracts” between us. In reality, however, we communicate in a human language, which gives rise to a myriad of associations. However, large language models (LLMs) can act as a kind of interface, a translator between people, institutions and blockchain systems. The overall message of the book is that technology is essentially neutral, and can be used for good or bad. Without exposing the Delphian “criminal organisation”, the other message of the book is that it is worth looking at our micro-environment first.

Ari Juels’ novel is rich in twists and turns, and its characters reflect the mindset and behaviour of the industry’s players. It explains the basic workings of blockchain technology and the technical details in a way that is easy to understand, but assumes a higher-than-average level of interest in the subject. To sum up, I recommend the book to all those interested in technology and finance, reminding them that they have a science fiction thriller in their hands.