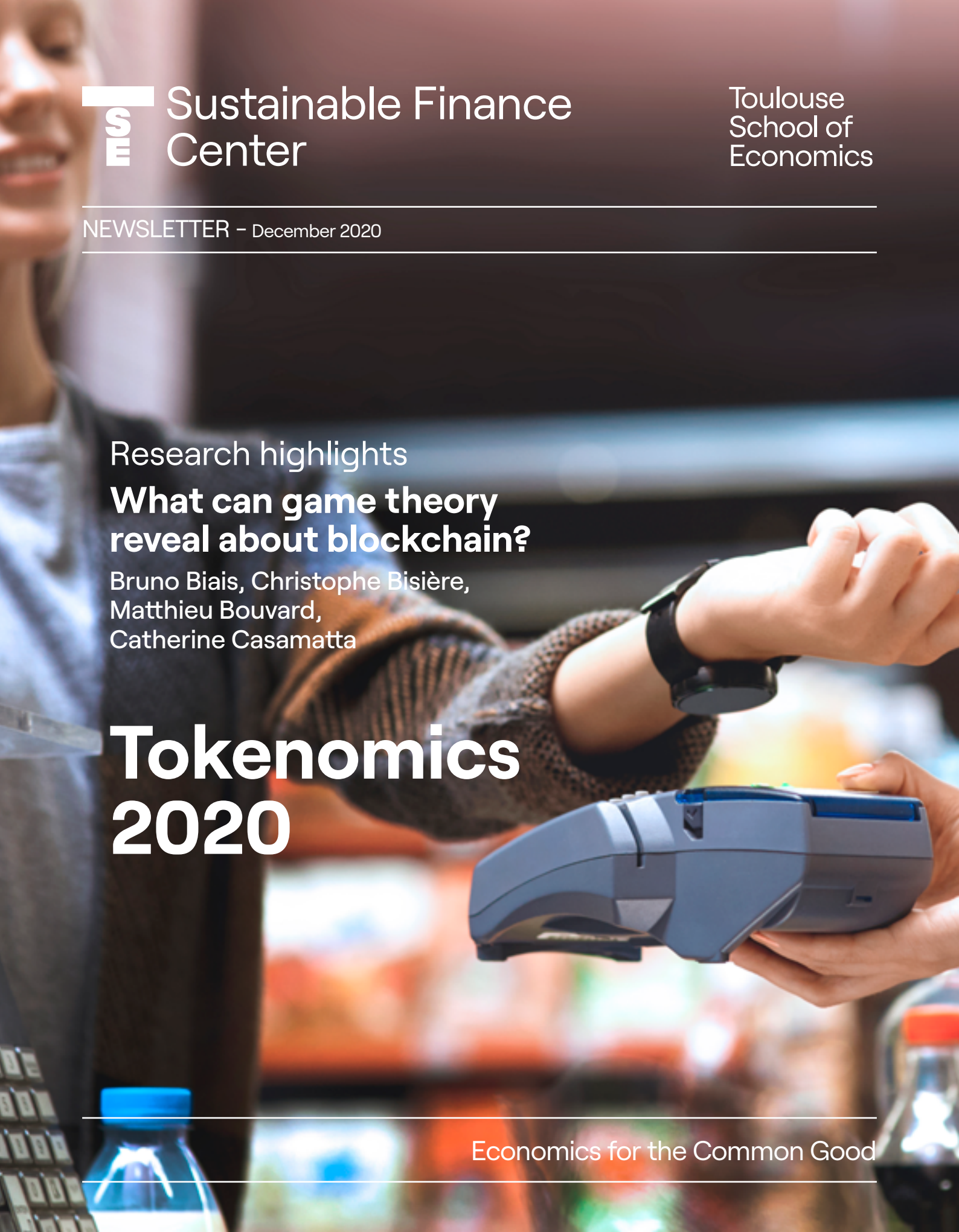
Sustainable Finance Center

Toulouse School of Economics

NEWSLETTER – December 2020



Research highlights

What can game theory reveal about blockchain?

Bruno Biais, Christophe Bisière, Matthieu Bouvard, Catherine Casamatta

Tokenomics 2020

Director's message

The fintech revolution

Digitization is remaking the world of finance, with far-reaching impacts for our economies and societies. In many respects, the breakneck pace of innovation has accelerated during this difficult year. The Covid-19 pandemic has highlighted the appeal of tech solutions such as cloud computing, online banking, and automation. Social distancing has only added momentum to the pre-crisis surge in digital payment systems and other innovative financial services. Soaring Bitcoin prices, which broke a new record in November, appear to be attracting long-term investors who are increasingly confident about blockchain security and accessibility.

How can we harness the benefits of digital finance? Have cryptocurrencies changed the nature of money? How can we regulate an unfamiliar world? TSE is firmly established as a global hub for gathering international multidisciplinary expertise to address such 21st-century challenges. Often now interacting remotely ourselves, TSE researchers are accustomed to embracing new technologies and new perspectives. At the Sustainable Finance Center, we are enthusiastic about engaging with other disciplines and adapting state-of-the-art economic tools to make sense of the latest developments.

In October, we were proud to host **Tokenomics 2020**, our second annual conference on blockchain economics, security and protocols. The event was held both in our new building and online. Working together with the TSE Digital Center and our partners at Ecole Polytechnique, Capgemini, Ethereum France and Kaiko, we were delighted to encourage the interaction of economists, computer science researchers and software engineers at this unique international forum.

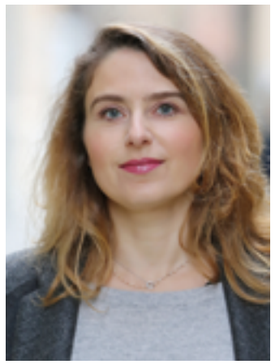
Inspired by their ideas, this issue of our newsletter focuses on the financial impact of blockchain technology. As emphasized at Tokenomics 2020, game theory can help us to understand the strategic interactions that take place on blockchains. In our research highlights, we are pleased to present excerpts from an upcoming review by TSE researchers Bruno Biais, Christophe Bisière, Matthieu Bouvard, and Catherine Casamatta of recent economic analysis on this subject. We also feature contributions from some of the keynote Tokenomics speakers, including economists Jean Tirole (TSE), computer scientists Timothy Zakian (Novi, Facebook) and Ittai Abraham (VMware Research) and the Ethereum France - Kaiko prizewinner Amin Shams (Ohio State University).

Wishing you an enjoyable read!

Sophie Moinas
Director, TSE Sustainable Finance Center

News

TSE pair to advise French stock market regulator



Catherine Casamatta

Fany Declerck

Catherine Casamatta has been appointed scientific advisory board member of the French stock market regulator (*Autorité des Marchés Financiers,* AMF). She joins a group of leading figures from the academic and financial worlds, including fellow TSE researcher **Fany Declerck**, whose appointment has been renewed for a further term.

Board members provide the AMF with information on current financial research. Catherine recently presented ongoing research on *equilibrium Bitcoin pricing*, a topic of great interest and concern for French regulators.

Find out more about *AMF*

TSE welcomes two new assistant professors

We warmly welcome **Patrick Coen** and **Eugenia Gonzalez-Aguado** to the TSE Sustainable Finance Center.

Patrick arrives with a PhD from London School of Economics and specializes in financial economics and industrial organization. He is currently examining the interbank network, in which banks compete with each other to supply and demand financial products, and its potential tradeoffs between surplus creation and risk propagation.

Eugenia alights at TSE with a PhD in Economics from the University of Minnesota. Her research interests are in international macroeconomics and labor. Her work explores how monetary policies from the United States affect developing countries through their ability to borrow internationally. She is also currently studying the relationship between economic downturns and migration patterns of workers.

More information can be found on their *TSE webpages*

Matthieu Bouvard

TSE expert wins grant to study fintech risk management

The French National Research Agency *(Agence Nationale de la Recherche, ANR)* has awarded **Matthieu Bouvard** a research grant to investigate the impact of technological innovation on risk management in financial institutions. Christophe Bisière and Catherine Casamatta will be working alongside Matthieu on this project, starting in March 2021.

They propose to use tools from information economics, industrial organization and experimental research to model how technology-driven changes in the finance industry create new sources of risks. They also plan to study the incentives for existing players and new entrants into financial services to manage these risks, with a special emphasis on the increasingly important role of data management in finance.

SCOR Chair rewards risk and insurance economists

SCOR The Art & Science of Risk | Fondation pour la science

The TSE Sustainable Finance Center is proud to belong to The European Group of Risk and Insurance Economists (EGRIE), a non-profit organization dedicated to promoting research on risk and insurance.

Two awards are granted during the EGRIE annual seminar, organized within the framework of the *SCOR Chair "Risk Markets and Value creation"* at TSE-P and Dauphine University, sponsored by SCOR and the Fondation du Risque.

This year we are pleased to award the SCOR-EGRIE Young Economist Best Paper Award to Richard Peter and Pascal Toquebeuf for ***"Separating ambiguity and ambiguity attitude with mean-preserving capacities: Theory and applications"*** and the SCOR-Geneva Risk and Insurance Review Best Paper Award to Céline Grislain-Letrémy and Bertrand Villeneuve for ***"Natural disasters, land-use, and insurance"***.

More information is available at *www.egrie.org/awards-grants*

European Group of Risk & Insurance Economists

Banque de France renews TSE partnership

Banque de France and TSE have a long-established scientific partnership based on deep insightful discussions and research activities. The aim of this recently renewed partnership is to support and complement the scientific expertise of Banque de France, and develop research projects, seminars and conferences in the fields of financial stability and macroeconomics.

Jean Tirole and François Villeroy de Galhau

In September, we were pleased to welcome *Bruno Cabrillac*, Deputy Director General of Economics and International Relations, for a "business talk" on the current challenges of monetary policy. These distinctive lectures are organized for our students to develop the economic culture and help build their future career plans.

Also within this partnership, a series of prizes was launched, granted every two years since 2012 to distinguished academic researchers who have developed central concepts to improve our understanding of monetary economics and finance. The next prizes will be awarded during a ceremony at Banque de France in Spring 2021. The winners will present their work to an audience of business leaders, decision makers, economists, TSE students and researchers.

This December, scientific director of the TSE-Banque de France partnership, Fany Declerck, took part in a online conference organized by the ACPR and the AMF, with the support of the Banque de France.
This series named *"Rendez-vous de l'Épargne"* has an educational purpose: to provide investors with key economic and financial insights, to increase vigilance against financial scams and to make the general public aware of the role of savings, particularly in times of economic recovery.

Find out more about this partnership on our *website*

Research highlights

What can game theory reveal about blockchain?

Bruno Biais, Christophe Bisière, Matthieu Bouvard and Catherine Casamatta

Blockchains are distributed ledgers maintained using technologies – such as cryptography and peer-to-peer networks – and protocols to ensure that nodes in the network reach agreement on the current state of the ledger. Specialized in the study of strategy, economics is particularly well equipped to analyze the choices made by 'miners' and other agents responsible for validating blockchain transactions. TSE researchers Bruno Biais, Christophe Bisière, Matthieu Bouvard and Catherine Casamatta have reviewed some of the latest game-theoretic research in this rapidly developing field for an upcoming book, 'Principles of Blockchain Systems'. Here, we present excerpts from their contribution, which focuses on some of the technology's key economic mechanisms.

Bruno Biais

Christophe Bisière

Matthieu Bouvard

Catherine Casamatta

To study the performance and reliability of blockchain protocols, computer scientists traditionally draw a distinction between processes (or miners) that conform to the protocol and faulty processes that don't. For example, the Proof of Work (PoW) protocol defined by Nakamoto (2008) considers the longest chain as representing the consensus, and faulty processes are attackers whose aim is to perturb consensus building by deviating from this longest chain rule. Here, the question of interest is the extent to which malicious nodes can succeed in breaking consensus, or equivalently, what proportion of honest nodes is required to maintain consensus. While this approach provides useful notions of robustness, it is silent on the reasons why processes adhere to the protocol or deviate from it.

This blind spot suggests a role for economic analysis to complement the work of computer scientists: economics offers a conceptual framework to model and understand the role of incentives that can be applied to blockchains. Instead of assuming specific behaviors (e.g., honest or faulty), the natural economic approach is to model processes as rational agents who choose actions to maximize their expected utility. This approach reflects the view that human decisions ultimately drive strategies in the blockchain and in particular whether processes conform to the protocol.

In addition, the economists' toolkit is able to account for situations in which agents' strategies exhibit complex dependencies. In particular, economists draw a distinction between competitive and strategic behaviors. Competitive agents take the characteristics

of the economic environment (e.g., prices) as given, and react optimally. Strategic players take into account the impact of their actions on the outcome of their interactions with other players. Game theory is well suited to the analysis of strategic interactions in a blockchain. Miners, or more generally, validators, face complex decision problems in which they need to anticipate the behavior of others. Which equilibrium strategies emerge? Are they compatible with the integrity and reliability of the blockchain?

> Economics offers a conceptual framework to understand the role of incentives that can be applied to blockchains. The natural economic approach is to model processes as rational agents who choose actions to maximize their utility. This reflects the view that human decisions ultimately drive strategies in the blockchain.

Mining strategies

In a blockchain, the history of transactions is represented by a chain of transaction blocks. The goal of a consensus protocol is to ensure that participants agree on which chain represents this history. Under Proof of Work, this is implemented through a distributed lottery: a miner is selected to append a block to the blockchain if it is the first to solve a numerical problem by random trials, an activity called "mining". Consensus is achieved when there is a single chain, without forks. This obtains when miners follow Nakamoto's "longest chain rule". Should we expect miners to deviate from this rule? If so, which patterns emerge? Will forks be transient? What economic forces make them more or less likely?

Longest chain rule

One of the first papers to consider consensus formation in the PoW protocol as the outcome of a game is Kroll et al (2013). First, the researchers view miner's strategy as a mapping from "the blockchain structure [...] to a choice of which branch to mine on." Second, they note that "reward is only valuable if the newly mined block ends up on the long-term consensus chain." In this context, following the longest chain rule is a Nash equilibrium strategy, but there are other equilibria.

In a previous paper (Biais et al, 2019a)*, we formally analyze interaction between miners as a stochastic game. For all parameter values, and in particular for any distribution of computing power among miners, following the longest chain rule is a Nash equilibrium strategy. In Kiayias et al (2016), this is the case when each miner's computing power is sufficiently small.

Our paper (2019a) assumes that the reward for a block is larger when more miners chain their blocks to its branch. This assumption is made to capture the idea that rewards are paid in units of cryptocurrency, whose value is higher when more agents accept it. An important consequence of this assumption is that miners want to chain their block to the branch they expect others to adopt, i.e., mining in the blockchain is a coordination game. Therefore, if miners anticipate that the other miners will follow the longest chain rule, their best response is to do the same. This explains why, in our paper (2019a), following the longest chain rule is always a Nash equilibrium.

Kiayias et al make a different assumption about rewards: *"at every level, only one node is paid for, the first one which succeeds in having a descendant d generations later. [...] When this happens, every sibling (as well as its descendants)"* gets no reward. In this framework a fork can only generate a reward if it reaches the d-block threshold before the honest branch. When miners' computing power is small, they have little chance to win that race if forking. Thus, in Kiayias the longest chain rule is a Nash equilibrium if each miner's computing power is sufficiently small.

Our paper (2019a) highlights that coordination effects give rise to other (multiple) equilibria. Indeed, if a miner anticipates that the others will fork and abandon the longest chain, his best response is to do the same. This generates orphaned branches at equilibrium. We characterize equilibria in which such forks can be of arbitrary length and shows that equilibria with forks exist for any distribution of computing power among miners. Next, we investigate the strategic consequences of the k-block rule which prevents miners from spending their rewards before k blocks are chained to the block they solved. This rule generates vested interests, in the sense that miners who solved many blocks on a branch strongly prefer that this branch survives. We give conditions on parameter values such that the combination of vested interests and coordination effects gives rise to equilibria with persistent forks. An example of persistent fork is offered by the split between Ethereum and Ethereum Classic in July 2016, that led to two blockchains that still coexist today.

While transaction fees are currently a small fraction of miners' rewards, they will become important when coinbase transactions disappear. Carlsten et al (2016) show that when a block includes transactions with large fees, miners have an incentive to fork and create an alternative block including some of these transactions. When doing so, they choose to leave some transactions out of their block, to induce subsequent miners to chain their own block to the fork. The strategic choice of transactions, in order to earn large fees, can thus give rise to equilibrium forks and protocol instability.

*B. Biais, C. Bisière, M. Bouvard, and C. Casamatta, 2019a, *"The Blockchain Folk Theorem"*, The Review of Financial Studies, 32(5), 1662–1715

> Game theory is well suited to the analysis of strategic interactions in a blockchain. Miners, or more generally, validators, face complex decision problems in which they need to anticipate the behavior of others. Which equilibrium strategies emerge? Are they compatible with the integrity and reliability of the blockchain?

Double spending

When others follow the longest chain rule, miners can deviate and 'double spend' if they are able to create a chain with more blocks than the original. This, however, requires large computing capacity. Bonneau et al (2016) analyze "bribery attacks" in which miners obtain large computing capacity for a limited period by renting it. Teutsch et al (2016) consider an alternative way to increase one's share of total computing power: the attacker offers prizes to other miners for solving puzzles outside the blockchain, thus reducing the pace at which blocks are added on the public branch. By doing so, if the attacker has sufficient initial capital, he can ensure that his private chain is longer than the public one. In our paper (2019a), we highlight that coordination effects also condition the success of double spending attacks. Early analyses of blockchains pointed to attacks relying on 51% computing power as the major threat to protocol security. These game-theoretical approaches, however, show that consensus can be unstable even if no miner (or pool) has the majority of the computing power.

Upgrades

Consensus is particularly difficult to achieve, and the risk of forks is particularly large, when decisions about the protocol must be made by participants. In practice, most forks have been triggered by protocol upgrades. In another paper (Biais et al, 2019b)*, we highlight the crucial role played by coordination effects: If each miner anticipates the upgrade to be adopted (resp. rejected) by all the others, then the upgrade is adopted (resp. rejected) in equilibrium, irrespective of whether it is socially optimal. We give conditions under which, if some miners derive private benefits from using one version of the protocol, equilibria with persistent forks can be sustained. Barrera and Hurder (2018) study whether governance mechanisms can solve coordination problems in this context and show that two common voting schemes (majority rule and quadratic voting) can fail to eliminate suboptimal forks.

Selfish miners

Rather than publishing blocks as soon as they are solved, 'selfish' miners can choose to withhold blocks. Eyal and Sirer (2014) show that if a colluding group of miners follows a selfish mining strategy, while the others are honest (i.e., stick to the longest chain rule), then the colluding group of miners obtains a fraction of total rewards that is larger than its fraction of the computing power, and consequently honest miners obtain a fraction of total rewards smaller than their share of computing power.

Under Eyal and Sirer's assumption that the attacker's objective is to maximize his share of total revenue, selfish mining is a best response to honest mining because some blocks solved by honest miners become stale. It is not a best response, however, if the attacker's objective is to maximize his expected reward. In practice, there appears to be no compelling evidence that selfish mining is prevalent. This may be due to the conceptual difficulties to rationalize selfish mining.

Supply of mining services

Blockchain is designed to operate as an open network, in which entry is free. Are miners' decentralized entry and capacity decisions socially efficient?

Computing capacity

A key feature of PoW protocols is that the difficulty of the hash puzzle adjusts to keep the average time between two blocks constant. Thus, when a miner increases his computing capacity, the difficulty of the hash puzzle increases for all participants. In this context, the probability that a miner solves a hash puzzle and obtains a reward is determined by his computing capacity relative to the total computing capacity on the blockchain.

Dimitri (2017) studies a simultaneous game among n miners who choose how much computing capacity to install. When choosing capacity, each miner takes into account its impact on his cost, as well as on his probability to solve a block, given the update in protocol difficulty. Intuitively, strategic miners choose to limit their impact on difficulty to maximize profits. This results in strictly positive equilibrium profits for miners, and implies that several miners are simultaneously active in equilibrium.

However, our study (2019a) points out that, in the above game, each miner exerts a negative externality on the others when increasing his own computing capacity. Indeed, when a miner builds up capacity, he makes it more difficult for the other miners to collect block rewards. Because of this negative externality, the computing capacity investment game can be interpreted as an arms race. In this

* B. Biais, C. Bisière, M. Bouvard, and C. Casamatta, 2019b, *"Blockchains, Coordination and Forks"*, AEA Papers and Proceedings 109, 88-92

context, equilibrium computing power is inefficiently high, relative to the social optimum. Using a similar model, Arnosti and Weinberg (2018) show that miners with lower marginal costs end up with a disproportionately higher share of total computing power.

With the inclusion of an initial stage during which miners invest in research to develop better hashing technologies, Alsabah and Capponi (2019) show that the R&D game is also an arms race. In this context, limitations of property rights on research output, such as spillovers or lack of non-compete clauses, can improve welfare. This R&D game can also result in centralization.

One could expect that as the dollar-value of Bitcoin rises and rewards from mining increase, entry and capacity acquisition should occur. Figure 1 shows there is some correlation between hashrate and Bitcoin price. To analyze this relation, Prat and Walter (2018) incorporate two key features: First, investment in computing capacity is largely irreversible. Second, the dollar-value of Bitcoin is highly volatile. Thus, when deciding to increase capacity, the optimal policy entails a threshold instantaneous revenue from mining that triggers new investment. This barrier is reflecting because as soon as miners invest, the difficulty adjustment pushes their revenue down.

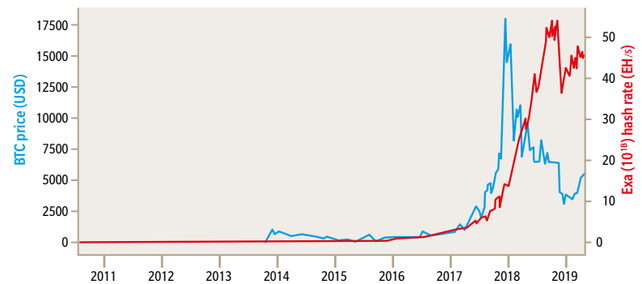


Figure 1: Evolution of hash rate and bitcoin price
(Source: authors'own computations and www.blockchain.com).

Pagnotta (2018) introduces a feedback loop where investment in computing capacity makes the blockchain more secure, which stimulates users' demand for the cryptocurrency and pushes its price up. This loop allows for the co-existence of multiple self-fulfilling equilibria. In one, because the cryptocurrency price is zero, no miner is active, which makes the blockchain insecure and users unwilling to pay any strictly positive price for using the cryptocurrency to transact. On the other hand, an equilibrium with strictly positive prices, active miners and a positive demand from users may also be sustained. These feedback effects may amplify volatility.

Mining pools

Given the increase in computing capacity depicted in Figure 1, any individual miner with limited computing capacity stands a very small chance of solving a block. Risk-averse miners, however, would benefit from mutualizing block discovery risk. Do mining pools provide efficient risk sharing? Do they exert market power? Can they adopt strategic behaviors that undermine the functioning of the blockchain?

Cong et al (2020) analyze how competing pools set membership fees. With no captive miners, Bertrand competition drives equilibrium fees down to zero. But if a pool has captive members, other miners can benefit from risk-sharing, so it can charge a strictly positive fee and still attract non-captive members. Pools with a larger captive base charge higher fees, and yet remain larger than the others. Moreover, these large mining pools partially internalize the negative externality imposed by the computing power of their participants on the protocol difficulty. This further contributes to driving their fees up. It also tends to reduce their growth compared to that of smaller pools. This result alleviates concerns regarding large pools' ability to capture an excessive market share. Ferreira et al (2019), however, argue that the structure of the market for specialized mining equipment known as ASICs (Application-Specific Integrated Circuits) can foster mining pool concentration that gives ASIC producers disproportionate control over the blockchain.

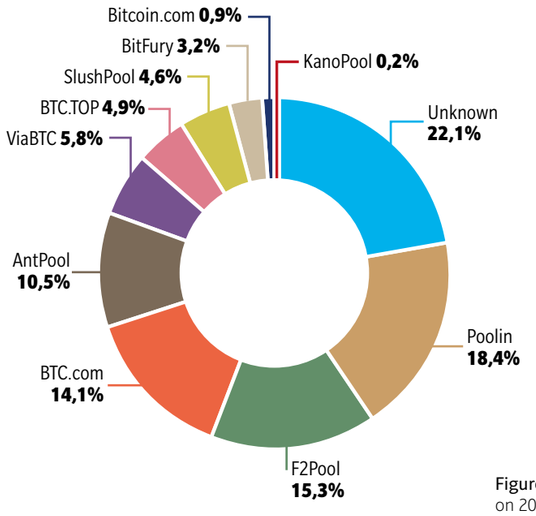


Figure 2: An estimation of hashrate distribution amongst the largest mining pools on 20 December 2019 *(Source: www.blockchain.com).*

Large mining pools can adopt other strategic behaviors that threaten the blockchain. Eyal (2015) shows that a pool can capture a share of the rewards of competing pools without contributing to block discovery by infiltrating miners who withhold their full proofs of work. In doing so, a pool reduces its own fraction of total rewards but gains a share of its opponent's fraction of total rewards. Eyal shows that in any Nash equilibrium of this game, pools send a strictly positive number of infiltrators.

> Any individual miner with limited computing capacity stands a very small chance of solving a block. Risk-averse miners, however, would benefit from mutualizing block discovery risk. Do mining pools provide efficient risk sharing? Do they exert market power? Can they adopt strategic behaviors that undermine the functioning of the blockchain?

Alternative consensus protocols

Proof of Stake (PoS) is an alternative consensus mechanism that may avoid the large electricity consumption and investment in hardware that PoW entails. PoS implements a version of the following protocol. At regular time intervals, a validator is drawn from the pool of token-holders and has the right to append a new block to an existing chain. Users with more tokens are more likely to be drawn, therefore agents with higher "stakes" exert more control over the blockchain. The presumption is that these agents have more to lose if the blockchain malfunctions, hence have better incentives to maintain consensus.

Under PoW, the computing power devoted to mining a block has an opportunity cost because it cannot be used to mine a block on a different chain. Under PoS, adding a block is seemingly free for the chosen validator. This gives rise to the concern that validators would append any branch to ensure that some of their blocks end up on the winning chain, perpetuating forks. Saleh (2020) argues that this line of reasoning misses one cost for validators to indiscriminately add blocks, namely that it delays the time at which consensus is reached.

In other protocols, a committee composed of a subset of deterministically selected processes executes an instance of Practical Byzantine Fault Tolerant consensus to decide on the next block to append. Amoussou-Guenou et al (2019) highlight that coordination failures and free-riding can lead to equilibria in which the committee fails to reach consensus or accepts an invalid block. Such dysfunctional outcomes arise when rational committee members fail to check the validity of blocks or to send messages. An equilibrium also exists in which committee members are pivotal, giving them the incentive to check validity and send messages so that the termination and validity properties hold.

Find out more

For research by Bruno Biais, Christophe Bisière, Matthieu Bouvard and Catherine Casamatta, see ***tse-fr.eu***.

Principles of Blockchain Systems is due to be published by Morgan & Claypool.

For a comprehensive survey of game-theoretical approaches to blockchain, see Liu, Z., et al, *"A Survey on Applications of Game Theory in Blockchain"* (2019).

Summing up

The analyses reviewed here shed light on the reliability and cost of blockchains. Game-theoretical analyses underscore that rational agents cannot be expected to blindly follow prescribed behavior, even if they do not derive any private benefit from failing the blockchain. Rational, self-interested behavior can threaten blockchain stability and consensus for two types of reasons. On the one hand, coordination failures can generate forks. On the other hand, profit-maximizing agents can engage in manipulative behaviors, such as selfish mining or infiltrating pools. An important insight of game-theoretical approaches is that consensus can be unstable even if no miner or pool has the majority of computing power.

Given a fixed maximum block size, transaction fees can serve as useful price signals, to incentivize investment in computing capacity or to allocate priority. Game-theoretical analyses, however, suggest that it would be efficient to relax block size constraint, and to rely on other features of the protocol to induce sufficient participation of miners. Another source of inefficiency is the negative externality imposed by miners on others when they increase their own computing capacity. This leads to an arms race with inefficiently high capacity. This underscores the need for more sober protocols than PoW, such as PoS. Strategic interactions in these new environments will raise new challenges that the literature has only started to investigate.

Outreach

Tokenomics 2020

Blockchain economics, security and protocols

Emmanuelle Anceaume (CNRS, IRISA) and Christophe Bisière (TSE), are two of the five members of the Tokenomics scientific commitee. Here they share the spirit and key takeaways from the event.

> New payment technologies can create meaningful value for consumers. However, technological disruption does not upend the fundamental economic principles that shaped our financial systems and regulatory framework.
>
> Jean Tirole *(TSE)*

> What determines the return structure of cryptocurrencies? What is the source of the underlying value?
>
> Amin Shams *(Ohio State University)*

Keeping up with the pace of new advances in digital finance requires nimble, flexible, and open minds that can draw on a range of perspectives from evolving and emerging disciplines. **TSE's second Tokenomics Conference on Blockchain Economics, Security and Protocols** invited economists, computer science researchers and software engineers working on blockchains to take part in a unique program featuring outstanding talks from world-class developers and academics.

Tokenomics is an international forum for the theory, design, analysis, implementation and applications of blockchains and smart contracts. Following the great success of the inaugural event last year, Tokenomics 2020 was a hybrid creation in several senses. Hosted both virtually and on-site at Toulouse School of Economics (TSE), it was also a multidisciplinary joint event held together with the TSE Digital Center's conference entitled Digital Platforms: Opportunities and Challenges.

In this section, we present some of the ideas and analysis from Tokenomics 2020 speakers. Nobel laureate **Jean Tirole** (TSE) reviews some of the economics of the fintech revolution; **Timothy Zakian** (Novi, Facebook) reveals how the Move programming language is used to represent digital assets on Libra; and **Ittai Abraham** (VMware Research) discusses the intersection of economics, computer science and blockchain technology. We also present highlights from the work of **Amin Shams** (Ohio State University) in his recent paper *'The Structure of Cryptocurrency Returns'*, which was awarded the Ethereum France - Kaiko Prize at the Toulouse conference. Along with Ethereum France and Kaiko, sponsors of the event included Ecole Polytechnique and Capgemini.

Tokenomics 2020 has been a fantastic event, showcasing the cross-pollination and effervescence of both the economics and computer science communities to combine their expertise to address the many facets of blockchains, ranging from cryptography, peer-to-peer, distributed computing, and robust incentives to create the blockchain revolution. Such interplay between these two academic fields is no surprise, as consensus protocols rely on both algorithms and incentives. The challenge is to bring this interplay into action - this is what Tokenomics aims for.

We look forward to welcoming you to the next edition in 2021.

> Imagine a meeting between Satoshi Nakamoto and John Nash: what would they talk about?
>
> Ittai Abraham *(VMware Research)*

> We can build a digital asset representation on-chain that is lossless by design: wherever it may go on-chain, such a digital asset cannot ever be 'lost' or accidentally forgotten, and no new digital assets can be created on-chain without the correct privileges.
>
> Timothy Zakian *(Novi, Facebook)*

Find out more on the Tokenomics event page *www.tse-fr.eu/conferences* and catch many of the recordings on the TSE YouTube Tokenomics playlist *youtube.com/TSEchannel*

Maria Potop-Butucaru
Sorbonne University

Marianna Belotti
Caisse des Dépôts

Yackolley Amoussou-Guenou
CEA & Sorbonne University

Fintech economics

Jean Tirole

Traditional financial practices are being overturned by a rising tide of new technologies, including digital payment systems. Avoiding the pitfalls will not be easy, TSE founder Jean Tirole reminded the Tokenomics audience, but a focus on fundamental economic principles may help to ensure that both businesses and consumers benefit from fintech's impressive potential.

> If left unsupervised, a private global digital currency could raise a range of public policy issues ranging from tax fraud and money laundering control, to loss of seigniorage revenue, impediments to monetary policy, and the potential threat to financial stability

The contours of digital payments are still in the making. Recent years have seen the emergence of new instruments best exemplified by public cryptocurrencies like Bitcoin and by Big Tech payment systems like Alipay. These developments in the private sector have in turn fueled discussions and projects around the creation of central bank digital currencies.

Digital currencies have a lot to offer. They can provide consumers with user-friendly, low-cost means of payment and facilitate the integration of payment systems across borders. They may also offer alternatives in countries with dysfunctional national monetary systems. On the supply side, private digital currencies can be a source of funding (such as initial coin offerings) and allow businesses to retain consumers and to collect information.

Which form of digital currency will eventually prevail has yet to be seen. In their current form, popular permission-less cryptocurrencies lack the price stability necessary to serve as a store of value: accepting a payment in Bitcoin exposes a merchant to costly financial risk. Stable coins pegged to a central-bank currency and backed by safe collateral (Tether or Libra, for example) are an attempt to dim excess volatility. But this guarantee creates new challenges: collateral must be segregated and prudentially supervised to ensure consumer protection. It is unclear which authority would have the capacity and incentives to provide that supervision for a global digital currency. More generally, if left unsupervised, a private global digital currency could raise a range of public policy issues ranging from tax fraud and money laundering control, to loss of seigniorage revenue, impediments to monetary policy, and the potential threat to financial stability.

In this context, Central Bank Digital Currencies (CBDC) may provide a solution that combines the convenience of private digital money with the institutional support of a state. But the scope of a CBDC's deployment needs to be carefully calibrated: a CBDC directly held by wholesale or retail depositors would compete with bank deposits, possibly limiting banks' ability to engage in their essential function of maturity transformation through long-term credit.

Overall, the deployment of new technologies for payments has the potential to create meaningful value for consumers. However, technological disruption does not upend the fundamental economic principles that have shaped our financial systems and regulatory framework. Applying these principles may be our best chance to understand the ongoing fintech revolution.

When Nakamoto meets Nash

Ittai Abraham

Ittai Abraham is a senior researcher and cofounder at VMware Research, working on algorithms and distributed computing. He previously worked at Microsoft Research Silicon Valley. Addressing the Tokenomics event in October, he shared his thoughts on the deep connections between blockchain technology, computer science and economics.

Imagine a meeting between Satoshi Nakamoto and John Nash: what would they talk about? Surveying the blockchain breakthrough through the lens of game theory, Ittai began by discussing the economic tools that might be used to model money and the new cryptocurrencies.

Traditionally money is defined as a medium of exchange using a scarce resource that can function as a store of value. Nakamoto's goal was to provide a low-friction payment system *"for two willing parties to transact directly with each other without the need for a trusted third party"*. The Bitcoin solution is to use electronic payments, a limited supply of 21 million bitcoins, and its ledger technology that solves the Byzantine General's problem.

How can we compare different types of money systems?

"We need a microeconomic theory of competition between money systems," Ittai argued. *"We must model money endogenously by assigning utility based on its beneficial properties, including friction (or how good the system is as a medium of exchange), fairness (how good the system is as scarce resource), and trust (how good the system is as a store of value)."*

What does it mean to not have a trusted third party?

Nakamoto wanted to ensure that authority was distributed among many participants, and adopted the Proof of Work chain as a solution. The main focus of Ittai's talk was on the importance of such efforts to incentivize trust. *"A lot of work has already been done, but there is a need to formalize a game theoretic approach to consensus and provide an analogue to Byzantine Fault Tolerance."*

Who maintains the ledger?

"Any time you have a Byzantine Fault tolerant consensus system, the players who are decentralizing trust and running this consensus protocol are those who are allowed to vote. In Bitcoin, honest nodes must collectively control more voting power (measured in CPU power) than any cooperating group of attacker nodes."

Is this the right way to assign voting power?

"There are many other approaches," Ittai observed, *"including Proof of Membership (one member, one vote), Proof of Work (one CPU, one vote), Proof of Stake (one coin, one vote) and Proof of Space (one GB of storage, one vote). There is evidence that Proof of Work causes centralization, waste, and prefers certain geographic regions and taxation regimes. How can we avoid monopolies, centralization and bribery?"*

How can blockchains be scaled?

"Technical challenges include building a better consensus protocol and recording transactions in an open and accessible ledger. But the hardest bottleneck in terms of scalability is the execution (or validation) of transactions. Are there game theoretic mechanisms to incentivize people to behave honestly?"

Ittai concluded by challenging researchers to find ways to incentivize fairness and welfare. Can we use notions of robust equilibrium to provide better notions of fairness and avoid selfish mining? Can a theory of blockchains as public goods help to enhance consumer welfare?

> On Scalability, the technical challenges include building a better consensus protocol and recording transactions. But the hardest bottleneck in terms of scalability is the execution of transactions. Can we scale execution by using game theoretic mechanisms to incentivize people to behave honestly?

Who puts a price on cryptocurrencies?

Amin Shams, *Ethereum France – Kaiko prizewinner*

Despite the growing importance of cryptocurrencies for innovation, investment and capital allocation, our understanding of their valuation and price movements remains limited. Awarded the Ethereum France – Kaiko Prize for Research in Cryptoeconomics at the 2020 Tokenomics Conference, Amin Shams (Ohio State University) shows that the tightly meshed dynamics of user and investor decisions play a crucial role. His recent paper is the first to document the power of network effects to amplify demand shocks in this market.

Feeding an astonishing surge in financial innovation in recent years, blockchain technology has put the development of financial instruments within reach of a rapidly growing community of entrepreneurs and investors. Thousands of cryptocurrencies already exist within a very active trading ecosystem, with more than 200 cryptocurrency exchanges around the world. Because of the unique features of this market and the rampant speculation it has inspired, economists like Amin are particularly interested in the pricing of these assets. *"So far we have a limited knowledge,"* he admits. *"What drives cryptocurrency prices? What determines the return structure of cryptocurrencies? What is the source of the underlying value?"*

Demand matters

Some researchers have attempted to shed light on these questions by looking at characteristics such as size, book-to-market ratio, past returns, and industry. The main focus for Amin's recent paper, however, is on investor demand as a key driver of cryptocurrency returns.

"Buying or selling pressures can affect the fundamental value of cryptocurrencies if the pressure comes from potential users," Amin observes. *"Because using the features of a cryptocurrency ecosystem often necessitates holding the token, the user base is inherently interwoven with the investor base. In this environment, because the market cannot completely distinguish between speculator and user demand, even purely speculative demand can have a substantial effect on prices beyond what is observed in traditional markets."*

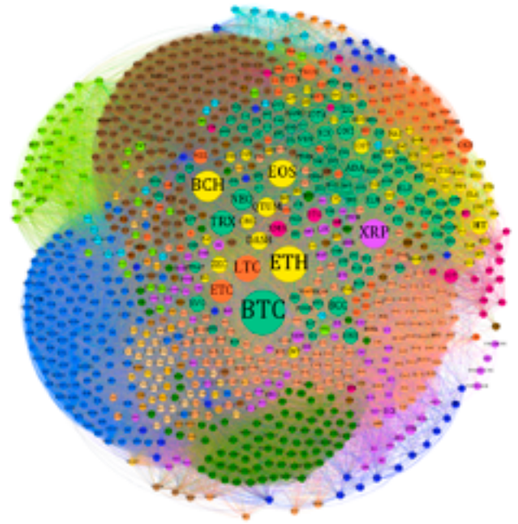
> Because the market cannot completely distinguish between speculator and user demand, even purely speculative demand can have a substantial effect on cryptocurrency prices beyond what is observed in traditional markets

Connected currencies

Amin's empirical setting exploits rich exchange-level trading data on a wide cross-section of cryptocurrencies merged with technical characteristics and social media content. Due to geographical and other restrictions, cryptocurrency exchanges attract different investor bases. For example, a South Korean exchange named Bithumb is only open to South Korean investors. Importantly, different cryptocurrencies show different levels of trading activities on different exchanges.

To create a proxy for exposure to similar investor clientele, Amin creates a "connectivity" measure based on cryptocurrencies' trading locations. Cryptocurrency pairs that trade on exactly the same exchanges are given a maximum score of one, those on entirely different exchanges score zero. Amin then examines the extent to which his connectivity measure can explain why the prices of some cryptocurrencies move together.

He first finds that cryptocurrencies with similar characteristics such as size, trading volume, age, and consensus mechanism show significantly higher comovement. Amin also finds that coin cryptocurrencies comove more with other coins, and tokens with other tokens.



This figure illustrates the connectivity of cryptocurrencies in the period from January 1, 2017 to June 30, 2018. Each node represents a cryptocurrency, where the relationship between each pair of currencies is defined as the average monthly connectivity, using Amin's measure. Different colors are used for illustrative purposes and represent different clusters derived from a modularity analysis of the network structure.

However, by far the highest comovement is explained by exposure to similar investor bases (as proxied by cryptocurrencies' trading locations). Currencies connected to other currencies that perform well generate significantly higher returns. *"This effect is very strong,"* Amin says. *"The magnitude is larger than can be explained by all other characteristics combined. The effect also increases with the time-horizon and leads to a strong cross-predictability."*

Potential channels

If cryptocurrencies with similar unobservable characteristics are more likely to be listed on the same exchanges, then it could be the underlying fundamentals, and not demand shocks, driving the relationship between connectivity and comovement. However, using evidence from new exchange listings and a quasi-natural experiment caused by the 2017 shutdown of Chinese cryptocurrency exchanges, Amin shows that unobservable characteristics cannot explain these patterns.

Instead, he told the Tokenomics conference, *"My results reflect commonalities in crypto investors' demand: a strong exchange-specific component drives cryptocurrency order flows, even after controlling for the currency-specific flows."*

Network effects

In a final step, Amin's paper examines the extent to which his results are driven by the network effects of adoption by users and developers. Cryptocurrencies vary in the degree to which they rely on network externalities. If the price impact of the demand shocks is amplified through the network effect, Amin's intuition was that the impact should be larger for currencies that derive more value from the network externalities.

Using machine learning techniques to analyze 25 million currency-specific comments on the social media platform Reddit, he tested this implication by quantifying variation in the beliefs of different crypto communities about their reliance on network effects.

Consistent with the theory of network effects developed elsewhere in the research literature, Amin finds that network-based currencies such as Ethereum show significantly higher volatility: *"The demand effects are 36.4% to 50.9% larger for cryptocurrencies that rely more heavily on network externalities of user adoption. This finding suggests that demand shocks are a first order driver of cryptocurrency prices, largely because they can be perceived as a sign of user adoption."*

This research shows that understanding the demand side of this market is a vital first step toward assessing its valuations and price movements. *"Due to novel features of the cryptocurrency market,"* Amin concludes, *"demand from users and developers may correlate with that of investors and speculators, implying that even pure speculative demand can have an amplified effect on prices. This feature can help explain why cryptocurrencies are prone to wild price movements and bubbles. Further research is needed to disentangle the roles of users and investors in this market and better understand the complex interplay between these groups."*

Summing up

This research shows that understanding the demand side of this market is a vital first step toward assessing its valuations and price movements. *"Due to novel features of the cryptocurrency market,"* Amin concludes, *"demand from users and developers may correlate with that of investors and speculators, implying that even pure speculative demand can have an amplified effect on prices. This feature can help explain why cryptocurrencies are prone to wild price movements and bubbles. Further research is needed to disentangle the roles of users and investors in this market and better understand the complex interplay between these groups."*

FURTHER READING

Research by **Amin Shams**, including his 2020 paper *"The Structure of Cryptocurrency Returns"*, is available to view at aminshams.com

Digital currencies as types

Timothy Zakian

Timothy Zakian is a software engineer at Novi, a new digital wallet Facebook is building for people to access the Diem network. As a keynote speaker at the Tokenomics Conference, he discussed how different digital assets are represented on the Diem blockchain[1] with the Move programming language.

"As shown by Jean-Yves Girard, a linear value can be moved from one place to another but can never be copied or forgotten," Timothy told the Toulouse audience. *"From its inception, Move - developed to implement custom transactions and smart contracts on the Diem blockchain - has had values (or resources) that behave in this linear manner as a central part of its semantics. Move enables significant parts of the Diem protocol, including the Diem Coins, transaction processing, and validator management."*

In the process of exploring the representation of digital assets on-chain in Move, Timothy's presentation revisited one of the first examples used to introduce linear logic; that of payments, and discussed other ideas from programming languages along the way, such as type-indexed data types and code modularity. He showed how we can leverage these ideas to provide strong guarantees of key asset properties such as losslessness, value conservation, and explicit representation of an asset, its currency, and its value.

"As we explore the implementation of a digital asset in Move, we see how code is organized into a number of different modules, with each module consisting of resources and functions that can be used with the resources defined in that module. This gives rise to a type of strong encapsulation around the resources defined within a Move module: only functions within the module that define the resource can create, destroy, or access the fields of that resource.

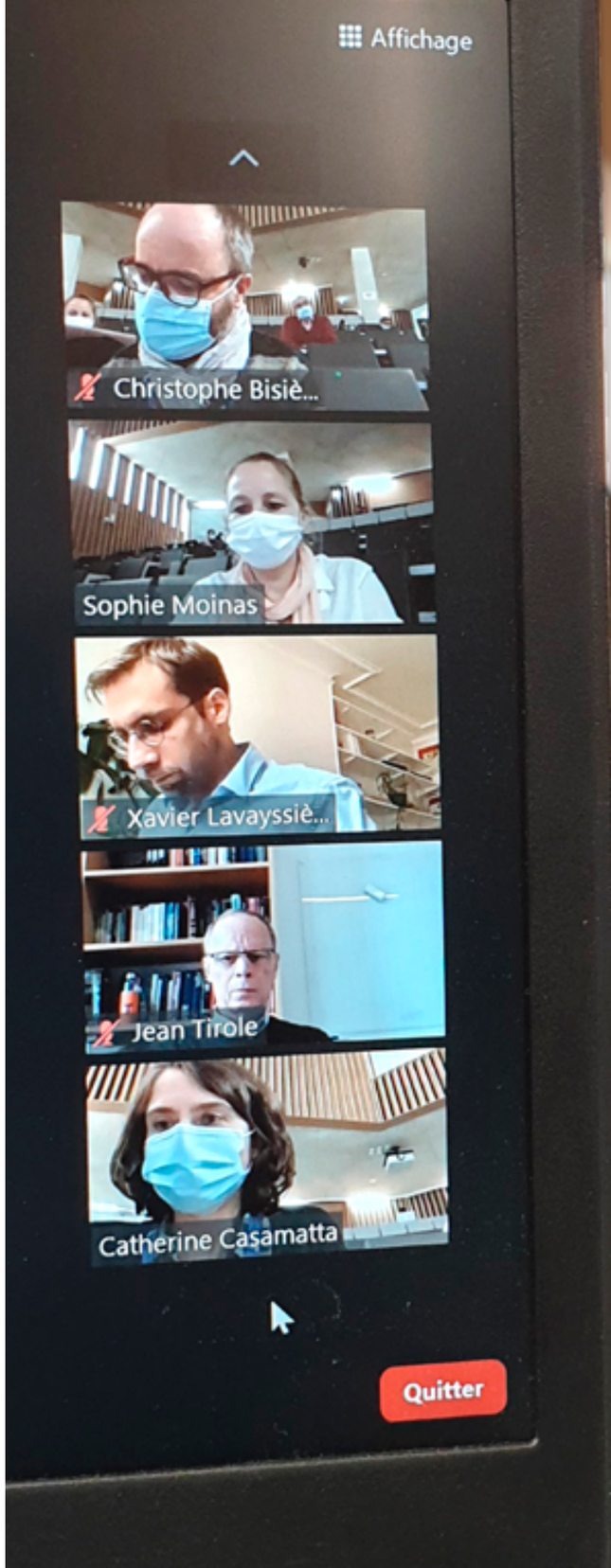
"Representing a digital asset as a resource, coupled with this strong encapsulation, and privileging the creation and destruction operations within the module means that we can build a digital asset representation on-chain that is lossless by design: wherever it may go on-chain, such a digital asset cannot ever be 'lost' or accidentally forgotten, and no new digital assets can be created on-chain without the correct privileges.

"We can then index this digital asset resource that we have built in Move by a type-level representation of each currency in the system to arrive at an explicit static representation of the currency of a digital asset. This representation statically disallows entire classes of possible issues, such as trying to combine two assets in different currencies, while still preserving all of the properties that we previously had, such as losslessness.

"With this representation of a digital asset that we have built in Move, we can also test and verify that the value of the digital assets on-chain are preserved outside of creation and destruction operations; since the only functions that can change the value of an asset must be defined within the same module we can heavily test, and in fact verify, that these functions preserve the value of any digital assets that they may interact with. At the end of this process we arrive at a testable, verifiable, and explicit representation of a digital asset in Move that is lossless, conserves value, and represents its currency and value explicitly."

> We can build a digital asset representation on-chain that is lossless by design: wherever it may go on-chain, such a digital asset cannot ever be 'lost' or accidentally forgotten, and no new digital assets can be created on-chain without the correct privileges

[1] Formerly known as Libra, the Diem Association (of which Novi is a member) announced its new name on December 1, 2020, emphasizing the network's organizational independence. Timothy Zakian's references to Libra have been updated accordingly.



Media

Members of the center regularly publish blog posts and newspaper op-eds that can be consulted in *TSE Debate's section*. Here we feature some of the recent posts

Debate

The regulation sandbox - Claude Crampes & Stefan Ambec */ December 02, 2020*

On November 5, 2020, the French Energy Regulatory Commission (CRE) ruled on the eligibility of the applications submitted as part of the regulatory experimentation mechanism provided for by the Energy and Climate Law. Why, out of the 41 applications received, did the CRE only declare 19 applications eligible?

Plugging carbon leaks - Stefan Ambec & Claude Crampes */ October 22, 2020*

'The border adjustment mechanism proposed by the European Commission is designed to reduce imported CO2 emissions. An attractive initiative on paper but whose implementation is a real headache. It conflicts with the trade negotiations conducted by the same Commission.'

God insures those who pay: Formal insurance and religious offerings in Ghana

Emmanuelle Auriol, Amma Panin & Paul Seabright / *September 19, 2020*

Do religious believers give money to their churches in the hope of receiving insurance against economic shocks? If so, is this because they expect the church to look after them when shocks occur? Or do they expect God to look after them by making such shocks less likely to happen?

Betting on hydrogen - Claude Crampes and Stefan Ambec */ September 14, 2020*

Hydrogen will gradually find its place in the energy mix. This is the wager that our governments in Europe are making with billions of euros of investment. For the moment, it rather sounds like wishful thinking: one day hydrogen will be a "clean, safe and affordable" energy carrier.

Let's be honest, the fight against climate change will cost us all - Christian Gollier */ September 11, 2020*

There is a fairly unanimous agreement that we have a huge problem with climate change, but there is no consensus on how to fix it. Our policy is in disarray, without an overview, and this generates great frustration and tension in society. Economists are used to disagreeing, but on this matter there is a 95% consensus. They all say we won't get by without carbon pricing.

Articles

- La médecine libérale, un gisement d'économies
  Frédéric Cherbonnier, *Les Échos*, November 19, 2020
- Confiner les personnes vulnérables, plutôt que les jeunes et les actifs
  Christian Gollier, *Le Monde*, November 5, 2020
- Barrières à la sortie des énergies fossiles
  Stefan Ambec & Claude Crames, *La Tribune*, November 3, 2020
- MAC : un écran de fumée pour cacher le bilan carbone des traités commerciaux ?
  Stefan Ambec and Claude Crampes, *La Tribune*, October 10, 2020
- Aux collectivités de sortir des sentiers battus pour tirer parti des plans de relance
  Jean Tirole & Marion Guillou, *Le Monde*, October 7, 2020
- Marion Guillou et Jean Tirole : préparer les territoires au monde d'après
  Le Point, October 1, 2020
- Economic policy under the pandemic: A European perspective
  by 30 economists including Christian Hellwig and Franck Portier, VoxEU, July 7, 2020
- Efficacité énergétique des bâtiments : la pratique loin des attentes théoriques
  Stefan Ambec and Claude Crampes, *La Tribune*, June 30, 2020
- Roulement de batterie chez Tesla
  Stefan Ambec & Claude Crampes, *La Tribune*, May 30, 2020
- Le leurre de l'épargne salariale
  Frédéric Cherbonnier, *Les Échos*, June 3, 2020

Interviews

- On pourrait confiner uniquement les personnes à risque important
  Christian Gollier, *Le Point*, November 9, 2020
- Faut-il durcir le confinement des seniors ? Voici les arguments qui s'opposent
  Christian Gollier, *La Dépêche du Midi*, November 7, 2020
- Laisser travailler les jeunes et les adultes et confiner les plus vulnérables
  Christian Gollier, *L'Opinion*, October 27, 2020
- Préservons l'avenir de notre jeunesse: ne confinons que les personnes âgées et vulnérables!
  Christian Gollier, *Le Figaro*, October 28, 2020
- Lundi vert : *"S'interroger sur nos habitudes alimentaires n'est pas anecdotique pour l'environnement"*
  Nicolas Treich, *20Minutes*, October 4, 2020
- Lundi Vert : est-ce que c'est utile d'adopter le "Lundi Vert" qui bannit viande et poisson ?
  Nicolas Treich, *Grazia*, September 28, 2020
- Les normes internationales sauveront-elles la planète ?
  Stefan Ambec, *France Culture*, September 23 2020
- Le paradoxe de la viande
  Nicolas Treich, *L'Usine Nouvelle*, September 30, 2020
- L'après Covid-19 : *"Toulouse peut se relever de cette crise"*
  Jean Tirole, *La Tribune*, September 29, 2020
- Airbus restera un acteur crucial pour la région
  Jean Tirole, *La Dépêche du Midi*, September 30, 2020
- "Lundi vert" : ni viande ni poisson une fois par semaine, les consommateurs vont-ils suivre ?
  Nicolas Treich, *Sud Ouest*, September 24, 2020
- The fight for the climate will cost everyone money
  Christian Gollier, *De Tijd*, September 19, 2020
- Quelle relance pour quelle reprise ?
  Christian Gollier, CCI Toulouse, September 2020
- L'accord UE-Mercosur risque d'accélérer la déforestation, selon les experts
  Stefan Ambec, *Le Monde*, Setember 17, 2020
- Climat: *"Il est illusoire de penser que les mesures coercitives ne sont pas coûteuses"*
  Nicolas Treich, *L'Opinion*, June 23, 2020
- Faire payer les Chinois pollueurs, est-ce réaliste ?
  Christian Gollier, *Capital*, June 16, 2020
- Emmanuel Macron : *"Une économie forte, écologique, souveraine et solidaire"*
  Christian Gollier, BFMTV, June 15, 2020
- Is this the most irrational trade in finance history?
  Sébastien Pouget, *Australian Financial Review*, June 18, 2020
- Les industriels français en faveur d'une taxe carbone aux frontières
  Christian Gollier, *Le Monde*, June 17, 2020
- Le monde d'après sera attentatoire au pouvoir d'achat
  Christian Gollier, *Les Échos*, June 19, 2020
- La crise renforce la nécessité de relancer le marché du CO_2
  Christian Gollier, *L'Agéfi*, June 2, 2020

Seminars

The Center organizes weekly academic seminars allowing faculty and members to meet and exchange ideas with fellow financial experts from leading universities, firms and institutions.

Seminars are also an opportunity for PhD researchers to get insightful information on various topics such as:
Bitcoin / Venture capital / Crypto economics / Banking crisis / Liquidity management

List of speakers

- Michaela Pagel *(Columbia Business School)*
- Elisabeth Kempf *(University of Chicago)*
- Marie Lambert (University of Liege
- Jacopo Bregolin *(TSE)*
- Xavier Gabaix *(Harvard)*
- Melissa Prado *(Nova School of Business and Economics)*
- Junyuan Zou *(INSEAD)*
- Kim Oosterlinck *(Université Libre de Bruxelles)*
- Simona Abis *(Columbia Business School)*
- Maria Guadalupe *(INSEAD)*
- Radoslawa Nicolowa *(Queen Mary University of London)*
- Gyuri Venter *(University of Warwick)*
- Huan Tang *(LSE)*

Sustainable Finance Center

Toulouse School of Economics

Main donors

Donors

Research project sponsors

- Ant Financial
- Axa
- BBVA
- Banque Centrale du Luxembourg
- Banque de France
- Chaire FDIR
- SCOR

Publication director: Sophie Moinas
Production Manager: Tiffany Naylor
Editorial contributions: James Nash
Graphic design and layout: Olivier Colombe
Photos: StudioTchiz, Boris Conte, I-Stock, Banque de France, VMware.

Toulouse School of Economics
1, Esplanade de l'Université
31080 Toulouse Cedex 06
Tel: +33 (0)5 67 73 27 68
www.tse-fr.eu / partnership@tse-fr.eu