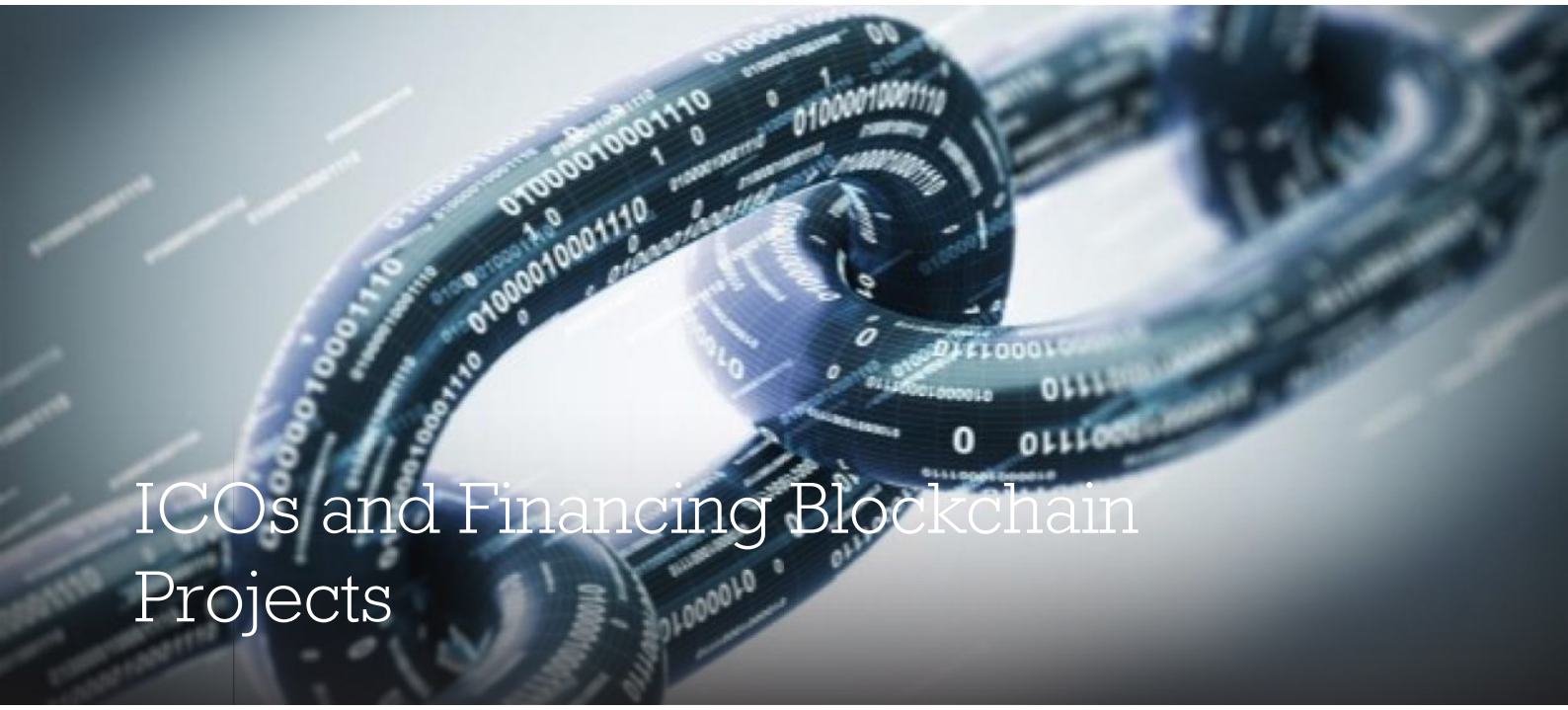


ICOs and Financing Blockchain Projects

A new mechanism for financing innovation: seigniorage.

Most blockchain projects are open source and therefore free to use. Despite this, developers of open-source blockchain projects can reap large financial rewards thanks to a novel class of assets, called cryptotokens (or cryptocurrencies).

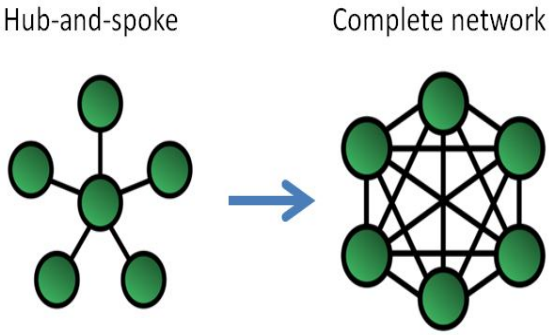
In a recent working paper **"Financial incentives for open source development: the case of Blockchain"**, I propose calling this novel finance mechanism *seigniorage.* Historically, seigniorage is profit earned by a government when issuing currency. For blockchain, it is profit earned by a software developer when issuing a cryptotoken that is required to use software. In my paper, I build a game-theoretic model and show that, despite its effectiveness at channelling funds from investors to developers and entrepreneurs, seigniorage can give rise to serious incentive problems.

Existing data show that seigniorage is becoming extremely relevant. In 2017, blockchain start-ups raised an estimated **US$7 billion** via initial coin offerings, or ICOs. (ICOs occur when tokens are first sold to investors; subsequent sales are typically held on the open market.) This figure is much larger than the funding by traditional VCs (estimated at US$1 billion in 2017) and by other non-traditional sources, such as crowdfunding.

Blockchain

Blockchain is better understood in relation to the internet. The internet protocol suite (commonly known as TCP/IP) was developed to allow decentralised data transmission, i.e. the transmission of data via a network of computers in which no individual node is essential to the functioning of the network. It is the technological foundation of a second set of protocols (also called application-layer protocols) handling specific types of data: HTTP for accessing web pages, SMTP, POP and IMAP for sending and receiving emails, etc.

The development of the internet protocol suite was financed by the Defense Advanced Research Projects Agency (DARPA). The goal was to increase military communication resilience by moving from a ***hub-and-spoke*** model of communication to a ***complete network*** model of communication.



In the hub-and-spoke model, a central node delivers all messages and is therefore essential: If eliminated, no communication can occur. In the complete network model, communication among any two nodes can occur even if any other node is eliminated.

These two network structures are also very different with respect to the economic environment they create. In the hub-and-spoke model, the central node acquires market power: It can filter information and charge fees. In the complete network model, no node has market power. Before the internet, intermediaries like media companies exploited their market power by making both accessing and transmitting information costly. For example, finding out the latest sport results or stock prices required the purchase of a newspaper. In the internet age, information can be sent, received, published and accessed for free, for the most part. This has brought about a historical transformation: The limiting factor in information consumption is no longer the availability of information itself, but rather the availability of attention and time.

Blockchain further expands the possible operations that a computer network can perform. Like TCP/IP, it allows for the decentralised transmission of data, but also permits the decentralised storage, verification and manipulation of data. Blockchain is also similar to TCP/IP in that both provide the foundation for a number of application-layer protocols. The most well-known is the bitcoin protocol, which allows a network of computers to store data (how many bitcoin each address owns) and enforce specific rules regarding how these data can be manipulated (no double spending). Importantly, without blockchain technology, maintaining the same type of data would require a traditional organisation (typically a bank).

Numerous other blockchain-based protocols currently exist or are being actively developed. For example:

- Protocols for building applications that can run on a decentralised network rather than on a specific computer (Ethereum, Tezos)
- Protocols for decentralised real-time gross settlement (Ripple, Stellar)
- Protocols enabling the creation of a decentralised marketplace for storage and hosting of files (Sia, Filecoin) and for renting in/out CPU cycles (Golem)
- Protocols creating fully decentralised prediction markets (Augur), financial exchanges (0x) and financial derivatives (MakerDAO)
- Protocols allowing for the existence of fully decentralised organisations (Aragon); and many more.

Profits from tokens

An important difference between the protocols built on TCP/IP and those built on blockchain is how their developers are rewarded. Most TCP/IP protocols are open source, free to adopt and use. Project contributors are not organised in a single, traditional company, but rather form a loosely defined group around one (or more) project leader, based on open collaboration. Developers do not receive direct financial compensation for their contributions and are motivated by career concerns (i.e. boosting their reputation to reap a future financial benefit) or by non-monetary considerations (i.e. contributing to public good). The development of blockchain-based protocols, on the other hand, can leverage financial incentives.

Seigniorage allows developers of open-source blockchain-based projects to benefit financially from their work. As an illustration, consider a population of agents who wish to transact but lack the required infrastructure. These agents may want to exchange a physical good, but there may be no legal system or agreed-upon unit of measurement. Alternatively, the exchange may be between computers, in which case the technical specifications governing communication between machines may be missing. An entrepreneur may decide to invest resources and create this missing infrastructure, and, with it, a market. One way to profit from this investment is to create a token and force all exchanges on this market to use it. All prices within the market can be expressed in fiat currency (i.e. a legal tender such as euros or dollars), but must be paid using the token. The entrepreneur owns the initial stock of tokens and can credibly commit to limit their supply. If the market is successful, there will be a demand for these tokens, a positive price for tokens and thus profits for the entrepreneur.

The way blockchain enables seigniorage is threefold. First, blockchain can be used to create the infrastructure and therefore a marketplace.[1] Second, the rules determining whether (and how) the supply of tokens increases over time can be set

initially and cannot be manipulated afterwards. That is, using blockchain, the entrepreneurs can commit to a specific supply of tokens. Finally, the protocol also prescribes the use of a certain token; it is not possible to transact using a different token.

The perils of seigniorage

But how effective is seigniorage as a mechanism to finance innovation? To answer this question, I built a game-theoretic model of blockchain financing. In the model, a developer (or a team of developers) exerts effort and invests resources in the development of a blockchain-based protocol. However, the developer may not have enough resources to invest efficiently in the protocol development. A solution becomes to hold an ICO and sell some tokens to investors to raise funds.

The key observation is that, post-ICO, investors and users of the protocol will start trading tokens on financial exchanges. The developer will also be able to sell additional tokens on those exchanges. This situation creates, in game-theoretic jargon, an **anti-coordination problem**. If investors, who are by definition forward-looking, expect the developer to diligently create a successful protocol, this expectation should be priced in. But in such case, the developer would be better off selling all his tokens, cashing in on the future work without completing the project. If investors instead believe that a developer is not likely to complete the project, then the token price should be zero. However, this does not mean the tokens are worthless: The developer could keep them all, improve the protocol and then sell them once the project is successful.

The analysis of the model reveals that, in equilibrium, the game always carries a positive probability that the developer will sell all tokens and stop development. Even though the environment considered here has no informational asymmetries (i.e. investors are perfectly able to evaluate the project quality and the developer's ability), a positive probability remains that the developer will simply walk away.

Implications

ICOs (and seigniorage) are effective in providing the developer with funds to invest in the protocol development. At the same time, holding an ICO also generates an incentive problem: There is some probability the developer will sell all tokens and walk away. The existence of this trade-off has several implications. To start, developers should hold ICOs as late as possible in the development cycle. Ideally, they should wait until the protocol is ready for use. Second, some form of vesting – a post-ICO period during which developers cannot sell their tokens – should be required. Third, post-ICO, developers should keep a sufficiently high share of tokens, to maintain "skin in the game" and continue the development of the protocol.

Blockchain has the potential to be a transformative technology. The realisation of this potential will depend on the incentives generated by seigniorage. My paper shows that seigniorage generates some incentives, but their strength is limited by the fact that, in equilibrium, there is some probability that developers will sell all their tokens and walk away. In the absence of better rules or regulation, the existence of projects that fail to deliver following an ICO should not be considered exclusively the outcome of a few scams, but rather an unfortunate consequence of the financing scheme adopted by these projects.

Andrea Canidio *is the Stone Fellow of the INSEAD James M. and Cathleen D. Stone Centre for the Study of Wealth Inequality and an Assistant Professor of Economics at the IMT School for Advanced Studies, Lucca, Italy.*

Follow INSEAD Knowledge on ***Twitter*** *and* ***Facebook****.*

[1] It may appear that not all blockchain projects have this marketplace element. Yet even in the case of cryptocurrencies such as bitcoin, there are two sides: people who need to exchange bitcoins, and computer owners who process these transactions (miners). Bitcoin users pay the miners directly and indirectly. Bitcoin senders can pay miners a fee to process a transaction faster. In addition, the network awards miners new bitcoins for their work. Because this increase in supply affects the bitcoin price, it amounts to a transfer from the bitcoin holders to the miners.