Encryption to implement mechanism design solutions

by

Nicolas Xuan-Yi Zhang
Diplôme d'Ingénieur, École des Mines de Paris (2017)

Submitted to the Institute for Data, Systems, and Society and
the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degrees of
Master of Science in Technology and Policy
and
Master of Science in Electrical Engineering and Computer Science
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2021

Author
……
Institute for Data, Systems, and Society
Department of Electrical Engineering and Computer Science
January 15, 2021

Certified by ……
Robert M. Townsend
Elizabeth & James Killian Professor of Economics
Thesis Supervisor

Certified by ……
Vinod Vaikuntanathan
Associate Professor of Electrical Engineering and Computer Science
Thesis Reader

Accepted by ……....
Noelle Eckley Selin
Director, Technology and Policy Program
Associate Professor, Institute for Data, Systems, and Society,
Earth, Atmospheric and Planetary Sciences

Accepted by ……....
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

Encryption to implement mechanism design solutions

by

Nicolas Xuan-Yi Zhang

Submitted to the Institute for Data, Systems, and Society and the
Department of Electrical Engineering and Computer Science on January 15th, 2021,
in partial fulfillment of the requirements for the degrees of
Master of Science in Technology and Policy and
Master of Science in Electrical Engineering and Computer Science

Abstract

Encryption - the process of encoding information - mitigates the damage that comes from obstacles to exchange: private information, limited communication, and limited commitment. Here I would emphasize specifically that encryption is a way to implement optimized solutions to bilateral and multi-agent mechanism design problems as smart contracts. To illustrate how such encryption schemes could be relevant to economic applications, I first revisit "classical" problems such as auction design with private values, constrained-optimal hybrid insurance and credit schemes for markets suffering from liquidity problem. The common thread in each of these applications is that messages are kept secret from other agents in a contract and from third parties, communication channels are optimized, and data are secured and immutable. Agents can commit to arrangements and to the way they are implemented, without inconsistencies, even in evolving situations where they would have liked to renege. I make use in particular of homomorphic encryption, HE, and multi-party computation, MPC, which I will describe in details in the text and concretely implement.

I will first decompose and examine the different technological components of encryption, to, by "translating them" into individual tools that I implement for the aforementioned cases, present here a "cookbook" on how to use cryptography technologies to implement mechanism design solutions. I will always keep in mind the various possible combinations of technologies and the engineering trade-offs associated to each, in the hope that economic and policy designers will be able to adapt these recipes to design new solutions to the problems they will be facing.

I then provide a more in-depth example of an "end to end" treatment of a complex economic topic, that of fiat monetary anchoring. I will model it using our mechanism design framework, calibrate it through empirical analysis, and propose concrete policies and designs, leveraging encryption.

Thesis Supervisor: Robert M. Townsend
Title: Elizabeth & James Killian Professor, MIT Economics

Thesis Reader: Vinod Vaikuntanathan
Title: Associate Professor, Department of Electrical Engineering and Computer Science

Acknowledgements

This document is the final fruit of a few chance encounters, and emerged from fortuitous ideas formed between people from different backgrounds and academic fields. Somehow, we all happened to meet at the right time in our different life paths, and managed to "stick" together and put in the work and efforts to understand each other's cultures, methods and perspectives, to finally create a framework and language that could be understood by researchers from both fields, and hopefully by the public at large – the targeted audience of this very document.

This gestation has only been made possible by MIT's extraordinary diverse community, fertile work environment, and unconditional support - that shielded us from the various shocks and distractions that could have made one's life bifurcate (and God knows how tenuous is a 20-something's attention, and what challenges the year 2020 exhibited!)

Within the MIT community, my acknowledgement would first go to the Technology and Policy Program, which accepted here in the first place. Specifically, I would like to emphasize what an extraordinary, multidisciplinary, yet intimate environment it provided – along with all the support and protection one could have hoped from a "family".

Barb – thank you for putting up with all the bumps on my journey here, always with a smile (a laugh often!) and infinite patience.

The same patience I found in Frank as well, with sometimes a little derision in it, that makes every situation appear less dramatic (at least to me). And for the great readings in your class, which I will think about oftentimes (especially, as I am about to graduate and go out in the world – on that about the "policy entrepreneur" and on the "engineer as designer"!).

Noelle – for your continuous understanding, for having taught us (one of) the roles of "honest broker" in policy, which guided this thesis, and for the unconditional support for the program and Technology and Policy overall.

Ed – for the great French conversations when I'd be homesick, and for the expert guiding through the streets of Boston (which I then took along with others – including fellow TPPers and roommates!). And, to all TPPers and friends – Benny, Maryam, Brandon, the SidPac/Ashdown crew!

Then, I would like to thank my lab mates and colleagues at CSAIL, and at the Internet Policy Research Institute. Thank you for having hosted me (and all my stuffs!) for these past two years, for having taught me how-to better my coding, and for all the serendipitous conversations on everything in life – from NASA's old school computer systems and farms with Jeff, to international organization and career planning with Taylor. And, for helping me navigate CSAIL from TPP – Nathaniel (the first TPPer I ever met in person!). Also, to my project members on SCRAM – Taylor, Danny, Professor Lo and Professor Vaikuntanathan, Susan, Leo. I will keep fond memories of late evenings and weekends setting up demos in Samberg center, along with the events themselves.

Finally, I would like to thank with equal fondness my family, my advisor Professor Townsend, and my fellow TPP roommates Karan, Himani (honorary TPPer), Frank, and Gabe (and Vivienne and Boyu and Lydia – you guys are part of the club as well! With a special mention to Charlotte who has been here from the very start to the very end of my MIT journey – Paris' airport departure to US departure). Your differences in academic backgrounds and in perspectives, were all the indispensable ingredients (spices!) that made my life flavorful, and that hopefully produced digestible food for thoughts. I can't thank you enough for the continuous support and stimulation over these years.

Table of Contents

Part I:
Innovative financial designs utilizing homomorphic encryption and multiparty computation

This Part has been the fruit of joint work with Professor Townsend, and is also being published as a working paper on https://www.leadmit.com/publications. I refer readers to that link for updates and improvements made to it subsequent to my MIT graduation.

Chapter 1 – Our design methodology: understanding cryptography technologies, and leveraging them (selectively) as new design possibilities

Financial systems can be viewed as systems allowing agents to enter into contracts. However, contracts are not-single dimensional (e.g., more or less money); the more contingencies financial systems can deal with, the more efficient and resilient they become. These contingencies are notably constraints generated by (1) untrusted messages - crucial for instance in the counting of ballots, or of auction bids -, by (2) unobserved actions - ex- acerbating risks from counterparties, settlements, and commitments), or by (3) unobserved states - while estimating competitors' bidding power and valuation of the good sold in an auction for instance. I will see in a range of applications how these issues can be raised, and how uncertainties, commitment issues and secrecy cause distortions and lead to asymmetric allocations.

Encryption, as the science of protecting messages' content and authenticity, while securing senders and receivers' identities and privacy, enables a large toolbox for economic design. I will then see how additional guarantees on authenticity, on commitments and enforcement of contracts can help solving the issues raised above. Moreover, I will also study how a wider range of public-privacy states of information and the ability to perform computations over encrypted data (thus preserving their secrecy) can fundamentally improve the design of financial contracts in linking agents' differing preference and risk profiles (the unobserved states that play a crucial role in mechanism design). I will thus be able to introduce flexible hybrids contracts, in between pure borrowing/lending and pure insurance contracts.

I follow three steps in the design of these new economic systems. First, I decompose and examine separately the different technological components of encryption, to" translate them" into

individual tools formulated within the usual mechanism design environment (de- scribed in the following section). Second, having these new economic design tools at our disposal, I ”revisit” several classical economic problems (such as the ones mentioned above - auctions, borrowing/lending, insurance...) and craft the incentives and constraints that have to be put in place or lifted for an improved contract to be designed, in an objectives- first and context-dependent approach (there can be different goals and values for a contract to aim to implement, and each economic application presents a different environment for the contract to take into account). Finally, I show how this contract devised in the abstract language of mechanism design can be implemented in real life using different combinations of existing technologies - each of them implementing the correct set of incentives, but potentially presenting different engineering trade-offs that I try to highlight. This way, our contribution will be to present an end to end” cookbook” on cryptography technologies to implement several mechanism design solutions. I hope to provide inspiration and methods for economic and policy designers to be able to leverage the right cryptography tools to design the right solution to the specific problems they will be facing.

Chapter 2 – The Mechanism Design Framework

In general, at an abstract level, an economic application is laid out in terms of preferences of the agents, their endowments, and the technology available to them. In fact, to examine the extent to which different historic forms of economic contracts and organizations can be explained by information-incentive problems, and to explore how to improve these contracts and organizations, it is useful first to retreat to the abstract setting of the exchange and endowment economy, in which I add constraints related to the flow of in- formation - for instance that an agent’s preference is fully

private and not observable, or that his endowment or output are not observable (at least not without considerable cost). These information related constraints are key in demonstrating how a seemingly imperfect form of organization was actually the best implementable possible, given the technologies of the time. Related, new technologies that allow to relax some of these constraints on the flow of information (such as homomorphic encryption and multiparty computation explored in the next subsection, which allow computations to run in a privacy-preserving fashion, guaranteeing each individual input's secrecy) can potentially lead to better implementable mechanism design solution. Townsend JME 1988's findings on limitations introduced by publicly communicated messages provides for instance guiding on the gains that could be collected from using privacy-preserving computation technologies.

For instance, Townsend, R. M. (1993). The medieval village economy: A study of the Pareto mapping in general equilibrium models. Princeton, N.J: Princeton University Press laid out the problem in the settings of a medieval village economy, in which many villas had been obligated to pay a fixed rental to lords or monasteries, that could be spread out at a considerable distance from each other. However, the prime determinant of output, the weather, was not uniform over space, and how well a particular villa did in a particular year may not have been known by monastery officials without a costly verification (one might call that an "audit"). So full insurance is not feasible here, as there would be too many possibilities for the villas to cheat the monastery without systematic (costly) auditing. Interestingly, that medieval setting is not so different from that governing most economic environments today, and some of the key results derived in that setting are also very much applicable. For instance, in a repeated interaction setting, borrowing and lending is not optimal - since changing a villa's "rent" as a function of past observables would lead to Pareto improvements for both the villa

and its owner. Hence in many cases, the information constrained optimum is a hybrid of credit and insurance (which I will see again in section 5).

Finally, though typically one thinks of models at the level of goods and direct utility functions, the modeling frame applies to securities and indirect utility functions for asset holdings. An application can include time (dynamics), uncertainty (private and public states of the world), and geography (assignments). All private information aspects are captured by parameter vector θ. A mechanism is a mapping from θ to allocations to the agents. A constrained-optimal mechanism maximizes ex ante expected utilities of agents subject to resource constraints (adding up) and incentive constraints (truth telling and obedience). However, mechanism design assumes implicitly the existence of a neutral "planner" as implementer.

(a) To trust a third party or not

Trusted third parties have been the institutional solution to problems arising from untrusted messages, unobserved actions and unobserved states. For instance, auditors are mandated to certify the veracity of a claim or of a ledger (problem 1), while notaries record transactions or commitments to conduct a transaction to make it final (problem 2). For sensitive information held by private firms as in problem (3)," neutral" regulators, researchers or organizations such as the BIS are entrusted to access them when they are needed part as part of bigger studies or policies.

However, trusting a third party gives him the possibility to misuse or steal the information entrusted to him, and to misexecute the operation he has been mandated to conduct, by accident or knowingly.

For instance, the numerous reports of frauds in BWIC (bid-wanted-in-competition) auctions (see for instance United States v.Litvak and United States v. Garmin which illustrate cases of manipulative auctioneers that hijacked the messages as in problem (1) mentioned above). There, dealers are being asked to bid on listed securities. A typical potential abuse: run over the telephone, the seller of the asset in question who is the organizer of the auction tells buyer A : "I prefer you my friend, but buyer B just offered a slightly higher price, so if you can just make some effort the good is yours". Vice versa with buyer B to prop up the price. Neither buyer A nor B can check the bid of the other buyer. Even in the case of normal auctions, what actually distinguishes a "good" auctioneer (and "good" ones are in fact highly sought after) is his ability to entertain and "manipulate" the crowd to get people excited, and maybe bid higher than one would have had under other circumstances.

Similarly, in financial transactions collateral or escrow held by a third-party guarantor can be used to mitigate counterparty risks, and prevent adverse unobserved actions as in problem (2) mentioned above. However, this implicit insurance comes at the cost of brokers potentially charging abusive markups and committing fraud (see for instance Grandon v. Merrill Lynch Co Inc.).

Finally, collusion between the third parties entrusted to audit the unobserved (or hard to observe) states of a private firms (problem 3 mentioned above) can lead to even bigger and more systemic fraud (from Enron, to the general misrating of financial instruments prior to the 2008 Great Financial Crisis). In some cases, it might not even be possible to set up such a third party, as private information is too sensitive to a country or a firm's strategy.

And, beyond the risks associated with trusting a third party, and the impossibility to obtain a perfect institutional solution given unobservable or untrusted information, the sheer costs associated with the set up of a "trustable" third party are often what prevented developing countries from building sound financial systems that would better support its agents to grow (see Townsend's 2012

IMF keynote reviewing the relevant literature[1]). Lowering its costs could then also lead to significant improvements in growth and development.

(b) Authentication and commitment with public-key cryptography

Public-key cryptography would solve in many instances the problems arising from un- trusted messages, unobserved actions and unobserved states. Let's first see how this asymmetric form of cryptography works. The key research question that leads to these solutions was how to get a secure conversation over an insecure line, when the two people in the conversation have never had previous contact. Obviously, if the two people hadn't known each other previously they would have had no opportunity to exchange secret keys before a private conversation. Indeed, until Whit Diffie's public key cryptography innovation, there was a set of assumptions that guided most cryptographic implementations. One of those was that the same key that scrambled a message would also be the instrument that descrambled it. This is why keys were referred to as symmetrical, and why keeping those keys secret was so difficult: the very tools that eavesdroppers lusted after, the decryption keys, had to be passed from one person to another, and then exist in two places, dramatically increasing the chances of compromise. Therefore, the original research question, formulated differently, would be on whether it is possible to create a system where people who had never met could speak securely, and in which one could get an electronic message from someone and be sure it came from the person whose return address appeared.

Under Whit Diffie's design, instead of using one single secret key, one could now use a key pair. The symmetrical key would be replaced by a dynamic duo. One would be able to do the job of scrambling a plaintext message — performing the task in such a way that outsiders couldn't read it —

[1] "Financial deepening, macrostability and growth in developing countries", accessible at literature https://www.imf.org/external/np/seminars/eng/2012/spr/pdf/rt.pdf

but a secret trapdoor (see appendix on one-way functions) would be built into the message. The other portion of the key pair built on this one-way function is then like a latch that could spring open that trapdoor and let its holder read the message. Notice that the core principle of this scheme is that the second key - the one that flipped open the trapdoor — was of course something that had to be kept safe from the prying hands of potential eavesdroppers. But its counterpart - the key that actually performed the encryption - didn't have to be a secret at all! In fact, one wouldn't want it to be a secret, and would be happy to see it distributed far and wide. This is why that part is called the public key. The second key that flipped open the trapdoor is called one's private key.

Therefore, by presenting an alternative to systems that worked with a single, symmetrical key, Diffie had solved one of the biggest problems of his time - the difficulty of distributing keys to future recipients of secret messages. In fact, if one is say a military organization, one might be able to protect the distribution centers that handled symmetrical keys (though we know that there are lapses even in the most vital operations). But if such centers moved into the private sector, and masses of people needed to use them, there would not only be inevitable bureaucratic pileups but also a constant threat of com- promise. Indeed, if one needs to crack an encrypted message, wouldn't the very existence of a place that stored all the secret keys present an opportunity for theft, bribery, or some other form of coercion?

But with a public key system, every person could generate a unique key pair on his or her own, a pair consisting of a public key and a private key. The public key can be distributed out and wide, while no outsider would have access to the secret key. Then, private communication could begin using these two asymmetric components.

Here's how it would work: Say that Alice wants to communicate with Bob. Using Diffie's concept, she needs only Bob's public key. She could get this by asking him for it, or she might get it from some phone-book-type index of public keys. Then she uses that public key to scramble the

message in such a way that only the private key — the other half of that unique key pair — can perform the decryption.

So, when Alice sends the scrambled message off, only one person in the world has the power to reverse the scrambling and decipher it: Bob, the holder of the private key. With- out that private key, reversing the mathematical encryption process is too difficult or slow, given the security assumptions of the specific implementation of the one-way functions chosen (though in image, one can say that going the wrong way in a one-way function is like trying to put together a pulverized dinner plate). Those who obtain the public key have no advantage in attempting to break the message. When it comes to encrypted messages, the only value of having Bob's public key is to, in effect, "translate" any message to a language that only Bob can read (by virtue of having the secret half of the key pair).

Bob then has no problem reading the message intended for his eyes only. He possesses the secret part of the key pair, and he can use that private key to decipher the message in a jiffy.

This encryption function was only part of Diffie's revolutionary concept, and not necessarily its most important feature. Public key cryptography also provided the first effective means of truly authenticating the sender of an electronic message. As Diffie conceived it, the trapdoor works in two directions. First, as we have seen, if a sender scrambles a message with someone's public key, only the intended recipient can read it. But if the process is inverted — if someone scrambles some text with his or her own private key — the resulting ciphertext can be unscrambled only by using the single public key that matches this private key. Therefore, if you receive such a message from someone claiming to be Albert Einstein, and wondered if it was really Albert Einstein, you now had a way to prove it — a mathematical litmus test. You can look up Einstein's public key and apply it to the scrambled ciphertext. If the result is a message in plaintext and not some gibberish, you'd know for

certain that it was Einstein's message — because he holds the world's only private key that could produce a message that his matching public key could unscramble.

In other words, applying one's secret key to a message is equivalent to signing your name: a digital signature. But unlike the sorts of signatures that are penned on bank checks, divorce papers, and baseballs, a digital John Hancock cannot be forged by anyone with the minimal skills required to replicate the original signer's lines and loops. Without a secret key, the would-be identity thief has scant hope of producing a counterfeit signature.

This technique also assures the authenticity of an entire document. A foe can- not hope to change a small but crucial portion of a digitally signed document (like switching the statement "I take full responsibility for my spouse's debts" to "I take no responsibility for my spouse's debts" all the while maintaining the signature of the unwitting sender). Indeed, let's suppose that such a message was signed using the original issuer's signature, then sent out in the open. The attacker could intercept it, use the sender's well-distributed public key to descramble it, and then make the change in the plaintext. But then what? In order to resend the text with the proper signature, our forger would require the private key to fix the signature on the entire document. That secret key, of course, would be unobtainable, remaining in the sole possession of the original signer.

If someone sending a signed message wanted secrecy in addition to a sig- nature, that's easy, too. If Mark wanted to send an order to his banker, Lenore, he'd first sign the request with his private key, then encrypt that signed message with Lenore's public key. Lenore would receive a twice-scrambled message: shaken for privacy, stirred for authentication. She would first apply her secret key, unlocking a message that no one's eyes but hers could read. Then she would use Mark's public key, unlocking a message that she now knows only he could have sent.

Digital signatures offer another advantage. Since it is impossible for a digitally signed message to be produced by anyone but the person who holds the private key that scrambles it, a signer cannot

reasonably deny his or her role in producing the document. This nonrepudiation feature is the electronic equivalent of a notary public seal.

(c) Smart contracts (with or without distributed ledgers) to automatically enforce commitments

”Smart” contracts can further the extent of which public-key cryptography solves problems arising from untrusted messages, unobserved actions and unobserved states. Indeed, one can combine the authentication and commitment schemes described in the previous subsection with an automated execution engine (such as that operating transactions on a distributed ledger - but it could also be just computer code without consensus algorithm, or even trusted third parties operating escrow accounts), so that settlement uncertainty and counterparty risks can be better mitigated. For instance, one concept of interest combining both public-key signatures and automated contracts would be that of atomic swaps. To simplify, these contracts make use of a multisignature transaction system (called hashed timelock contracts) that holds both traders accountable for a swap to be successful. Traders are only allowed to access funds once both parties have signed off on their respective transactions using their private keys, and a ”timelock” is added as an insurance policy that ensures that both users will have their funds returned to them if the trade is not successful under a specific timeframe. Hence, these atomic swaps are transactions that can only fully succeed or nothing happens[2].

[2] There are also more ”exotic” applications built on it, such as ”flash loans” - in which people make use of such swaps to borrow money and conduct arbitrage-type transactions with it, at supposedly zero default and illiquidity risk for the lender. However, this has more to do with the fact that time on many blockchain is discrete (in ”blocks”) which is why such a borrowing-arbitrage-reimbursing sequence can be seen as a swap, and hence cannot be reproduced outside of the blockchain world. Even within, this type of flash loans opened the doors to massive attacks again vulnerabilities within blockchain protocols, that can be seen as arbitrage opportunities. Again, I emphasize the importance of being clear on the economic incentives created by different engineering implementations, to evaluate the feasibility and value created by any technological design.

(d) "Decentralizing" the trusted third party through homomorphic encryption and multiparty computation

This solves problems arising from the unobserved states mentioned above. I will lay out some mathematical principles key to MPC and HE here, and reference these in the detailed examples in subsequent sections to highlight how it translates to engineering design.

The key property of homomorphic encryption, HE, is that a function f can operate on a true underlying space or equivalently operate on the space of encrypted (i.e. encoded) values. That is, in order to utilize a function f in some application, one does not need to input the "plaintext" information which reveals the original and true values of a given agent, but rather, one can encrypt the agent's data, so that data can be kept private, apply the same function f on encrypted input data, get a result in the encrypted space, and all of this is the same as if the message had been true private values and the output from f were encrypted. That is f(Enc(m)) = Enc(f(m)) . Equivalently, what we want in normal space is on the right but the way to get it is in the encrypted space on the left of this equation: Decipher[f(Enc(m))] = f(m). Note that this is for one agent, one message at a time, in contrast to MPC below for multiple agents (but which is less flexible). **Further, the "distributivity" of the encryption operation with the function operation gives flexibility in navigating between the normal space and the encrypted space** (see concrete examples of such "navigation" in sections 3, 4 and 5). The distributive property is telling us what rules manage the parenthesis that order the sequence of operations - a distributive scheme allows operations outside the parenthesis to be "distributed" to the elements within, whereas a non-distributive scheme doesn't allow such treatment of the parenthesis. This allows us to per- form a series of composed transitive functions g all on top of the encrypted message, as on the left: g[f(Enc(m))] = g[Enc(f(m))]. Thus, the agent or contract performing all the functions never gets to see the actual content of the message, nor the true outcome of f in the normal space. And thus, through agents sending encrypted messages back and forth

between, with each of the agents re-encrypting the message before sending it back, allows computations to be conducted, while preserving the privacy of the initial message (in subsections sections I will write in parenthesis "distributivity" next to steps in which this property is used).

The key property of multiparty computation, MPC, is that rather than determine the value of a linear function f using inputs values from multiple agents, seeing the inputs and the result of f directly, in normal space, one can run the function f on encrypted private inputs, then decrypt the output value or relevant summaries, and finally share that result. Namely, for J agents Decipher[f(c_1, c_2,..., c_J)] = f(m_1, m_2,..., m_J)] where (c_1, c_2,..., c_J)=Enc(m_1, m_2,..., m_J) are the encrypted values of the inputs from m different agents. Distributivity of MPC fails, and we can't compose transitive functions g on top of f - ie Decipher[g(f(c_1, c_2,..., c_J))] ≠ g[f(m_1, m_2,..., m_J)]. But combining MPC with HE, we have what MPC means plus the distributivity in operations - ie the inequality above becomes an equality.

Further, we now have flexibility in choosing how many agents need to agree in order for the result to be decrypted. In pure MPC all J agents need to agree. But in HE+MPC any number of agents k between 1 and J can be chosen - prior to the computation - to allow for decryption. The point more generally: what to reveal as public in both HE and MPC cases becomes a choice element of the design.

Other aspects of encryption such as multi party signature schemes, cryptographic puzzles, hashes, and Merkle trees are more familiar and more widely utilized, notably in the distributed ledger community. We also rely on these in some applications, as well, but I take pains to clarify exactly what is needed, utilizing the best available technology. We do not force financial applications onto a given technology, but go the other way around, starting with the economics.

Chapter 3 – An example of improvement replacing the trusted third parties - auctions without auctioneers

To see an online interactive tutorial guiding through this example, please visit the following Jupyter Notebook http://bit.ly/FHEauctions

Generally, auctions are used frequently but are organized typically by a third party, as in Mortgage Capital Trading's use of a Trade Auction Manager. However, trusted third parties are not always needed, and not always beneficial. In the previous example of current bid-wanted-in-competition schemes, BWIC, dealers are being asked to bid on listed securities. A typical potential abuse: run over the telephone, the seller of the asset in question who is the organizer of the auction tells buyer A : "I prefer you my friend, but buyer B just offered a slightly higher price, so if you can just make some effort the good is yours". Vice versa with buyer B to prop up the price. Neither buyer A nor B can check the bid of the other buyer. Some of China's P2P platforms also presented misleading information to investors or engaged in AI cream-skimming in the creation of securitized pools. Trumid, on the other hand, markets itself as a Wall Street company with an algorithm intended to replace OTC dealers who are thought widely to trade on the proprietary information of their clients.

However, companies like Trumid are "replacing" OTC dealers by being more efficient and better trusted third parties. However, I argue here that these improvements could be brought further, by totally "getting rid" of the trusted third party. There are for instance several ways to implement our auction-without-auctioneer scheme with HE and MPC. Let's give one example here, building on lattice cryptography (so that this is post-quantum secure, ie secure against attacks from quantum computers, when they will exist), using the mathematical and security properties of the Ring-Learning with Errors (RLWE) model. Note that many of the mathematical properties I make use of, such as commutativity, comes from those of mathematical Ring. However, for the purpose of our exposition

here to be self contained, let's see simplify and see all elements drawn from these Rings as polynoms, for which the commutativity and distributivity properties are verified. The complexities in the theory of rings and lattice cryptography concerns more public and secret key generations and operations on them, but one can first put these parts aside for the rest of this exposition, since I start from a point in which the right polynoms with the right properties (commutativity and distributivity) have already been drawn and built, and I am more interested in how they can interact with each other in a privacy-preserving and homomorphic way. For the avid reader more details can be found on the general homomorphic encryption scheme I adapted here in Brakerski (2012) and Fan and Vercauteren (2012) - hereafter and in the literature called the BFV scheme. The specific key generation protocol and corresponding decryption protocol I make use follows the work of Asharov et al. (2012), of which no understanding is necessary here to follow the mathematical operations I describe below.

Step 0. Distributed Key Generation

Let's run our example with two agents, A and B, who want to see whose bid is higher and whose is lower, without relying on a trusted third party but without revealing to each other the exact value of each one's bid.

Consider the standard BFV key generation protocol, which outputs a public-key (pk)/secret-key (sk) pair of the form

$$(pk, sk) = \big((a, \delta), (\ s, e)\big) \tag{1}$$

where a and δ are two uniformly random samples over the ring $R_q = Z_q[x]/f(x)$ where $f(x)$ is some degree-n polynomial. The error term e is sampled from a discrete Gaussian with large standard deviation (such noise terms are sometimes referred to as 'flooding' or 'smudging' terms). Our key generation protocol relies on the common random string (CRS) model and begins with the assumption that all participants have access to the same truly random seed for a pseudorandom number generator

(PRNG). All participants then use this seed to generate the same pseudorandom sample a from R_q. Each party i then generates the following key pair:

$$(pk_i, sk_i) = \big((a, \delta), (\ s_i, e_i\big) \tag{2}$$

So agent A has the following key pair :

$$(pk_a, sk_a) = \big((a, \delta), (\ s_a, e_a)\big) \tag{3}$$

And agent B the following key pair :

$$(pk_b, sk_b) = \big((a, \delta), (\ s_b, e_b)\big) \tag{4}$$

Step 1. Multiparty encryption of each agent's bid

Now that each agent has its unique secret key, while sharing a public key, they can start using these to encrypt their bids. To describe this encryption process I will follow a sequential description, even though the actual order of the sequences doesn't matter (both can even happen at the same time).

So A (let's say A starts, even though it would be the same if it's B first): A sends to B its bid m_a, obfuscated by its secret key s_a, in the following encrypted message (let's call it ct_a , for ciphertext from A) :

$$ct_a = a \cdot \ s_a + \delta \cdot m_a + e_a \tag{5}$$

B cannot guess (from the security proof of the BFV scheme) the value of A's bid m_a. He sends similarly his encrypted bid m_b to A (let's call it ct_b , for ciphertext from B) :

$$ct_b = a \cdot \ s_b + \delta \cdot m_b + e_b \tag{6}$$

Step 2. Multiparty addition of each agent's bid

Let's make each agent "add in" his own secret key to the encrypted message he received from the other party. Ie, for agent A, do the operation

$$a \cdot \ s_a + e_a + ct_b \tag{7}$$

and for agent B the operation

$$a \cdot \ s_b + e_b + ct_a \tag{8}$$

So now agent A has the new ciphertext, by writing

$$e_a + e_b = e, \tag{9}$$

and

$$s_a + s_b = s \tag{10}$$

$$ct_b\prime = a \cdot \ s + \delta \cdot m_b + e \tag{11}$$

And agent B has the new ciphertext

$$ct_a\prime = a \cdot \ s + \delta \cdot m_a + e \tag{12}$$

And, if both of them resend the ciphertext each one had of the other, then both can do the operation

$$ct_a\prime - ct_b\prime = ctFinal = \delta \cdot (m_a - m_b) \tag{13}$$

, the sign of which reveals which agent's bid was higher at the start.

Let's note that here with only 2 agents this is a limit case that would reveal, by difference, each agent's bid value to each other. For strictly more than 2 agents, this wouldn't be a problem unless all but one agent coordinate and share their inputs, in which case they can also infer the input from that last agent as well. For just 2 agents, let's see now how δ can be a value kept secret to each other, hence hiding the real value of both agent's bid.

Using the 2 agents case to introduce the concept of "pseudo agent" nodes

We have the previous setting with agents A and B. Let's now introduce a "pseudo agent" C, which can be for instance a server that has been jointly set up by A and B, and then left as a "deterministic box" on its own (I use the "deterministic box" image of some box that has been pre-

coded to do some things, and that then can be guaranteed to do it, even if no one audits what is going on inside). In a distributed ledger language, C would be a smart contract node. But here I present a more general case than just DLT-based smart contract. This node will be very useful in the generalization work presented later in the document.

A and B still have the following key pairs :

$$(pk_a, sk_a) = \big((a, \delta), (\, s_a, e_a)\big) \tag{14}$$

and

$$(pk_b, sk_b) = \big((a, \delta), (\, s_b, e_b)\big) \tag{15}$$

However, now in **step 1** both A and B send their ciphertexts to C, instead of to each other. C also asks both A and B to send the following combination of A and B's public and private keys (let's call them nn_a and nn_b for "not so random noise from A" and "not so random noise from B") :

$$nn_a = a \cdot \ s_a + e_a \tag{16}$$

and

$$nn_b = a \cdot \ s_b + e_b \tag{17}$$

.

nn_a and nn_b have sufficient cryptographic properties (as in BFV) to conceal A and B's private keys (s_a, e_a) and (s_b, e_b), while allowing C to decrypt ct_c , where ct_c is obtained through C adding the two ciphertexts ct_a and ct_b he received from A and B. I.e.

$$ct_c = ct_a + ct_b = a \cdot \ s + \delta \cdot (m_a + m_b) + e \tag{18}$$

. Indeed, we have :

$$nn_a + nn_b = a \cdot \ s + e \tag{19}$$

so that

$$ct_c - (nn_a + nn_b) = \delta \cdot (m_a + m_b) \tag{20}$$

Similarly, C can just do the operation $ct_a - nn_a - (ct_b - nn_b) = \delta \cdot (m_a - m_b)$. And, since I assume that C has "pre-coded" in him :

- "STEP1 TAKE INPUT 1 FROM A, SUBTRACT INPUT 2 FROM A.

- STEP2 TAKE INPUT 1 FROM B, SUBTRACT INPUT 2 FROM B.

- STEP3 TAKE RESULT FROM STEP1, SUBTRACT RESULT FROM STEP2.

- IF RESULT FROM STEP 3 IS POSITIVE THEN AGENT A WON THE AUCTION. ELSE AGENT B WON THE AUCTION."

Then C can just announce to both A and B who won, with A and B never seeing anything else than the "not so random noises" and ciphertexts each of them sent to C, which do not reveal their bid values.

Going back to the BWIC auction example, in which the seller of an asset organizes an auction scheme, one could apply the homographic encryption scheme I laid out above to limit the seller's incentives to misreport. Then, each buyer's bid will be encrypted by him using his unique secret key, to prevent anyone else from tampering with it (especially the seller/organizer of the auction, who agrees to not possess each buyer's individual secret key). Furthermore, the organizer of this BWIC auction agrees to only provide the matching (or ranking) operation of this auction, performed homomorphically on top of each buyer's encrypted bid, as "pseudo-agent" C above does. The encrypted bids thus protect buyers' privacy in both keeping it untampered, and by keeping them anonymous, to reduce potential conflict of interest and collusion between the organizer of the auction and some participants (if the public/private keys are allocated randomly to each participating agent).

Some decryption may come at the end if the winner needs to be revealed. The as- set purchased might be on a distributed ledger with the transfer executed under a smart contract, but this part is separate and is not necessary per se. An alternative, a third party might be trusted to make the asset transfer. Both are an option, a choice for possible auction designs.

Chapter 4 – An example of improvement replacing the central planner - in flexible, hybrid contracts between borrowing/lending and insurance

In the previously described auction scheme, the secrets, the underlying messages be- fore encryption, need never be revealed to other agent or an institution performing the matching/ranking operation. With HE, encrypted inputs can be kept private and still contribute to operations performed homomorphically on top of them. This is what I call the" private-but-contributing-state-of-information". I now make full use of this" private-but-contributing-state-of-information" to tackle one of the core problems in mechanism design - that surrounding the treatment of private information held by agents, which are needed to convince its counterparties of its truthfulness and secure their commitment, but which cannot be fully revealed for fear of some counterparties exploiting the information. One such example is that of the borrowing/lending and insurance literature. The contract is a hybrid in that it has aspects of both. In interbank lending markets for instance, banks try to buy or sell specific amounts of liquidity, that are linked to their funding needs. If all banks real funding needs were known, some optimal distribution and pricing schemes could be devised. However, if anyone of these banks accessed some others' real funding need, they would gain negotiation power and could exercise leverage with this knowledge, or sell the information to others.

Townsend, JME 1988 presents for instance a schematic case between two agents, one can be thought of as a potential borrower but with varying needs and the other who is on the other side of the trade, the lender who in turn has varying needs at the time of repayment. the two agents agree in a first-time step what the amounts that will be borrowed in the second time step, depending on the realization of a shock. However, to keep privacy as to whether the borrower is in a high or low liquidity need, "a layer" of scrambling will be added for the lender not to be able to infer for sure if the borrower

is in the high or the low liquidity situation. This scheme exhibits the full power of encryption, as here it is even harder to conceal agents' "bids" than in the auction case presented before.

The context includes a variety of payments arrangements. For example, money transfer organizations run short of liquidity, of one object or another, and would benefit from a more organized or improved market. In Kenya, agents for Safaricom are frequently running out of fiat Shillings or M-Pesa, seeking gifts or loans informally from other agents. In Indonesia agents acting on behalf of banks in towns and rural areas are also typically short of liquidity, want to rebalance, but complain it is difficult to do so. Broker dealers as agents in New York markets have their own liquidity problems, and despite borrowing and lending though repo markets, participation is segmented and interest rates have moved erratically, counter to policy rates.

One can view agent specific shortages in these contexts as idiosyncratic shocks, for which ex ante insurance would be good. But revealing those shocks over time too quickly can damage the possibility of beneficial trade. Though a simplified analogy, this is much as with standard insurance, in which ex ante insurance possibilities are lost once the ex post adverse event has occurred. This is known to be a problem in the foreign exchange markets in the sense that information on trades should not be revealed too quickly.

These applications can be cast as mechanism design problems that feature concealment, that is keeping private messages private but utilizing these as inputs to generate outcomes. For example, two agents have utility functions subject to privately-observed preference shocks. The first agent in the first period, agent a, can be patient or urgent to consume, private knowledge, and likewise for the second agent in the second period, agent b. The 'planner', to use the standard language of mechanism design, sees the messages that each of the two agents sends, but makes sure the other agent does not. Incentives to tell the truth in the second period are easier to muster if the sender in the second period, agent b, does not know what message was sent by agent a in the first period. The information-

constrained optimal allocation is such that lying in the second period generates a very bad outcome for the sender with positive probability.

But we do not rely on this mythical central planner. Let's examine now how one would build such a scheme without him.

Implementation notes for the hybrid borrowing lending case without central planner

Let's use the same setting as the previous auction between two agents : we thus have agents A and B, and "pseudo agent" C. I introduced "pseudo agent" C here to help conceal a new elements of privacy - we now want to protect the "actual message" sent by agent A at time step 2 (conceptually similar to protecting a bid value), but we also need to compare that value with preset values WHICH ALSO HAVE to be protected (as we don't want B or C to be able to retrospectively guess from the value transferred what the "actual message" sent by agent A at time step 2 was. This is done through randomization as de- scribed above, but also through another layer of homomorphic encryption and decryption enabled by interactions between A and C, and between B and C, in addition of the interactions just between A and B. See for instance the summary schematic view I draw below detailing how messages exchange between A, B and C happen, and how information can be concealed by being encrypted by one agent but still used in computations by another agent even while being encrypted).

The economic framework is that of Townsend, JME 1988. To summarize, agents A and B negotiate a risk pooling contract over two periods, time step 2 and time step 3. There is also an initial contract setting at time step 1, and at the end of which they put their initial assets as endowments into escrow. In period two A sends a message - either h_A, in the case A has a high need for liquidity, or l_A, in which case A has a low need for liquidity. The "central planner" as in Townsend, JME 1988 then takes this message, and requests money from B or vice versa accordingly (with some randomization going on if the message is h_A, for B not to be able to retrace with certainty what A sent in the first place).

Here the ”central planner” is replaced by the ”pseudo agent” C. The scheme goes as follows:

Step 1. At time step 1, contract setting step

Agent A sends messages $\mathrm{Enc_A}(h_A)$ and $Enc_A(l_A)$ to agent B, without telling him which ciphertexts correspond to which value (ie without telling him which order he sent the two messages). This is in order to help conceal at time step 2 the value of the actual message h A will send - indeed, when B will receive h at time step 2 then he will have to differentiate h with h_A and (l_A (please see the schematic view of the messages being sent in our protocol at the end of this section). By scrambling the order, A can thus prevent B from knowing what the value of h is. By adding "pseudo agent C" in the protocol one can now split the information, as C would know the order in which A sent h_A and l_A to B, but not how to read Enc_A [Enc_B (h_1-h)] and $ Enc_A [Enc_B (h_2-h)] since C cannot decrypt A and B's encrypted messages (but C can perform homomorphic operations on it, such as using these values as encrypted *weights* in determining the encrypted final allocation value, which will then be sent back to A and B for decryption (see FIRST OPERATION, SECOND OPERATION and COMPUTE steps at the end of this section). B on his side knows the values of Enc_A [Enc_B (h_1-h)] and Enc_A [Enc_B (h_2-h)] , but not what $h_1$and $h_2$correspond to.

Concerning the encryption, the subscript A after Enc means that it has been encrypted using A’s key pair. So, recalling the notation of key pairs and encryption from last section:

$$Enc_A(h_A) = a \cdot \ s_a + \delta \cdot h_A + e_a \tag{21}$$

and

$$Enc_A(l_A) = a \cdot \ s_a + \delta \cdot l_A + e_a \tag{22}$$

Let’s assume for simplification in this case that δ = 1, so that the Enc operator I just define here is commutative, ie

$$Enc_B(nc_A(x)) = Enc_A(Enc_B(x)) = a \cdot \ s_a + a \cdot \ s_b + x + e_a + e_b \tag{23}$$

for any message x. In practice schemes such as BFV can be made commutative, even if the mathematics behind become a bit ”heavier”. I will use this commutative property in the encoding at Step 2, Period 2, of the deterministic protocol ”pseudo agent C” will follow.

From there on let's call $Enc_A(h_1)$ the first value agent B received, and $Enc_A(h_2)$ the second value agent B received. If A sent $Enc_A(h_A)$ first and $Enc_A(l_A)$ second then $Enc_A(h_1) = Enc_A(h_A)$ and $Enc_A(h_2) = Enc_A(l_A)$ and vice and versa. But B doesn't know.

Agent A also sends to B

$$Enc_A((1,0)) = (a \cdot s_a + 1 + e_a, a \cdot s_a + 0 + e_a) \tag{26}$$

if he sent to him $Enc_A(h_A)$ first and $Enc_A(l_A)$ second. Else A sends to B

$$Enc_A((0,1)) = (a \cdot s_a + 0 + e_a, a \cdot s_a + 1 + e_a) \tag{27}$$

, if he sent to B $Enc_A(l_A)$ first and $Enc_A(h_A)$ second. As encrypted messages, these are uninterpretable by B. B then encrypts this message with his own key pairs, so that the message is encrypted using the “combined” multiparty key pair built using both A and B's pairs (similar to what we did for the auction without auctioneer example). B sends that to C. That message is then now

$$Enc_B(Enc_A((1,0))) = (a \cdot s_a + a \cdot s_b + 1 + e_a + e_b, a \cdot s_a + a \cdot s_b + 0 + e_a + e_b) \tag{28}$$

if A sent to B $Enc_A(h_A)$ first and $Enc_A(l_A)$ second, else it is $Enc_B(Enc_A((0,1)))$ in the reverse case. Let's call that message ”C's input from B from STEP 1”. Here the value 0 means null, and the value 1 means non-null as will be in the rest of the document.

Step 2. At Period 2

Agent A sends the encrypted version of its actual message $Enc_A(h)$ (which can only take two values, either h_A or l_A) to B.

B then sends back to A for reference $Enc_B(0)$. This reference will be encrypted by A using A's own keys, and sent to C, to have a "null reference" encrypted by both B and A's keys, $Enc_A(Enc_B(0))$ (let's call it the "null reference" from now on). We will see right here already how this "null reference" will "show up" in the set of messages sent between B and A. Indeed B also sends to A the encrypted pair $Enc_B(Enc_A(h_1) - Enc_A(h), Enc_A(h_2) - Enc_A(h))$. This pair's value is for instance $Enc_B((0,1))$ if $h_1 = h_A$ AND if $h=h_A$. For clarity I will list below all the pair's value depending on all possible cases, as listed be- low. There the numbered cases denote which underlying shock in step 1 was sent first, and alphabetical cases denote the actual underlying and the corresponding sent values, due to incentive compatibility are : (I also organized all the entries below in a summarizing table put at the end of the document, for more readability)

case 1) h_1 is equal to h_A, then h_2 is equal to l_A

case 2) h_1 is equal to l_A, then h_2 is equal to h_A

case a) h is equal to h_A

case b) h is equal to l_A

So the corresponding messages sent by B to A become:

- in the pair (case 1, case a) $Enc_B(Enc_A(h1) - Enc_A(h), Enc_A(h2) - Enc_A(h)) = (Enc_B((0,1))) = (Enc_B(0),Enc_B(1))$.

- in the pair (case 2, case a) $Enc_B(Enc_A(h1) - Enc_A(h), Enc_A(h2) - Enc_A(h)) = (Enc_B((1,0))) = (Enc_B(1),Enc_B(0))$.

- in the pair (case 1, case b) $Enc_B(Enc_A(h1) - Enc_A(h), Enc_A(h2) - Enc_A(h)) = (Enc_B((1,0))) = (Enc_B(1),Enc_B(0))$.

- in the pair (case 2, case b) $Enc_B(Enc_A(h1) - Enc_A(h), Enc_A(h2) - Enc_A(h)) = (Enc_B((0,1))) = (Enc_B(0),Enc_B(1))$.

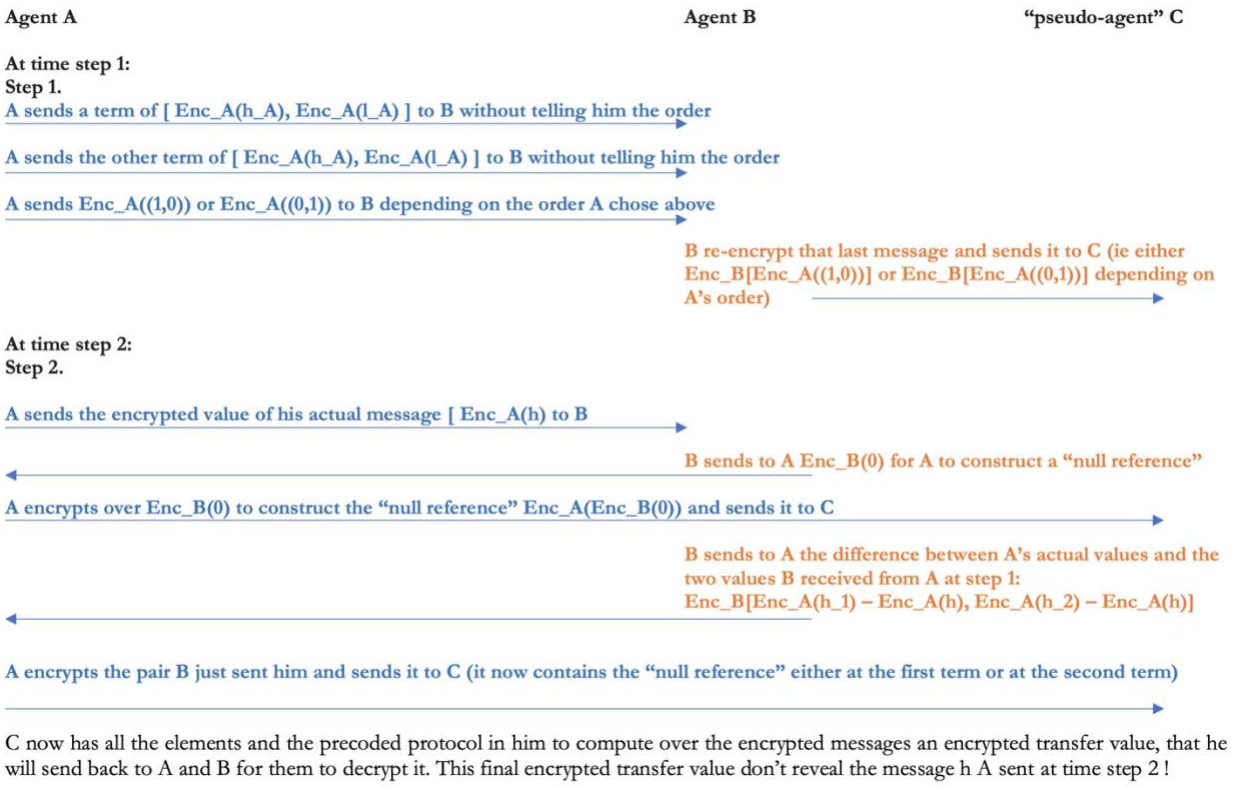
Note that here the notation is 0 = null, 1 = non-null. Indeed we define a "peculiar" algebra here, which says that ALL non-null numbers will take the same value 1 ie if $Enc_A(h2) - Enc_A(h) \neq 0$ then $Enc_A(h2) - Enc_A(h) = 1$; same if $Enc_A(h1) - Enc_A(h) \neq 0$ then $Enc_A(h1) - Enc_A(h) = 1$. So there are only two different outcomes resulting from the four possible cases 1,2 combined with cases a,b. That will make it easier to conceal what the actual message agent A sent at period 2 is - see summarizing table at the end of this section.

A encrypts back the two messages received from B using his own keys, first the reference $Enc_A(Enc_B(0))$ (the "null reference"), and the new pair message which value is now encrypted with both B and A's keys, and equal to either $Enc_A(Enc_B((0,1)))$ or $Enc_A(Enc_B((1,0)))$. A sends both the "null reference" and this new pair message to C. Let's call the new pair message "C's input from A from STEP 2". Indeed, this is linked again to the "information splitting" I described at the start of the protocol, as B doesn't know the order in which h_A and l_A have been sent, but C who knows this order doesn't have the keys to read any of the messages it has to perform homomorphic operations on. Let's note that these messages are also encrypted with A's private key, so even if a malicious

B intercepts these messages B still wouldn't be able to read them. Let's also note with the commutative and the distributive properties of the Enc operator, $Enc_A(Enc_B((0,1)))$ = $Enc_B(Enc_A((0,1)))$ = $(Enc_B(Enc_A(0)), Enc_B(Enc_A(1)))$ = (null reference, $Enc_B(Enc_A(1))$ and $Enc_A(Enc_B((1,0)))$ = $Enc_B(Enc_A((1,0)))$ = $(Enc_B(Enc_A(1)), Enc_B(Enc_A(0)))$ = $(Enc_B(Enc_A(1))$,nu reference) .

Let's sum-up all the messages sent between the agents in the following schemata:

Schematic view of the messages being sent in our protocol:



C is constructed to have "precoded" in it (made sure both by agents A and B as they agree to the scheme) :

- FIRST OPERATION: COMPARE the two terms in the pair of "C's input from A from STEP 2" with the "null reference", and FIND which term of the pair is equal to

the "null reference" (at least one of the terms should be, since "C's input from A from STEP 2"'s value is either $Enc_A(Enc_B((0,1)))$ or $Enc_A(Enc_B((1,0)))$. And with the notation that $Enc_B(Enc_A((1,0))) = (Enc_B(Enc_A(1)),Enc_B(Enc_A(0))) = (Enc_B(Enc_A(1)),$null reference$))$. Keep in memory which term in the pair matched the "null reference", through a variable $memorized_t$ and one variable NON $memorized_t$, with $memorized_t=1$ and NON $memorized_t=2$ if the first term matched the "null reference" or $memorized_t=2$ and NON $memorized_t=1$ otherwise. The variable memorized is in the end keeping track of whether the eventually realized true value was encrypted and sent first, or second, at the very first stage at time step 1 when A sends a message to B, without in itself revealing whether A sent a message for high liquidity need or for low liquidity need. Indeed, I built a summary table at the end of this appendix, of all possible values of $memorized_t$ depending on the case we are in. There we can see for instance that for the high liquidity needs value cases (case a, combined with case 1 and case 2) one moves across the two columns with $memorized_t$ going from 1 to 2 depending on if the realized true value (here high liquidity need) was sent first or second by A to B (who then encrypted it using his key and sent to C) at STEP 1. Similarly, for the low value cases (case b, combined with case 1 and case 2), $memorized_t$ goes from 2 to 1.

Depending on the result "pseudo agent C" will have to perform the randomization function of Townsend, JME 1988, or execute the transfer corresponding to the low liquidity need (thanks to the randomization in the high liquidity need case, this low liquidity case cannot be distinct with certainty to the result of the randomization in the high liquidity need from A case). However, because we don't want "pseudo agent C" to know in which case we are even while he is doing it (so that no ones that even manages to "hack" C can reveal A's true liquidity needs) the "pre-programmed" sets

of operations has to take place on encrypted space, and has to cover both high liquidity need and low liquidity need cases at once. For the first of these two requirements we can invoke the homomorphic property of the encryption scheme we have been using all along. For the second requirement we can notice by looking at the table above showing all four cases combining cases 1,2 and cases a,b, that we can use the resulting (at this stage encrypted) 0 and 1 in all four cases as ”switches” activating either the randomization function, or the low liquidity need. Indeed, the randomization function AND the low liquidity need transfer are coded beforehand IN EACH outcome. So, no matter if the actual message sent by agent A at period 2 is the high liquidity need or the low liquidity need both the code doing the randomization and the low liquidity transfer will run. However what changes - the ”switches” - are the weights in front of each of these two terms (the randomized number and the fixed low liquidity number). The weights come from C’s comparing inputs from A and B, and thus putting an encrypted 0 in front of one of these two terms as weight, and an encrypted 1 in front of the other of these two terms as weight. So in all cases both terms are ”computed”, but in each case only one of them will actually have a non-null weight in the result. Let’s write this down more in details:

- SECOND OPERATION: $memorized_t$ from FIRST OPERATION will tell us how each of the two terms in the pair ”C’s input from B from STEP 1” will be used as the ”switches” in the following operation. Let’s note $memorized_t$(”C’s input from B from STEP 1”)= the first term of the pair (”C’s input from B from STEP 1”) if $memorized_t$=1, else the sec- ond term of the pair (”C’s input from B from STEP 1”) if $memorized_t$=2. Let’s also note NON $memorized_t$(”C’s input from B from STEP 1”)= the second term of the pair (”C’s in- put from B from STEP 1”) if $memorized_t$=1, else NON $memorized_t$(”C’s input from B from STEP 1”)= the first term of the pair (”C’s input from B from STEP 1”) if $memorized_t$=2.

I.e., if ("C's input from B from STEP 1")=$Enc_B(Enc_A((0,1)))$ and $memorized_t$=1, then $memorized_t$("C's input from B from STEP 1")=$Enc_B(Enc_A(0))$ and NON $memorized_t$("C's input from B from STEP 1")=$Enc_B(Enc_A(1))$. Please see all possible cases in table below.

Notice that in each case one of the two above variables $memorized_t$("C's input from B from STEP 1") and NON $memorized_t$("C's input from B from STEP 1") will be $Enc_A(Enc_B(0))$, while the other of the variable will be $Enc_A(Enc_B(1))$ (with as a reminder 0 meaning null and 1 meaning non null, and with ALL non null values being equal to 1).

We can now build the following generic set of operations, covering all four cases from the table above with the same sets of instructions:

COMPUTE the output transfer amount resulting from C as the sum between the amount corresponding to the randomization from Townsend, JME 1988, with weight equal to the value of the NOT-YET-DECODED-$memorized_t$("C's input from B from STEP 1"), and the amount corresponding to A's low liquidity need with weight equal to the value of the NOT-YET-DECODED NON $memorized_t$("C's input from B from STEP 1"). In each of the four case of the table above, only one of the amounts corresponding to the randomization or corresponding to the low value will be non-null, since there is in each case one and only one null weights (even if that null probability is NOT-YET-DECRYPTED - the first of the two requirements to conceal to C and everyone whether randomization was done or not, since even if it's done it's been computed in the encrypted space).

For clarity let's write down the summary table of what messages are sent in each of the four cases above (case 1 or 2, combined with case a or b, where the numbered cases denote which underlying shock in period 1 was sent first, and alphabetical cases

done the actual underlying sent at period 2 due to incentive compatibility). Let's note that in all four cases at item 4) C ALWAYS computes, in all four cases, the generic formula $memorized_t$(C's input from B from STEP 1).(randomized amount) + NON $memorized_t$(C's input from B from STEP 1).(low liquidity amount). Let's also note that the homomorphic encryption property is used in 5) of the summary table below, in the equality $Enc_B(Enc_A(1)).$(randomized amount) + $Enc_B(Enc_A(0)).$(low liquidity need amount) = $Enc_B(Enc_A$(1.(randomized amount) + 0.(low liquidity amount)) = $Enc_B(Enc_A$(randomized amount)) and in $Enc_B(Enc_A(0)).$(randomized amount) + $Enc_B(Enc_A(1)).$(low liquidity need amount) = $Enc_B(Enc_A$(0.(randomized amount) + 1.(low liquidity amount)) = $Enc_B(Enc_A$(low liquidity amount)). We can verify that in all four cases such a homomorphically computed sum between one null term and one non-null term will give the amount corresponding to the specific combination of case 1 or 2, with case a or b that occurred.

So at this point C's output is already a NOT-YET-DECRYPTED numerical value without trace revealing for certain whether the numerical value is the result of a randomization function - the one corresponding to the amount of the transfer that should happen.

Then C sends this NOT-YET-DECRYPTED numerical value first to B (or A - the order is not important) who decrypts using his key, then to A (or B if sent to A first) who also decrypts, so that all three agents and pseudo agent A, B and C knows the value of the transfer in plain numerical form. Thus, C's intermediate steps, all on encrypted space, and its generic coding that handles at once the high and the low liquidity need case, prevents anyone that could even see C's intermediate results from knowing A's liquidity need.

Chapter 5 – Generalization principles

Let's see what "generalizing" these examples would first mean in the mechanism design framework, before studying how that could be implemented on the technology and encryption side. Let's notice first that generalizing the contracts would mean, in the mechanism design framework, to either increase the number of interacting agents (a), the complexity of the message space (b), or the interaction (computations) to be run between them (c). Let's see for each of them how that would translate to technologically, using the implementation examples I exposed above.

(a) Increasing the number of interacting agents - illustration using the auction example above

The auction example presented in section (4) presents both ways one could tackle an increase in interacting agents - first would be to use the 2 agents case as a basic building block that could iterated over all agents, second would be by adapting the computation function between agents in a way that fit the problem better. For instance, if one chooses to use the 2 agents case, one can realize that "pseudo agent" C from section (4) is in fact a ranking operator. I.e. presented with any two bids, "pseudo agent" C can figure which is highest without knowing any of the initial bid values. One can thus design a sorting algorithm between N agents' bids using this ranking operator, to find the maximum. One can add in privacy-preserving features if needed - for instance, presenting pairs of bids to be compared randomly to C; letting C encrypt the name of the "winner" of a pairwise comparison so that no agents can know if other agents' bids are higher or lower than his... The engineering gains are in terms of design here since we don't need to alter any of the section (4) set up,

while we might be trading off computation time (since we would need to go through all pairs of bids using such a design).

The second approach can improve the number of comparisons, if we increase the complexity of the computation so that instead of taking just 2 agents' bids it can take N agents'. For instance, instead of just doing a subtraction of 2 agents' bids to see which is higher, one could do a multiparty addition of all N agents' bids to then compute the difference of all N agents' bids vs the median bid value among the N of them. For the roughly half of these agents that have bids lower than the median, we drop them from the auction, and repeat the process for those agents left in the competition. The multiparty computation complexity is of the same order than the previous case, since we are just doing additions instead of subtractions, and increases linearly with the number of bidders. Please note that one could do that with or without the "pseudo agent C", depending on privacy requirements (as without pseudo agent C then all agents themselves are in charge of running the multiple rounds of multiparty computations, with less and less agents participating in them. But there the values of the successive medians can still be encrypted and kept secret from all, as one only needs to know the sign of the subtraction of a bid vs a median. With a "pseudo agent C" then it can be done all by him, so that agents themselves only see the final winner. But that reintroduces the control problem of a trusted third party - in this case pseudo agent C, which can be a server that has been jointly set up by all agents, and then left as a "deterministic box" on its own, or in a DLT setting a smart contract).

All in all, the trade-offs are that linking to the complexity of a potential (re)design process, the complexity of added encryption and multiparty computation steps if needed, and added computation time from repeating encryption and multiparty computation steps if needed, and the privacy considerations one needs to keep.

b) Increasing the complexity of the message space - illustration using the hybrid contract

Increasing the message space is equivalent, in mathematical terms, to increase the dimensions of that space. For instance, go back to the hybrid's setting above, and assume there are now three different messages (high, medium, low) that could be sent by the borrowing agents instead of the two (high, low) in the previous setting. There are now two ways one could accommodate such an enlarged message space. The first would be, similarly to the first approach in more agents auction described above, to adapt the existing set up as a basic solver to be repeated several times. Indeed, because there are now 3 potential message values now, I will break these 3 potential values into 2 subproblems containing each only 2 potential values, so that each of these 2 subproblems are EXACTLY the same problem as the case presented above. Therefore, we would have

- one pseudo agent (C1) that will "treat" the low and medium messages - but C1 doesn't know which ones they are doing

- one pseudo agent (C2) that will "treat" the medium and high messages, but they don't know which ones they are doing

- one pseudo agent (C3) that will "treat" the low and high messages, but they don't know which ones they are doing

Then, the first pseudo agent is EXACTLY like in our previous hybrid write up, but just with (low, medium). That nodes sends out at the very end: Dec[Enc(actual message value - low)] * Allocation corresponding to low + (1/2) * Dec[Enc(actual message value - medium)]*Allocation corresponding to medium , with the notation that if a subtraction is equal to zero above then

Dec[Enc(0)]=1, else then Dec[Enc(non-null value)]=0 (as described in section 5 in the 2 message value case). The second contract does EXACTLY the same with medium and high as it did in the 2 value case, and that node sends out: Dec[Enc(actual message value - high)] * Allocation corresponding to high + (1/2) * Dec[Enc(actual message value - medium)]*Allocation corresponding to medium. Finally we just sum the values sent by both contracts.

The second approach, as described in the auction case, would be to adapt the de- sign of the existing set up so that it can take into account more messages at once. For instance, through the intermediary variables used to ”store” messages in the 2 agents case. In the language of section (5), the memorized variable used previously will be a vector in- stead of the previous scalar values it would take (0 or 1). ie memorized is now taking values in (0,0,1), (0,1,0), (1,0,0) for the 3 values of high, medium, or low. Then the SECOND OPERATION performed by pseudo agent C would now be for C to allocate the value [(first term of the memorized vector) times value corresponding to low message + (second term of the memorized vector) times value corresponding to medium message + (third term of the memorized vector) times value corresponding to high message ” (eventually with interaction terms)].

c) Increasing the interaction (computations) to be run between agents

This now touches upon the maturity of the underlying technologies. If we use FHE and MPC as described in this document, then for linear functions increase in complexity of the computation functions are feasible (with associated costs in computation time, see next subsection). Where things are harder are if we introduce non-linear functions, which is still a field of current research (the state of the art is now to see if one can do neural network machine learning as multiparty computation - see for instance Blatt, Gusev, Polyakov, Rohloff and Vaikuntanathan 2020). For these alternatives

technologies could be used, such as trusted executed environments (TEEs), though they are hardware solutions so necessarily introducing a discussion on how to maintain them, similar to that around the ”pseudo agent” concept we introduced in this paper.

As for a review and benchmark of existing FHE-MPC applications and computation times, I refer to the following selection of literature listing notable implementations. MPC and/or HE have been for instance utilized to develop a method for protecting privacy in large-scale genome-wide association studies (Kamm et al., 2013). This is an analysis of the likelihood of diseases based on private medical information, phenotype (age, gender, height) and genotypes, so that physicians can make tailored recommendations to their patients while all the individual data used in the analysis remains secure. I think of previous research that has used MPC to run a double auction for the Danish sugar beet market (Bogetoft et al., 2009); securely link Estonian education and tax databases (Bogdanov et al., 2016); run a simulation of a decentralized and privacy-preserving local electricity trading market (Abidin et al., 2016); perform an analysis of the gender wage gap in Boston using data from a large set of Boston employers (Lapets et al., 2016); and proof of concept using real data from large firms to show how to securely calculate aggregated measures over sensitive cybersecurity data (Castro el al., 2020).

Though encryption has its limits, in that problems do not scale up easily, the limit in practice is more for the overall number of participants rather than the number of lines of data or interactions in analysis. Overall advancements are promising. For example, the Estonia project ran on 10 million tax records and half a million education records.

Chapter 6 – Conclusion: implementation of mechanism design problems as contracts and without ledgers

We do not need a planner or trusted third party. This idea should be clear from the two previous examples, auctions without auctioneers and hybrid borrowing/lending insurance schemes with secrets and no third party. To be clear how this generalizes, for a given environment, we solve for the constrained-optimal multi-party arrangement. Then to implement the scheme with our tools, we make the code that generated the solution to the planner problem available for participating agents to see line by line, so they can validate that the code does what it is supposed to do. This contract node now replaces the planner entirely. This initial validation process can include multiple potential simulations as if being implemented in real time, following the time line which follows. Agents get convinced it achieves their desired purpose, the reason for contracting, and that information is concealed.

The contract can be hashed and signed into an immutable record that agents have entered into it. No denials later. Next, each agent deposits owned assets or liquidity into an escrow account. This could be an escrow account with a trusted third party such as a commercial bank or an escrow account that is a digital asset on a ledger with programmed conditions for use. The messages are sent internally, as described above.

Similar constructions allow delegated portfolio management without trust, consultation with public oracles, and implementation of solutions which mitigate or potentially eliminate bank runs through automated state contingent gateways dependent on recorded immutable history.

To reiterate we do not need distributed ledgers for the mechanism design part of the problem. Indeed, there is a bit of a disconnect in the different uses of the word trust between computer science and economics literatures. Morris and Shin come to the essence of the problem by modeling the incentives

of participants to follow the prescribed protocol in the Byzantine Generals problem. This is a classic and seemingly simple problem of coordinating a successful attack when the enemy may be prepared, in which case an attack even if coordinated will not be successful, and only one general is informed of this state. Generals can send messages back and forth, but messages are noisy, that is, may not arrive albeit with a low probability. Strategic maximizing behavior in an explicit information game, without commitment, is inconsistent with intuitive prescribed protocols, as agents start to second guess each other as in a Bayesian sequential equilibria. An alternative counter-intuitive protocol with commitment and less communication, one that prevents the second general from replying with a validating message, achieves the optimum, ironically.

The larger point is that we cannot be sure that the validators on distributed ledgers will blindly follow the protocol. Instead we should consider strategic behavior. The Morris and Shin example is particularly damning as it is in the group's interest to coordinate. The opposite tactic is taken in implementation of multi-party mechanism design problems, as protocols take into account strategic behavior and private information and thus are constrained- optimal and incentive-compatible from the get go. Apart from faulty computers, there is no need for validation protocols. Future work could focus on implementing more complicated schemes, such as the Green and Lin Bayesian solution to the bank run problem (work in progress, will be published on www.leadmit.com) or schemes like the one on monetary anchoring, presented in the next Part of this thesis.

Chapter 7 – Appendix for Part I

Table 1: Summary of messages computed and sent in each of the four cases

	Case 1: h_1=h_A and h_2=l_A	**Case 2: h_1=l_A and h_2=h_A**
Case a: h=h_A	1) C's input from B from STEP 1 =$Enc_B(Enc_A((1,0)))$ 2) C's input from A from STEP 2 =$Enc_A(Enc_B((0,1)))$ 3) C finds $memorized_t$=1, so that NON_$memorized_t$=2 as well 4) The "switches" here take values: $memorized_t$(C's input from B from STEP 1) = $Enc_B(Enc_A(1))$ in front of (randomized amount), and NON_$memorized_t$(C's input from B from STEP 1) = $Enc_B(Enc_A(0))$ in front of (low liquidity need amount) 5) Thus the generic formula takes here the values $Enc_B(Enc_A(1))$.(randomized amount) + $Enc_B(Enc_A(0))$.(low liquidity need amount) = $Enc_B(Enc_A$(1.(randomized amount) + 0.(low liquidity need amount)) = $Enc_B(Enc_A$(randomized amount))	1) C's input from B from STEP 1 =$Enc_B(Enc_A((0,1)))$ 2) C's input from A from STEP 2 =$Enc_A(Enc_B((1,0)))$ 3) C finds $memorized_t$=2, so that NON_$memorized_t$=1 as well 4) The "switches" here take values: $memorized_t$(C's input from B from STEP 1) = $Enc_B(Enc_A(1))$ in front of (randomized amount), and NON_$memorized_t$(C's input from B from STEP 1) = $Enc_B(Enc_A(0))$ in front of (low liquidity need amount) 5) Thus the generic formula takes here the values $Enc_B(Enc_A(1))$.(randomized amount) + $Enc_B(Enc_A(0))$.(low liquidity need amount) = $Enc_B(Enc_A$(1.(randomized amount) + 0.(low liquidity amount)) = $Enc_B(Enc_A$(randomized amount))
Case b: h=l_A	1) C's input from B from STEP 1 =$Enc_B(Enc_A((1,0)))$ 2) C's input from A from STEP 2 =$Enc_A(Enc_B((1,0)))$ 3) C finds $memorized_t$=2, so that NON_$memorized_t$=1 as well 4) The generic formula takes here the values $Enc_B(Enc_A(0))$.(randomized amount) + $Enc_B(Enc_A(1))$.(low liquidity need amount) = $Enc_B(Enc_A$(0.(randomized amount) + 1.(low liquidity amount)) = $Enc_B(Enc_A$(low liquidity need amount))	1) C's input from B from STEP 1 =$Enc_B(Enc_A((0,1)))$ 2) C's input from A from STEP 2 =$Enc_A(Enc_B((0,1)))$ 3) C finds $memorized_t$=1, so that NON_$memorized_t$=2 as well 4) The generic formula takes here the values $Enc_B(Enc_A(0))$.(randomized amount) + $Enc_B(Enc_A(1))$.(low liquidity need amount) = $Enc_B(Enc_A$(0.(randomized amount) + 1.(low liquidity amount)) = $Enc_B(Enc_A$(low liquidity need amount))

Part II:
An end-to-end analysis and implementation of our framework on a complex system – that of the current fiat international monetary anchoring

For this second part of my thesis, I now make full use of the "recipes" and design principles listed in the first part, to propose an end-to-end solution to now a real life, concrete topic – that of monetary anchoring. For that I follow first an economic modelling effort to highlight what I deem to be currently the most "defective" feature of the current monetary anchoring – a bias in the incentives of the system leading to great financial imbalances and power-law like distribution of debts between countries (Chapter 8). I then try to empirically estimate and validate this model (Chapter 9), to finally focus on Pareto improving this feature with the use of our mechanism design framework, to "correct" the biased incentives, and provide an applicable implementation of such a rebalancing scheme between central banks using encryption as communication and consensus-finding medium (Chapter 10).

Chapter 8 – a model of fiat monetary anchoring

NB: this section also contains code that can be run interactively on https://bit.ly/inflationSAS

Executive summary:

As part of the economic modelling effort to highlight the most first present here a dynamic and computational model of the international monetary system encompassing both the safe asset shortage hypothesis and Claudio Borio's financial cycle buildup hypothesis.

Our model harks back to Keynes' rejection of the "natural" rate of interest in his General Theory. Building on the argument that there is no single natural rate of interest that balances the economy at full employment, and the possibility that various paths depending on the sequence of monetary policy actions raise or lower the prospect of the economy evolving along unsustainable paths - including on what concerns inflation, I define a game-theoretic model between central banks to illustrate how globalization and the new entrants in world markets it brought along could have driven down long-term rates and inflation (a hypothesis first formulated by Rogoff, 2003).

Following that view, there would be an international component of inflation, in addition to each country's domestic term. And, in globalized markets, country's domestic inflation terms might react to central banks' policies to a lesser extent than what would be necessary to achieve central bankers' nominal targets. Attempts to forcefully do so might even lead, as described by Borio, 2019c, in making them act "like a forcing variable that sustains the system at some arbitrary level for an extended duration". Then, given path dependence, actions today condition outcomes tomorrow that, in turn, constrain choices taken at that point. And they can do so in ways that increasingly narrow the room for manoeuvre and worsen economic outcomes.

And what might be true of interest rates should be true for inflation as well, according to our unifying framework. Supply of money and supply of goods are, after all, the two faces of the same

coin. Thus, secular decline in world interest rates should be matched by a secular decline in the international component of inflation. Hence, by targeting the wrong values and by following wrong analysis for inflation's various components we might be building up risks, whether through monetary or fiscal stimulii. Economic policies consist, after all, for a good part in fixing the flaws of previously applied models - for no model is perfect in itself, with any one model used long enough building up its set of imbalances over time.

(a) Opening motivating question: the link between price stability and monetary anchoring

Through a model of monetary anchoring, I aim to provide an unifying framework explaining how it is in fact a safe asset shortage that enabled central banks such as the Fed (by creating an environment with less inflationary/deficit funding pressure) to "keep output high today", thus "weakening the financial sector and narrowing policy choices tomorrow" (Borio, 2019c). Hence lower interest rate today, first made possible in the US by the demand from the Rest of World for USD denominated safe assets, but which then raised the likelihood of a future burst, "whose materialization justifies even lower interest rates" (still made possible by the still ongoing safe asset shortage). Hence lower and lower US rates, which spilled over the rest of the world's monetary policies, thus creating a secular decline in natural real rates.

Furthermore, our model also highlights how globalization would have been the main driver of lower inflation worldwide - an hypothesis first formulated by Rogoff (2003). Indeed, if one views globalization as the connection of advanced countries' consumer markets to developing countries' industrializing labor forces, while the supply of USD (the global trading and reserve currency) is roughly stable (at least compared to the scale and the magnitude of the new production forces introduced to global markets), then following John Stuart Mill's demand and supply factors

determining the value of money (ie what money can acquire ; "the supply of money being, in a nutshell, the totality of money is circulation at the present moment [...]. The demand of currency is composed, on the other hand, of all merchandises put to sale". John Stuart Mill, Principles of Political Economy, book III, chapter VIII, paragraph 2, Paris, 1861) global disinflation occurs naturally as a consequence of globalization. Even more, inflation in every country is then at least partly defined by a component resulting only from international trade and finance parameters beyond domestic parameters (let's call this global component common to all countries the "neutral" inflation rate). Interesting questions follow, that we'll try to answer here: "how much does this "neutral" inflation rate account for in domestic inflation rates?" and "how much influence do monetary policies have on inflation rates then?".

Indeed, let's imagine for a minute that monetary policies only have a limited action on this "neutral" inflation rate, such that no matter how much monetary eastings are allowed the inflation rate will never reach the target. An important consequence that then follows, if we write inflation π_t as a combination of this "neutral" inflation rate $\widetilde{\pi_t}$ mainly determined by international trade and finance and only partially responsive to Taylor rules, and of a financial asset price index $a_t$such as $\pi_t = \widetilde{\pi_t} + a_t$, then changing interest rates i_t to change π_t will affect domestic financial asset prices a_t to all the extent in which the "neutral" inflation $\widetilde{\pi_t}$ does not react to the interest rate change. It can thus be worth studying what factors affect this "neutral" inflation rate and how much power each country has over it (to explain inflation rates that can still differ from one country to another). These are the objects of the study of our Part I.

If our model and hypothesis are confirmed, then the Fed and advanced economies' central banks' over-reliance on inflation targeting rules will lead them to double down on efforts to make this "neutral" inflation rate reach their domestic target, in the process compounding the "low rates beget

lower rates" financial buildup aforementioned with active inflation of financial assets and bubbles, hence riskier and riskier, and more and more ample financial cycles (as in Borio 2019c).

All in all, our model of the existing monetary system provides an explanation of the "secular long term rate trends" as entirely a consequence of the current (lack of) monetary anchoring, compounded by misconceived models of inflation and of monetary policies (Taylor rules as above, DGSE and New Keynesian models as criticized in Borio 2019c). Price stability is hence dependent on the stability of the anchoring, which then has to be a sustainable, strategy-proof scheme.

(b) Central banks' behavior in the "global village" and the use of a mechanism design framework

For our model I will stay at a highly abstract, central bank level, game theoretic point of view. Indeed, let's first note that national debts and individual debts play along different rules. Indeed, to adopt Graeber and Polanyi's language, insofar as individual debts are contracted along impersonal markets with "foreign" entities - people we don't know personally, with whom there is no preexisting history of trust nor incentive for future collaboration - so sets of rules and guarantees are needed to enforce the repayment by the borrower.

Countries among themselves are however known neighbors in the global village, condemned to interact with each other for eternity (at least by the standards of our individual lives). Hence rules of debt closer to that of "human economies", in which neighbors are "always slightly in debt to one another [...] - a delicate web made up of obligations to return three eggs or a bag of okra, ties renewed and recreated, as any one of them could be canceled out at any time" (ibid, p.122), along with display of gifts, generosity and hierarchy following the much richer and more complex meanders of human psychology, which cannot and could never be exactly quantified in monetary terms.

We are however only at the beginning of a phase of truly "globally" connected planet, so that the rules of individual and impersonal markets are still the ones been used between nations (through the monetary anchor, which exactly quantifies and enforces what countries owe each other).

However, what happens when a country default? It can't be imprisoned, beaten to death to serve as example to others, etc. There is then a friction there not existing in individual markets, since countries have more "relaxed" rules of default, that distort risk pricing and establish a "hard" separation between what are considered safe assets (they are then really safe), and not as safe assets (pretty much the vast majority of countries' debts).

This is what I referred to as "top-down vs bottom-up modeling in international economics": indeed, while Borio argues that "in sharp contrast to the current standard New Keynesian frameworks, the friction underlying deviations of market from natural interest rates is a capital market failure rather than price (and possibly wage) stickiness", I would like to add that this "capital market failure" is in turn a result of bad incentives created by a even broader game, that of fiat monetary anchoring. Especially, different countries and cultures might provide different preferences and behaviors both at the micro level, which have to be accounted for in any macro framework derived from these foundations (or, as in our case, be left as exogeneous parameters that can be adjusted on a country-by-country basis). Certain of these behaviors are productive for the global economy, while others are toxic, and have to be limited by the system of anchoring. Then the village economy analogy I used in the previous part naturally calls for mechanism design models, such as those underpinning the borrowing and lending and insurance literature as in Townend JPE 1982, 1982a, 1989, and in the "global game" literature, to provide a better framework for design of an improved anchor.

(c) Inflation and long-term rates - an allocation problem of imbalances among countries

I will start first with a most basic allocation scheme of N assets between N agents (or countries - the two terms will be used interchangeably in the rest of this notebook), that of Bogolmonaia and Moulin (2001)'s cake-eating game, which I will progressively complexify and merge with standard open macroeconomy models.

Indeed, in the broad "money vs goods" balance à la John Stuart Mill, any imbalance can also be viewed as a shortage of one of these sides. Allocating these shortages during times of imbalances is thus the key in evaluating how lower neutral rates (shortage of safe assets) or inflation (shortage of goods) occur and spread between countries.

Furthermore, the description of agents' actions in Bogolmonaia and Moulin (2001)'s cake-eating game provides close analogy on how safety considerations are being carried out dynamically in time, along with risk vs returns logics, by central bank officers. That analogy sustains the practicality of use and predictive power of our model, which can thus also serve as foundation and complement of existing models such as Mundell-Fleming, by enabling calibration of practical values and of curves slopes in highly stylized model such as the Safe Asset Scarcity and Aggregate Demand version of IS/LM developed by Caballero, Farhi and Gourinchas (AER, 2016). Indeed, the slope of the AS curve can be derived from the amount of inflationary pressure computed by our model (through the allocation of a shortage of goods among countries) and the slope of the AD curve can be derived from the amount of pressure on interest rates computed by our model (through the allocation of a shortage of safe asset among countries).

The original Bogolmonaia and Moulin "cake eating" allocation game

Before seeing how our model unfolds, let's first describe the original Bogolmonaia and Moulin "cake eating" allocation game. I will then show how to extend it to a dynamic model of inflation and interest rate trends.

Their original paper provides a "natural constructive algorithm" which characterizes the entire set of ordinally efficient assignments. Ordinal efficiency is a notion they defined, in between ex post efficiency - ordinal efficiency being stronger - and ex ante efficiency - ordinal efficiency being weaker. An assignment problem being an allocation problem where N objects (the "cakes") are to be allocated among N agents (the "mices"), and each agent is to receive exactly one object (I will relax that last constraint in our extension).

Their constructive algorithm (the "cake eating) works as follow: think of each object as 1 unit of an infinitely divisible commodity - or "cake" (a different commodity for each object). Each agent now is given an exogeneous eating speed function, specifying a rate of instant consumption for each time t between 0 and 1, and such that the integral of each function is 1. Given a profile of preferences (over sure objects), the algorithm works as follows: each agent eats from his or her best available object at the given speed, where an object is available at time t if and only if less than one unit has been eaten away up to time t by all agents.

This solution (called probabilistic serial) is a central point in the set of ordinally efficient assignments; indeed, if I choose the eating speeds independent of the preference profiles (which I will in our extension), the probabilistic serial assignment is the only equitable one (similarly, random priority assignment is a central point within the set of ex post efficient assignments). I will explore further the mechanism design properties and comparisons of their allocation game in Part 2, but let's now explore first how I extend it to a monetary model.

NB: Ordinal efficiency means that we only consider mechanisms that elicits only individual preferences over sure objects ordinal (whereas a cardinal mechanism collects a full-fledged Von Neumann-Morgenstern utility function from every agent). The restriction to ordinal mechanisms is the central assumption in their paper. As they put it, "it can be justified by the limited rationality of the agents participating in the mechanism. There is convincing experimental evidence that the

representation of preferences over uncertain outcomes by VNM utility functions is inadequate (see, e.g., Kagel and Roth [11]). One interpretation of this literature is that the formulation of rational preferences over a given set of lotteries is a complex process that most agents do not engage into if they can avoid it. An ordinal mechanism allows the participants to formulate only this part of their preferences that does not require to think about the choice over lotteries. It is genuinely simpler to implement an ordinal mechanism than a cardinal one".

This can be linked to the discussion of countries in our model behaving in a (mostly) non-strategic fashion. I will discuss that in the end of the next paragraph, in which I examine in detail the approximations and assumptions I am making in our modelling.

Let's see now how such a one-round game can be extended into a multiround game, and what properties and incentives will such an extension present.

If agents are countries (I will from here onward use the two terms interchangeably) condemned to interact with each other for eternity (at least by the standards of our individual lives), I will thus play the previous game on an infinite number of rounds.

Each round would unfold as described just above in the original Bogolmonaia and Moulin scheme. However, as in history, the outputs of each round impact the inputs of the next. To record that I will use an endowment/consumption matrix, for each agent to store the pieces of cakes he ate during a round, and carry it on to the next.

So for round T, the allocation algorithm follows that of Bogolmonaia and Moulin (2001) described just above. Each country i (out of N) - the "mouse i" - simultaneously absorb each other's cakes $\zeta_{j,T}$, with j ∈ [1,N] at different absorption speed ($\omega_{i,T}$ for country i), and each one following its own preference ranking $P_{i,T}$. While $\zeta_{j,T} \in \mathbb{R}_{>=0}$ and $\omega_{i,T} \in \mathbb{R}_{>=0}$ $P_{i,T}$ is a 1xN matrix which contains a

single time every integer between [1,..N]. When a cake by one country is finished the countries j that were eating it move to the item below in their ranking matrices $P_{j,T}$

Each agent stores what he absorbed during the round in that agent's aggregated reserves, which is formalized through the consumption matrix. The state of the world at the end of each round T can thus be represented by one NxN consumption matrix ET, which records how much cakes in total each agent has generated up to round T, and which agent are holding which proportion of these cakes. For convention we can fix column j of this matrix as all the cakes issued by agent j AND absorbed by agent i (in line i of this matrix). Cell (i,j) hence denotes the size of the cake issued by agent j that agent i absorbed into its own reserve.

Hence E_T=

$$\begin{bmatrix} c_{1,1,T} & c_{1,2,T} & \dots & c_{1,j,T} & \dots & c_{1,N,T} \\ c_{2,1,T} & c_{2,2,T} & \dots & c_{2,j,T} & \dots & c_{2,N,T} \\ & & \dots & & & \\ c_{i,1,T} & c_{i,2,T} & \dots & c_{i,j,T} & \dots & c_{i,N,T} \\ & & \dots & & & \\ c_{N,1,T} & c_{N,2,T} & \dots & c_{N,j,T} & \dots & c_{N,N,T} \end{bmatrix}$$

And we have the relation, to denote the fact that column j of E_T represents all the different shares of the cake $\zeta_{j,T}$ issued by agent j at round T, absorbed by all agents i (if $\zeta_{j,T}$has been totally absorbed during round T - which is not necessarily the case. See section below to define what happens when a country's cake is not totally absorbed during a round $\zeta_{j,T} = \sum_{i=1}^{N}(c_{i,j,T} - c_{i,j,T-1})$

Axiomatic properties of this extended multiround game

Let's build on the axiomatic study Bogolmonaia and Moulin designed, for their one round scheme.

Repeating the game on multiple rounds does not change the non strategy-proofness of the scheme (and introduces, in fact, the question of whether agents will solve inter-round optimization problems). I will discuss that in later sections.

The equal treatments of equals is preserved.

Is the ordinal efficiency still working though ? To answer that let's take a look at how the incentives introduced by the now dynamical process :

A quick mathematical view of the incentives introduced by the repetition of the game:

Let's now look only at the dynamic process, without caring about how the inner mechanism within a round works.

Let's define D_t^i as the cake generated by country i at round t and $\overline{D_t}$ the average cake size accross all agents at t. So using the previous notations with the endowment/consumption matrix, $D_t^i = \sum_{j=1}^{N}(c_{i,j,T})$ and $\overline{D_t^i} = average\left(\sum_{j=1}^{N}(c_{i,j,T})\right)$.

Let's also define γ_t^i as country i's average ranking and the average eating speed of the countries which ranked i highly (so the ones most likely to eat country i's cake during this round t), over all countries' average ranking and average eating speed.

Finally, by defining $S_t^i = D_t^i/\overline{D_t}$, we thus have, through the terms I just defined (and if we accept the assumption that cake size has something to do with how much other countries are willing to accept it) the growth equation of our dynamic system $S_{t+1}^i = \gamma_{t+1}^i . S_t^i$

- Let's recall Gabaix (2009)'s proof that one would only need to assume that the growth rates γ_t^i are i.i.d. random variables to give a resulting power law distribution (with the existence of the steady-state distribution guaranteed by frictions that both prevents small countries from becoming too small and a lower bound for sizes enforced by a reflecting barrier - for instance a fixed cost that prevents anyone to start a very small country).
- In our case it is sure that these growth rates γ_t^i introduce increased inequalities, because of safety as a positive feedback loop. Indeed, by repeating such a game with a large number of countries integrate the notion of "safety", which brings here a positive feedback loop.

A country that doesn't default in the past will be perceived as safer, so would be ranked higher, hence will indeed become safer (and thus could issue bigger debts at each round). Then the resulting distribution would be even more inequal than the power laws obtained just above.

So, this is to give a quick intuition of how through our model the distribution of cake sizes will be at least power law imbalanced. Hence huge incentives introduced, to strategically game the system and improve one's ranking by other agents. This can be related to some conclusions from the He et al. AER 2020 paper, in which countries strategically optimize their issuance "to capture a safety premium" (I will examine this conclusion further in our analysis). This can also be linked to how a winner-takes-all reserve currency can account for a larger and larger share of the global economy's reserve, due to its "safety" advantage.

But let's now examine other trends that arise from such a modelling, notably that concerning interest rates and inflation. Once all these have been explored, I will come back to the axiomatic approach to re-define strategic proofness, ordinal efficiency and cardinal efficiency in the context of this exact model, to provide a framework for design of improvements to the current international monetary system.

The linkage from this multiround shortage allocation game to a dynamic model of inflation and interest rate trends

For our extension of the "cake eating" model let's specify what the N objects that are to be allocated to the N agents are, what the eating speed functions are, what determines each agent's preference ordering, and how the outputs of one round of this game influences the inputs of the next (the goal of our model being to enable a multiround, multiagent formulation of the monetary system).

- What the N objects that are to be allocated between the N countries are:

Because shortages on one side or the other of the broad "money vs goods' balance can be viewed as symmetric, a single allocation model of any shortage on one side of the balance (ie any surplus on the other side of the balance) should both be able to explain inflation trends and interest rate trends. Hence, the only "asset" (the "cake" in Bogolmonaia and Moulin (2001)'s cake-eating game) whose allocation I will be modelling could be described using the concept of "purchasing power" - which quantifies the state of the balance between money (a nation's currency) and goods at a given time.

In a fiat monetary anchoring, we can define each national currency's "purchasing power as the amount of it which trading partners accepts to receive and keep in reserve" (here we can recall Schacht's analysis of "the war of 1914, which provided telling proof of the fact that state-guaranteed paper money, unlike gold and silver coins, does not represent any substantial value [...]. The war of 1914 isolated Germany from the greater part of the world market. The Mark had become unusable on enemy markets. It has lost its purchasing power". (Schacht, The Magic of Money, p94). Hence our model of the international monetary system, which consists in just countries. Each of these countries prints fiat money, which has to be accepted by others in order for it to have any purchasing power.

And, now that this purchasing power that we are allocating have been define, let's examine the two sides of the imbalance it can find itself caught in:

- **in a safe asset shortage environment**, in which there is an excess of good being produced compared to the available quantities of safe assets - each country can be represented by a "mice (the country's aggregated investors and consumers - ie its financial investment capacity in a monetary language, or its consumption capacity in a goods language), which absorbs the "cakes" (countries' liabilities - ie their industrial investment needs in a monetary language, or their production capacity in a goods language) generated by himself and by other countries. The liability side

here can also more simply be viewed as bonds, link to the He et al. (2015) model of safe asset pricing. It can also be linked to the view of the US as "the world's banker", as in Despres, Kindleberger and Salant 1966.

In that case**, inflation can first be seen as just the corollary of devaluations** (a country that fails to see its monetary funding needs met, ie a country that failed to have its "cake" entirely eaten at the end of a round, devalues. It thus sees the prices of goods imported increase - hence inflation). For an easier mental picture here, since there is an excess of goods being produced in this environment, I would just assume that all goods are imported, from a fictional third-party supplier of goods not playing the game - which is made possible by the normalization of our game to an unique unit of account). **So a devaluation in one's currency would automatically lead to a rise of prices in that country**.

- **in an excess of money environment** (the Price Revolution in Europe after the arrival of gold and silver from the New World, or after the Gold Rush) - in which there is an excess of money being produced compared to the available quantities of goods - each country can be represented by a "mice (the country's aggregated production capacity in a goods language - or its industrial investment capacity in a monetary language), which absorbs the "cakes" (countries' consumption needs in goods language, or their financial investment needs in a monetary language) generated by himself and by other countries.

In that case, a failure to have one's cake eaten totally at the end of a round is sign of unmet consumption demands, which will thus drive prices up.

Thus, in both cases, failure to unload a cake at the end of a round would lead to increased inflationary pressure (hence a single modelling being sufficient to cover both these two cases at once).

I will hence describe from now on our model in a safe asset shortage environment language (that of the past 30 years). While keeping in mind that in case of a serious reversal in world trade, we might "switch" to an excess of money environment, in which case the modelling and approach above will still be valid, with just the nature of the allocated objects being switched (I will see in the paragraph just below that the mechanism that give raise to inflation - the failure to have one's cake eaten entirely at the end of a round - is the same in both environment, even if at different scales and speeds of inflation rates, so that one can view interpret the outputs of the model interchangeable whether we are in the safe asset shortage environment or the other - with again just the scale and growth rate of inflation differing.)

- **What the eating speed, and the cake eating process represent:**

Time is discreet, in rounds, to represent the discretionary decision process of investors such as central banks and asset managers. Each country can be represented by first the "mice" part - or its aggregated investors (central bank reserve managers and asset managers), who stores what they absorbed in the country's aggregated reserves (central bank reserves and asset managers funds). And second by the "cake generating" fiscal part, who generates debt during each round.

To represent private information and secrecy of the decision process, all parameters involved in the decision process (each "mice"'s preference ordering of the "cakes", each "mice"'s absorption

capacity at this round) are decided before the start of each round, and can't be modified once the round starts.

A round can be viewed for instance as a new Treasury bills emission auction for instance. And the different absorption speed ($\omega_{i,T}$ for country i) to reflect the fact that some country's reserve managers have bigger budget and bidding capacities.

Let's note that the fact that the "sequential eating order" within a round doesn't match any "real life" mechanism (except maybe the image of traders executing trades sequentially) is not an object of concern, since only the result at the end of the round (which countries - if any - failed to have their cake fully eaten) matters.

The way they are affected by this shortage is seen at the end of each round, which has a pre-fixed duration. At the end of each round a country's cake that hasn't been totally absorbed will face a devaluation in monetary language - since the rest of the world is denying it its current purchasing power. Also, it will face a reduction in production capacity in goods language - since the rest of the world is not willing to consume its current level of production. Both are reflected in the endowment matrix as a decrease in value of the parts of all reserves that contained pieces of cakes - from all previous rounds, not just this round- from that country. This can be seen as decreasing the values of an entire column j in the endowment matrix, if country j's cake hasn't been totally absorbed by himself or others at the end of the round. So, the endowment matrix remains normalized to an unique unit of account throughout the entire game!

This devaluation could be linked to rollover debt and default à la Calvo (1988) and Cole and Kehoe (2000), as described in He et al. 2015. But it could also be seen as described by the role of limited financial risk bearing by financial intermediaries in the exchange rate determination theory of Gabaix, Maggiori (JPE 2015).

This link to Gabaix, Maggiori (JPE 2015) will be important in the policy implications of our model, and the attempt of designing strategy-proofness of Chapter 10.

- **What countries' utility functions are:**

One question that could arise from the previous paragraph concerns countries' utility functions; how indeed would a decrease in their endowments affect them ?

The question of what utility function each country has is a big one, which impacts directly how countries' rank their preferences (and notably if they would try to "manipulate" the game according to these utility functions).

To answer what utility function each country has, let's first decide how to model whether countries could "manipulate" the game. What would actually manipulation mean in our model ? By manipulating preference rankings, the only outcome that could be changed are:

1) To make countries who would otherwise have unloaded successfully their entire cake fail to unload all of it, hence suffer a devaluation (and so, inflation, reputation... Think of Russia selling off US Treasury bonds in the aftermath of the 2008 Financial crisis, to add panic maybe). However, the world has been mostly peaceful for the past 30 years, so this type of "weaponization" of countries' eating order has been mostly marginal.
2) The second outcome of manipulation would be to allow countries who would otherwise have failed to unload all of their cake unload it successfully, hence providing them some funding (and inflationary) relief which would not correspond to fundamentals. A lighter version of that - let's call it 2)bis - would be to encourage a country to issue more debt than it should have, "for its own good". This could be motivated by development and industrial policy motives - one could for instance think about China funding the US debt to incentivize the latter to consume and invest more in the prior's production capacities

and technologies, even as some American companies or workers suffer from this new competition. However, this motive closer to the political economy sphere has not usually been taken too much into account by monetary theorists and tenants of free markets, which could explain why most (non-Asian) countries don't try to manipulate so much in such a fashion. Similarly, the fact that in real life there are secondary markets on which even a very demanded bond can still be purchased (if needed at a higher price) is not within the scope of study. Indeed, our model is only here to allocate the safe asset shortage, and determine based on countries' preferences and parameters, which ones will be affected by it.

For now, let's assume that countries do not manipulate then (I will come back on that assumption in Part 3, when concerning ourselves with the design of a strategy-proof system). Indeed if we make the approximation that the number of countries manipulating their ordering following "weaponized" motives (as in 1), or following industrialization motives (as in 2) are low, we can then assume that the countries only follow aims of maximizing the value of their endowment matrices, and this only round by round (ie they are not trying to predict over the long run which countries' currencies will appreciate in the long run, nor which countries debt will be more likely to default in the long run).

Countries' behaviors can then be "coded" following a set of criteria, which will also allow us to see what long-term 'natural' tendencies come out of this game. I postulate that in real life most private investors like asset managers don't think about the 'global game' consequences à la He et al., AER 2020, except in an Instability zone à la Farhi, Maggiori, QJE 2018.

Indeed, uncertainty about both other players' private preferences and about future events limit their capacity to be more strategic than looking at safety, through the "history" of in what proportion of time did a country successfully unloaded all his cake, from round 1 until the current round. The case in which players' don't have access to others' private preferences and estimations corresponds in

fact in He et al., AER 2020 to "the case where investor-j is almost sure that fundamentals are $\delta 0$, but is unsure about what other investors know, and whether other investors know that investor-j knows fundamentals are $\delta 0$. If $\delta 0 > \delta*$ then country 1 debt is the safe asset, while if $\delta 0 < \delta*$ then country 2 debt is the safe asset. Given that all investors know almost surely the value of $\delta 0$, investors are then almost sure which debt is safe. Mapping this interpretation to thinking about the world, the model says today may be a day that US Treasury bonds are almost surely safe, i.e., $\delta 0 \gg \delta*$".

Furthermore, I could also add here the observation that fund managers benchmarked on credit indexes with relative notional weighting - so linked to the outstanding debt, such as Barclays Agg, or tracking them, often have to follow the evolution of the bigger weights within this index, who if they issue more debt will also automatically have more of their debt being acquired by managers tracking indexes, since their share within the index will have increased.

So safety is really one of the main parameters determining this preference ordering, which are thus parametrized computationally by weights on the following factors :

- long-term safety, ie what proportions of rounds did the country successfully unloaded all his cake, from round 1 until the current round
- the sizes of each economies, approximated by the sum of reserves that a country i holds from all countries - his own included (ie the "asset" portfolio of country, seen as the sum of line i in the endowment matrix)

I also introduce interest rate as a weighted parameter in this, so as to study how "natural interest rates" would evolve in such a game. Indeed, I add the deterministic rule that, after some random initialization of countries' initial interest rate at round 1, at each round that a country succeeds in unloading all of its cake it will lower the interest it promises debt holders, whereas at each round that a country fails to unload all of its cake and suffers devaluation he will raise this interest rate, to make his debt more attractive.

Finally, I introduce a qualitative "alliance graph", called trading_preferences below, to allow for exogeneous preferences of some countries for others. This will also enable us to model in Part 2 shifts in trade environment, or to implement the manipulation à la 2)bis defined above. I explore that way in Part 2 a few different alternatives of debt, reserves, interest rates and inflation evolution following the Covid shock, depending on how the US-China confrontation evolves.

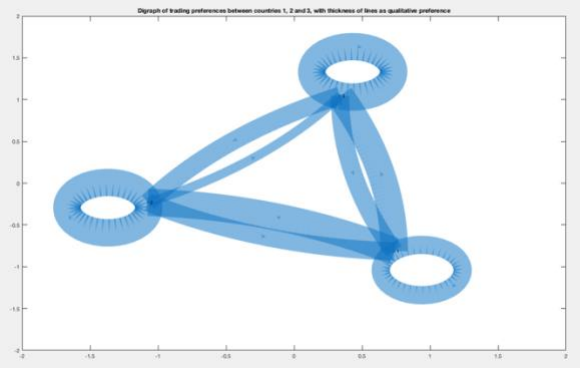
For instance, from the 1945-now simulations, the trading_preferences matrix between the US (i=1) , the UK (i=2) and France (i=3) trading with each other in 1945 until 1953 can be written trading_preferences = [3 2 2 ; %US prefers doing business with others 2 3 2 ; %UK prefers with itself 2 2 3]; %France prefers with itself as well

$$TradingPreferencesExample = \begin{bmatrix} 2|3|3 \\ 2|3|1 \\ 2|2|3 \end{bmatrix}$$

Which means that the US (line 1) relatively prefers absorbing the UK (j=2) and France's (j=3) debts, both with value 3 in that matrix, than absorbing its own (case i=1, j=1, with value 2). Similarly, the UK prefers first absorbing its own value (case i=2, j=2, with value 3), then absorbing the US' debt (case i=2, j=1, with value 2), and lastly France's (case i=2, j=3, with value 1). France prefers indifferently its own debt or the UK's, but not as much as it likes American debt.

This trading_preferences matrix thus introduce personalized bias that any one of countries hold toward the others, even as the other parameters described above (safety, interest rate and size of economies) gives a ranking of countries common between all of them.

This matrix can also be represented by the digraph below, with the thickness of the lines linking the 3 nodes representing their relative bias in favour of each other. I will use this representation later in simulations.



So the exact coding of the preference ranking, determined by each country round by round, is as follow (and can be found in the code that you can run yourself below) :

[~,trading_order]=sort(trading_preferences(k,:).(ones(1,number_of_countries)+max(0,successfully_loaded_cake_last_round(k,1).(history_counter(k,1)-deval_history(k,1)).endowments(k,:)(interest_rate(k,1)))),'descend');

That also takes us back to the original Bogolmonaia and Moulin's ordinal efficiency notion, in which preferences are declared only over sure objects, and not subsets of objects taken together.

- What determines countries' cake size and cake eating speed at each round:

I also model countries to have exogeneous growth rules, simple mechanistic rules : when at the end of a round a country managed to successfully unload all of its cake there's demand, so it will increase the size of the cake issued the next round, until that hits a threshold - in which case it will start over with a very prudent issuance. The argument for that would be an "electoralist" spending view, à la Barro-Gordon.

Also, we can recall the He et al. AER 2020 conclusion I mentioned earlier, "when countries are roughly symmetric and when global demand for safe assets is high, countries will engage in a rat race to capture a safety premium. Starting from a given smaller debt size, and holding fixed the size decision of one country, the other country will have an incentive to increase its debt size since the

larger debt size can confer increased safety. But then the first country will have an incentive to respond in a similar way, and so on and so forth.

Their second result, however, that "when countries are asymmetric and one country is the natural “top dog.” In this case, the larger debt country will have an incentive to reduce debts to the point that balances rollover risk and retaining safety, while the smaller country will have an incentive to expand its debt size" has not been validated by a reduction of US debt since the 90s!

The eating speed at a round is approximated by the sum of debts that a country i has issued up to this round, across all countries that hold it (ie the sum of column i in the endowment matrix resulting from the previous round). Indeed that gives a proxy of how developed a country's financial sector is (since the eating speed at that round determines the total quantity of debt - no matter from which country - that this country will absorb during this round, which can be formalized by the following equation: $\sum_{j=1}^{N}(c_{i,j,T}) = \omega_{i,T} * \text{durationOfRound}_T$

Finally, let's conclude our model's description by noting that the combination of the fact that countries "mechanistically" rank preferences (and according to exogeneous biases), and follow "mechanistic" growth rule,

- they don't solve some dynamic problems, one round at the time
    - the combination of the two points above (mechanistic debt issuance and mechanistic preference ordering) makes them not solving dynamic problems (except in the two manipulation cases described above)
    - strong approximations but the only way to simulate long term trends (many rounds) among many agents. And can empirically reproduce historical trends and simulate alternative scenario

(d) Results from the model (that can be reproduced using the code in the interactive notebook online - https://bit.ly/inflationSAS) - the incentives and trends it produces

I have described above the demand side, and the deterministic rules guiding the supply side (the exact coding of the supply side can be seen in the code cells below, which you can change and relaunch yourself using the "Cell" button at the top of this interactive notebook. Basically the supply side starts by some random initialization, then whenever a country does not suffers a devaluation then it will try to increase the size of the cake it will generate at the following round, and if there is a devaluation it will reduce the size of the cake it will generate at the following round. The absorption speed for each country at each round is a function of the size of its total reserves, as a proxy of its GDP for instance).

One could encode in the supply side more sophisticated monetary rules such as the Taylor one, or some cyclical aspect like the domestic financial cycles described by Borio et al (2020).

But for now our simple simulations (that you can reproduce yourself with the code provided below, and that you can run directly in this interactive notebook) already shows the following figures and results:

First a 6 countries in 3 trade groups, 7 rounds simulation (just 7 rounds are enough to see trends !)

- in our simulations the interest rates are computed deterministically - after a random initialization, after every round during which a country successfully (unsuccessfully) unloaded the piece of "cake" it generated during that round its interest rate will be decreased (increase). It is for us a very visual way to see how much inflationary pressure

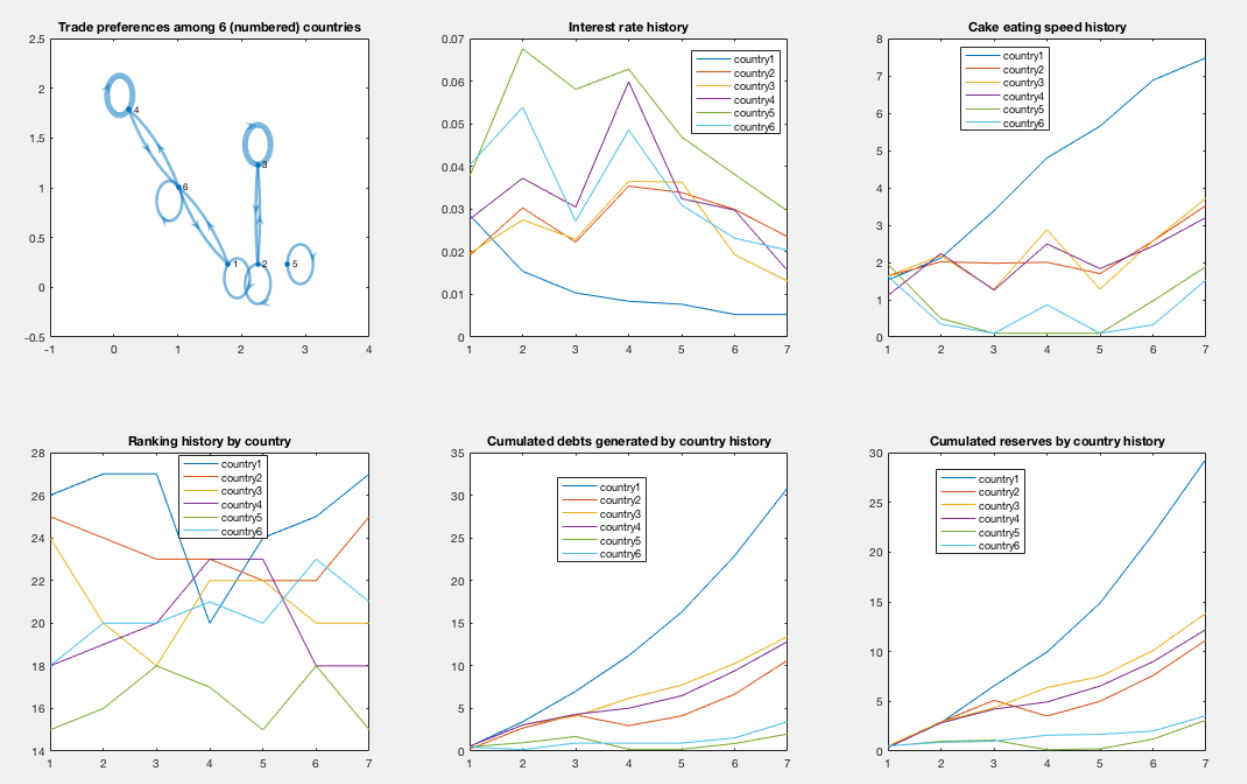
there is on a country round after round (so how flat its AS curve is - the higher that "interest rate" the steeper it will be).

- the size of cakes, absorption speed... all tend to powers law i.e. one country (here country 1) gains much more than any more in that trading group (mathematical proof in paper). Intuition is that as it is perceived "safer" by other countries (because it devalues less) the "cakes" it generates are always eaten first by other countries, and thus this "popularity margin" / "monetary latitude" allows country 1 to emit bigger cake later, invest more in its cake absorption speed (proxy of GDP), absorb more in other countries' cakes as well, etc.

This already highlights how the USD's position as the dominant reserve currency is easily self-sustaining, and allows its monetary policies to reach for lower rates without funding or inflationary pressure (simulations and calibrations in Part II will explore more closely the limits of even a dominant reserve currency, and the conditions in which Triffin events might arise).

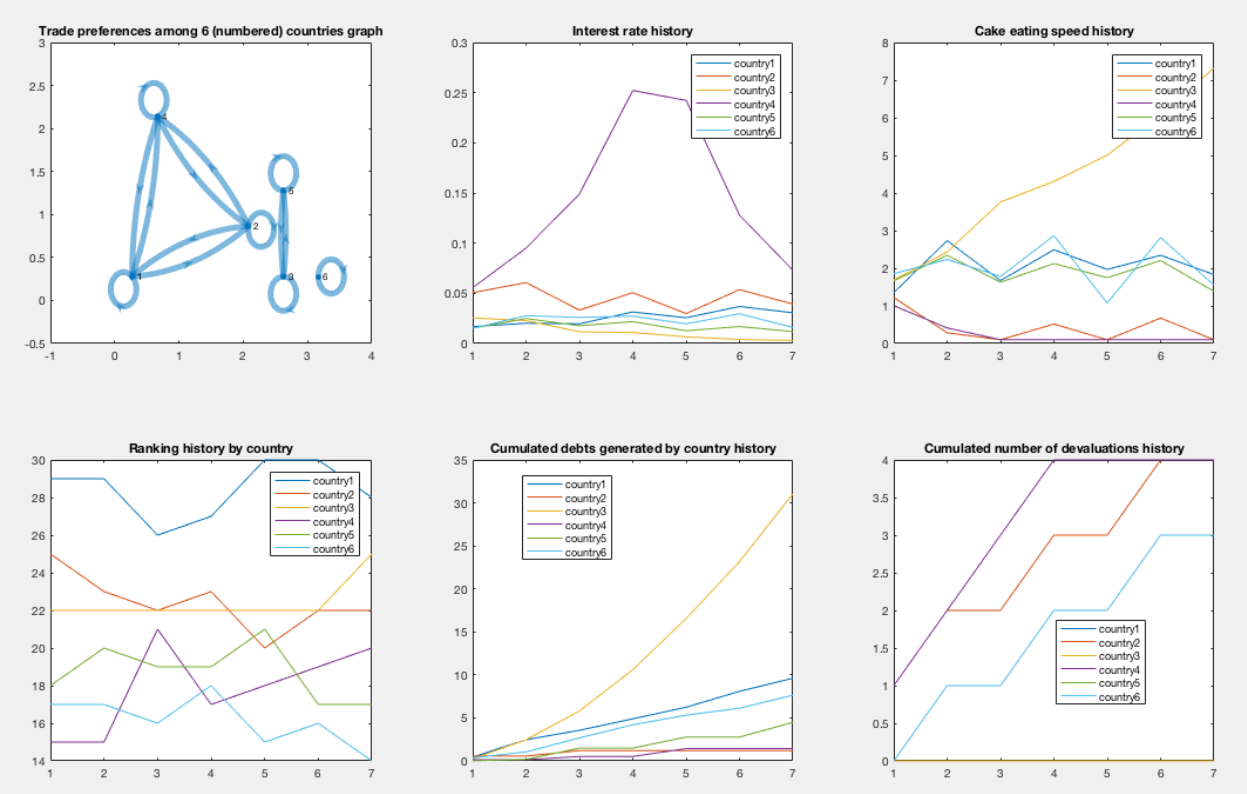
Additional observations:

- the country that would gain the most is determined by initial conditions (in this very easy example everything is initialized at random, but looking at the initial ranking - the higher the score the most sought after a ranking is - and the initial interest rate I can already tell that country 1 will be winning !)
- the country that would gain the most in a trade group is not necessarily the one determined by fundamentals - i.e. not the most connected one or the most prudent one (in the trade group between country 1, 4 and 6 country 1 is neither the most connected - since country 6 has more connections than it does - nor the most self preserving - since country 4 ranks its own debts to others' higher first)



A second 6 countries in 3 trade groups, 7 rounds simulation

- Here the winner is country 3 - which is less connected (only to country 5) than the cluster with countries 1, 2 and 4
- The worse off country in the group (1, 2 and 4) is doing even worse than country 6 in autarky (extreme case of the model, because country 4 started (randomly) at the least preferred country in country rankings, and failed to get its cakes eaten at the end of round 1, thus devalues round 2, its interest rate surge, and it gets stuck in a devaluation spiral from round 1 to 4.
- Note that here country 1 had better initial conditions to be the be winner of the simulations (best ranked country at the start, lowest interest rate at the start). But its trading partners - country 2 and 4, are the ones devaluing the most



Finally a 9 countries, 1000 rounds simulation

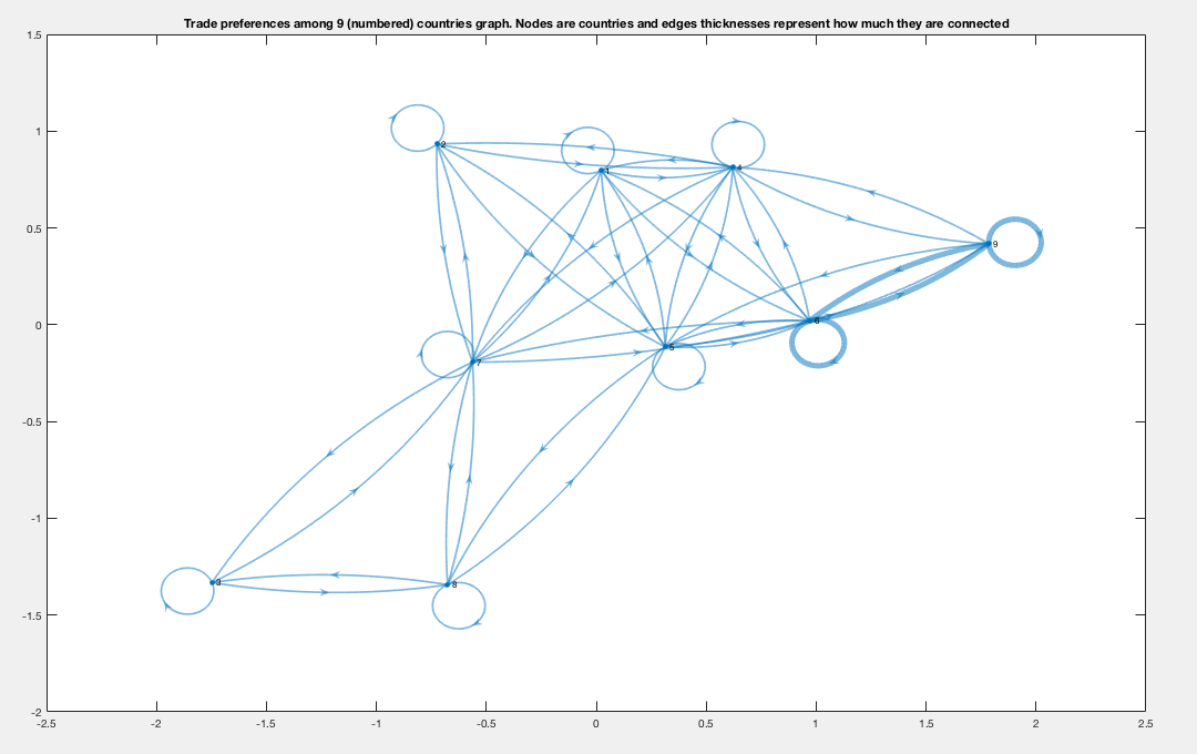
The figures below illustrate the long rung trends in this model :

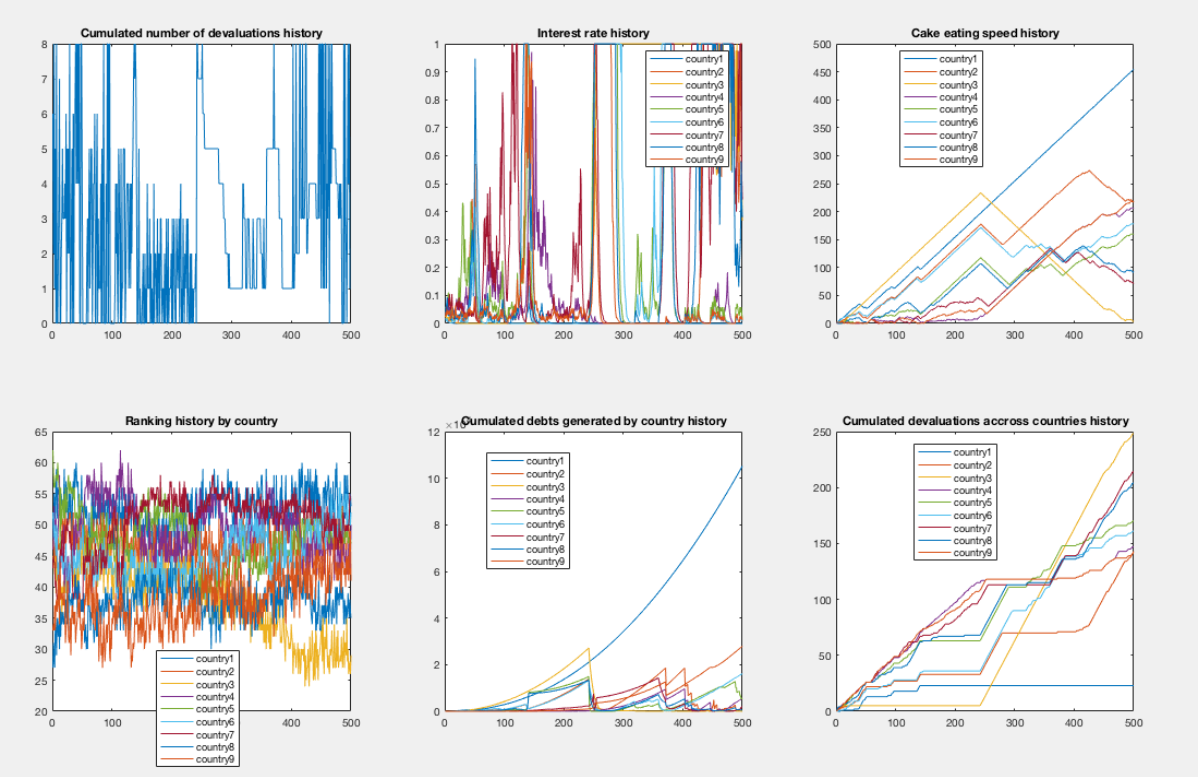
- Reduction of average global rates / average global inflationary pressure can happen (see rounds 120 to 220 on both the cumulated. This is when the total absorption speed is faster than a period's timer times the total generated cakes in each of these rounds, hence the reduced number of devaluations rounds 120 to 220

Indeed, in a world with a floating monetary anchor inflation could be seen as a corollary of the levels of stock view imbalances. The fact that traders are mainly reasoning - unconsciously but also consciously - along short-termist, flow views of markets, make them blind to this stock imbalance buildup - otherwise the financial risk buildup - that thus only becomes visible during bursts. Hence

the link between Caballero, Farhi, and Gourinchas' asset shortage hypothesis, and Borio et al's financial cycle buildup hypothesis.

- Triffin events exist: the yellow country (country 3) started as the winner of this simulation, until around round 220 at which point it is overtaken by country 1 in deep blue and don't stop devaluing until the end of the 1000 rounds. This corresponds to fundamental analysis (country 3 is only trading with 2 countries whereas country 1 with 4. But countries 6 and 9 for instance are both connected to 4 trading partners, with stronger ties among some of them and with themselves. These two countries are in respect the 2nd and 3rd most sought after countries, both in rankings, in upward trends in rankings, and in how much of their cakes are absorbed by others as reserve).





(e) Some extensions - estimating counterfactuals, fiscal latitude and yield curve control feasibility

Our computational and game-theoretic model can also provide guidelines for policies such as yield curve control, and conditionality on their feasibility. In fact, given privacy-preserving surveys such as those described in Abbe, Khandani, Lo, AER 2012, institutions such as the BIS could use aggregated data to estimate how much governmental bonds can be issued by each country without a downgrading of its financing conditions and a potential raise in inflation, all other parameters held equal.

For instance, a simple calibration of our model coded in the online interactive notebook (https://bit.ly/inflationSAS) will show how the evolution of the inflation rate, the financial cycles, and reserve composition of the main economies, from 1945 to now, can be obtained from just a few initial (and two discretionary) inputs. For that I first calibrate, by just initializing with data from 1945,

and changing three times some preferences (the Marshall plan between 1948 and 1951, US investments in Japan between 1953 and 1955, and China's opening since 1978), to reproduce by letting the game play by itself the main trends observed from 1945 to now (2020), and to obtain after 75 rounds today's reserve composition. Being able to capture these features of past history will provide confidence and intuition in the model's inner workings.

That also lead us to provide several scenarii in how the models' parameters will change following Covid-19's increase in debts (these parameters from the model being for instance the change in debt levels, while debt absorption speed are maintained roughly constant. I will discuss these more in details in Chapter 10. Different degrees in shifts in trade and supply chain preferences are also considered). I thus generate 50 more rounds after a common departing point, and report here the different outcomes, and the different probabilities of each outcome (since they are intervention of random perturbations in the model the probabilities of each outcome is calculated based on how many of different random sequence generate this specific outcome). The details are accessible there https://mybinder.org/v2/gh/NicolasXYZ/MPC_experiment/master?filepath=second_notebook.ipynb. In both notebooks, one can run the exact coding to see the current results, and modify the code at will to test out new ideas.

This computational and game-theoretic model can thus provide guidelines, through simulations such as the ones I did, for policies such as yield curve control, and conditionality on their feasibility.

Chapter 9: Empirical testing of the model presented here: US inflation regressed on foreign central banks' reserve size and composition variations (here China, Japan)

NB: more data, procedure and results can be found at the following link: https://docs.google.com/document/d/1iCrCGe507SbsV-xF7tR0BfAX0yVDUSydcwcZ5TdDy60/edit?usp=sharing

These regressions are used to support our "cake-eating" model of the international monetary system, linked the safe asset shortage hypothesis on long-term rates and inflation with the rollover risk model of He, Krishnamurthy and Milbradt (AER 2019) through a multiperiod, multiagent risk allocation model.

(a) Main findings:

No correlation/causation between PBoC reserve changes and US inflation except between 2012-2015 (with a negative coefficient) and between 2018-now (with a positive coefficient). Bank of Japan holdings of US Treasury linked to US inflation prior to 2009.

(b) What I want to prove using these regressions

To support that globalization and new entrants in world markets could have driven down long-term rates and inflation (a hypothesis first formulated by Rogoff, 2003), I built a game-theoretic model of imbalance allocation across central banks in the spirit of Farhi, Maggiori, 2017.

The "cake-eating" allocation scheme from Bogolmonaia and Moulin provided us with an illustrative (and computational) way to simulate the incentives created over the long run by the current anchors. However, at its core, one could simplify it as "US inflation will lower/stay low as long as other countries agree to exchange USD against their exports". Importantly, what is true over the long run should be (at least partially) reflected in short-term variations of the studied quantities.

I will thus focus on studying these short-term (monthly) variations, especially around periods of central bank policy break, to see changes in the relationships (regression coefficients) before and after the breaks. Proving that foreign central banks' actions DO have an impact on US inflation, even on short-term fluctuations, will give an intuition of how, *a fortiori,* the external component of inflation ("external" as opposed to the part of inflation directly managed through the domestic central bank's rates, which I will call "internal") could have contributed to a worldwide "disinflation" over the past 30 years - following Rogoff's expression.

(c) A first "sanity check" regression on US inflation and PBoC reserves

If the external component of inflation is viewed as the result of a balancing process between imported goods on the one hand, and acceptance of one's currency as payment for the imports on the

other ("acceptance" formalized through holdings in foreign central banks' reserve accounts), the evolution of foreign central banks' holdings of US Treasury bills could be an indicator of the state of this balance through time, which I can symbolize as:

ForeignComponentOfUSInflation_t = Goods from all Trading Partners_t / Amount of USD held by all Trading Partners_t (equation 1)

One could either regress the *entire* amount of US Treasury bills held by *all* foreign entities, or focus on a few single large holders of it. I chose the latter, since it will allow easier interpretations of "breaks" in foreign central banks' reserve investment policies - in the vein of a narrative approach to explain regression coefficient changes.

Let's start with a regression between US inflation and the evolution of reserves held by the People's Bank of China (PBoC). This regression should be the most obvious sanity check since China is the US' biggest trading partner, and that both economies present the largest (reversed one vs the other) imbalances. Examining the entire reserve evolution of the PBoC (vs examining just the dollar denominated part of it) should also cover the effects on US inflation created by US imports from China, by Chinese direct investments to the US, and by the effects created by the long-term storing of US Treasury bills mentioned in (simplified) equation 1.

--

Let's first see whether each of these three effects would be accounted for, and in which ways their movements would be related to movements in US inflation.

If one recalls the definition of the national account balance between, the current account (CA), the capital account (KA) and the reserves (ORT) are linked through the equation

CA + KA = - ORT (equation 2)

However, to be able to link movements in Chinese CA, KA and ORT with that of US inflation, let's distinguish, as in our full model paper, two mutually exclusive situations depending on whether the balance of goods vs safe assets tilts. The first situation will be that of "safe asset shortages", during which there's overproduction of goods - hence a less elastic numerator on the right-hand side of equation 1, so that most movements in the **ForeignComponentOfUSInflation_t** are driven by movements in the denominator of the right hand side of equation 1 (think of the world economy after the 2008 Financial Crisis, during which China had too much production capacity). The second situation is that of "goods shortages", during which there's a shortage of goods (for instance of PPE during the Covid pandemic). Then it is mainly fluctuations in quantities of this numerator that drive movements in **ForeignComponentOfUSInflation_t.**

Let's see how the above links could be measured between the PBoC's balance sheet and US inflation. Viewed from the PBoC, if we are in a goods shortage situation, when CA goes up (↑), and when KA goes up (↑), both upward trends would results in an upward trend on US inflation (since CA ↑ could be viewed as more imports from the US, so an occasion to renegotiate prices for Chinese exporters in the goods shortage; and KA ↑ can be viewed as a "drop" of a higher amount of more in the US, some of which will contribute to higher imports and renegotiation). So in that case the coefficients in front of Chinese reserves should be positive in their regression against US inflation, *if there are no significant changes in the storage of US denominated reserves at the PBoC that would "interfere", as described by simplified equation 1.*

In an excess of goods situation, when CA and KA go up (↑) inflation goes down (↓), since there's more goods for roughly the same import prices (excess production of goods so exporters are happy to sell anything at any price - reversed bargaining power). So in the blue case an increase in the

trading counterparty (here China)'s reserves should be reflected by a decrease in the importing party (here the US)'s inflation - so negative regression coefficients, *if there are no significant changes in the storage of US denominated reserves at the PBoC that would "interfere", as described by simplified equation 1.*

The effect from official reserve transfer (ORT) from China on US inflation is for its part more complicated and mixed. Indeed, the part of it that is invested in US Treasury bills should contribute to lower US inflation, following our cake-eating model (as in the simplified equation (1) above, an ↑ in China's holdings of USD denominated reserves would ↑ the denominator of the right hand side of the equation, so ↓ US inflation). So if the cake-eating model is proved to be correct, one will not be able to simply say, in a goods shortage case (the red case above) that "when PBoC reserves ↑ US inflation will also ↑ through pure import effects", because of the reverse effect that dollar denominated changes in Chinese reserves have on US inflation. However, in the safe asset shortage (the blue) case above "when PBoC reserves ↑ US inflation will ↓ through both import effects, FDI effects, AND through the addition of Treasury bills in the PBoC's reserves".

--

Let's measure both of these in different points in time of the PBoC's history (along with its policy changes, which provides great break points for a narrative causality approach).

Let's first note that for most of the history since China's reopening, there's no statistically significant link between Chinese reserve movements and US inflation. This might be interpretable as we would be in the goods shortage case (the red case above), with both constant buying AND selling of dollar denominated reserves by the PBoC to keep the exchange rate smoothed.

Except, however, during the following : **January 2012-August 2015** and **May 2018-now, during which I can show cointegration and Granger-causality** (following the Toda and Yamamoto (1995) procedure, see appendix and stata logs)

(d) Regression 1 : between January 2012 and August 2015, PBoC v US inflation

I perform a VAR between (all data are monthly percentage changes computed from FRED. The input file can be seen there along with the calculation formulae. Finally dropping some of the variables below don't change the results much, as reported in the appendix)

- monthly change in US inflation (less food and energy)
- monthly variations in exchange rates
- monthly change in effective Fed Fund rates
- monthly change in energy prices
- monthly change in total Chinese official reserve changes (less gold)
- monthly change in inflation expectation (Michigan University surveys of consumers, retrieved from FRED)
- monthly change in US GDP (it sometimes breaks the stability of the VAR, in which case I extended the period of regression a bit - see stata logs in appendix)

I add the following constraints in the VAR :

- The coefficients in front of all lags of ***monthly change in total Chinese official reserve changes (less gold)*** are null in the equations of the ***monthly change in***

effective Fed Fund rates and in that of ***monthly change in inflation expectation*** (since according to current theories the first term should not affect US inflation)

- The coefficients in front of all lags EXCEPT the first of ***monthly change in inflation expectation*** are null in its equation (since I argue that one will look at previous months' actual inflation numbers instead of older expected numbers)

I regress on 2 or 3 lags, selection by BIC and AIC respectively (the results don't change much between these) ; the Toda and Yamamoto Granger results are (the exact coefficients, residuals, and postestimation cross-check procedures are reported in the appendices of this document)

vargranger

Granger causality Wald tests

Equation	Excluded	chi2	df	Prob > chi2
InflationMOMLes~y	ChangesInEffect~s	.9528	2	0.621
InflationMOMLes~y	ChinaReserveCha~t	7.8056	2	0.020
InflationMOMLes~y	ChangeInInflati~C	3.2651	2	0.195
InflationMOMLes~y	ALL	10.499	6	0.105
ChangesInEffect~s	InflationMOMLes~y	.74665	2	0.688
ChangesInEffect~s	ChinaReserveCha~t	.	0	.
ChangesInEffect~s	ChangeInInflati~C	3.5465	2	0.170
ChangesInEffect~s	ALL	4.3231	4	0.364
ChinaReserveCha~t	InflationMOMLes~y	.43999	2	0.803
ChinaReserveCha~t	ChangesInEffect~s	.75153	2	0.687
ChinaReserveCha~t	ChangeInInflati~C	8.0712	2	0.018
ChinaReserveCha~t	ALL	10.407	6	0.109
ChangeInInflati~C	InflationMOMLes~y	4.8788	2	0.087
ChangeInInflati~C	ChangesInEffect~s	.767	2	0.681
ChangeInInflati~C	ChinaReserveCha~t	.	0	.
ChangeInInflati~C	ALL	5.2971	4	0.258

--

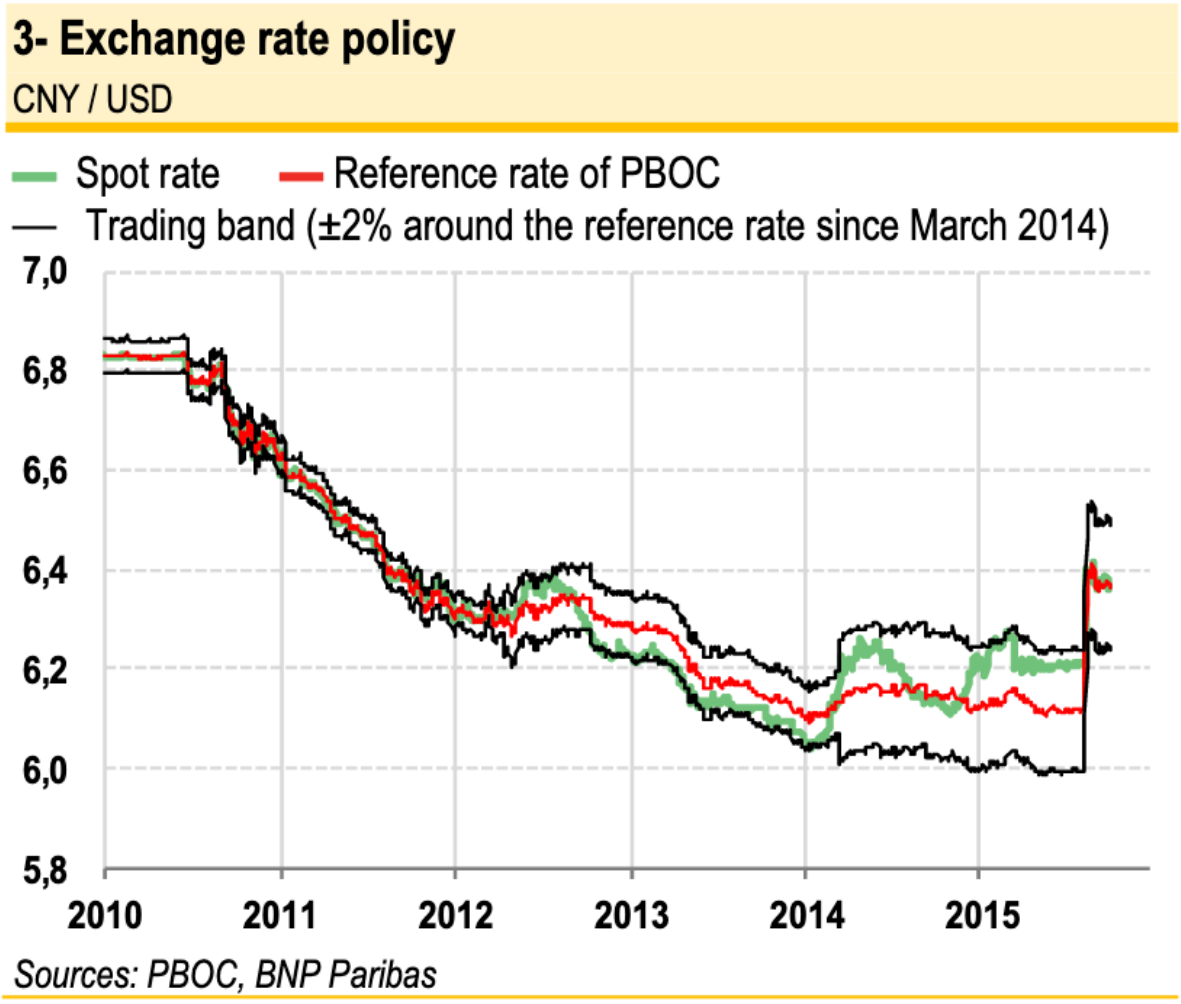
I see a (Granger)-causality between month-to-month changes in PBoC reserves and in month to month change in US inflation (less food and energy), during the January 2012-August 2015 period !

And actually every month that I add before or after that period to the regression *reduces* the statistical precision of the estimates (see appendix just below). A "heatmap" of confidence intervals ranges for each regression starting month to ending month makes this very apparent, and the January 2012-August 2015 period particularly stands out (as outside of it, the Granger causality totally disappears). NB : the coefficient is (statistically significantly) negative !

--

What has been so special during this period

Let's recall the reforms the PBoC introduced gradually, to internalize the RMB. These reforms (illustrated on the graph below) allowed exchange rates to be more market based (with less interventions from the central bank - so less high frequency buying and selling of US denominated reserves, i.e. less mitigating effects on the regression of US inflation and PBoC reserve movements). However, these brutally stopped in August 2015, as to stop a capital flight the PBoC reintroduced strict management of the exchange rate policy (and frequent interventions in markets that tamper with the regression coefficients - here negative!).



And the negative coefficient in front of Chinese reserve changes in the US inflation equation

(More on it in appendix and in stata logs, links of which are provided in appendix) **:**

--

Vector autoregression

Sample:	2012m1 - 2015m10		Number of obs	=	46
Log likelihood =	-136.6763	(lutstats)	AIC	=	-8.297088
FPE =	.0005011		HQIC	=	-7.820552
Det(Sigma_ml) =	.000062		SBIC	=	-7.024989

Equation	Parms	RMSE	R-sq	chi2	P>chi2
InflationMOMLe~y	14	.605815	0.3462	23.49918	0.0361
ChangesInEffec~s	11	.013108	0.1065	9.310842	0.5029
ChinaReserveCh~t	14	1.08135	0.3110	34.6092	0.0010
ChangeInInflat~C	8	10.7828	0.1488	5.985545	0.5414

(1) [ChangeInInflationExpectationMIC]L.ChinaReserveChangeInPercent = 0
(2) [ChangeInInflationExpectationMIC]L2.ChinaReserveChangeInPercent = 0
(3) [ChangesInEffectiveFedFundRates]L.ChinaReserveChangeInPercent = 0
(4) [ChangesInEffectiveFedFundRates]L2.ChinaReserveChangeInPercent = 0
(5) [ChangeInInflationExpectationMIC]L.ChangeInInflationExpectationMIC = 0
(6) [ChangeInInflationExpectationMIC]L2.ChangeInInflationExpectationMIC = 0
(7) [ChangeInInflationExpectationMIC]L3.ChinaReserveChangeInPercent = 0
(8) [ChangesInEffectiveFedFundRates]L3.ChinaReserveChangeInPercent = 0
(9) [ChangeInInflationExpectationMIC]L3.ChangeInInflationExpectationMIC = 0

	Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
InflationMOMLessFoodEnergy						
InflationMOMLessFoodEnergy						
L1.	-.4209349	.1777648	-2.37	0.018	-.7693475	-.0725223
L2.	-.3705439	.1578024	-2.35	0.019	-.6798309	-.061257
ChangesInEffectiveFedFundRates						
L1.	-.0190861	8.489985	-0.00	0.998	-16.65915	16.62098
L2.	-8.068017	8.27118	-0.98	0.329	-24.27923	8.143197
ChinaReserveChangeInPercent						
L1.	-.2309308	.0879322	-2.63	0.009	-.4032748	-.0585868
L2.	.1027562	.0865018	1.19	0.235	-.0667842	.2722966
ChangeInInflationExpectationMIC						
L1.	.0249073	.0138803	1.79	0.073	-.0022976	.0521123
L2.	.0205913	.0173005	1.19	0.234	-.013317	.0544995
InflationMOMLessFoodEnergy						
L3.	-.2905184	.1758026	-1.65	0.098	-.6350852	.0540484

(e) Regression 2 : between May 2018 and July 2020, PBoC v US inflation

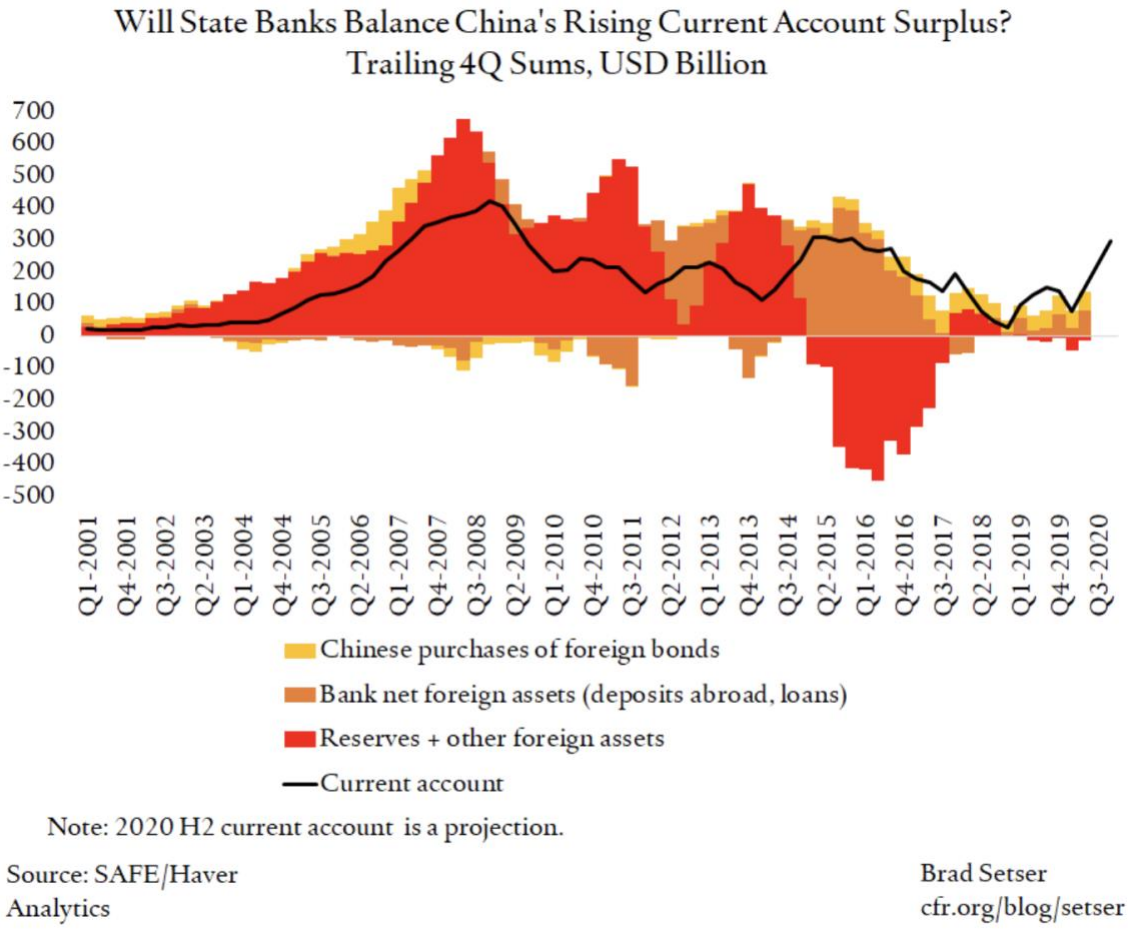
I perform the same VAR, with the same data and with the same constraints.

I find : a significant (Granger)-causality between month-to-month changes in PBoC reserves and in month to month change in US inflation (less food and energy)**, but now with a statistically significant positive sign for the coefficient in front of PBoC reserve changes !**

--

How can this be explained?

First, according to the framework I have followed so far, a positive sign for this coefficient should be the mark of a goods shortage (the red) case. However, in that case the effect of the buying/selling of US Treasury should have mitigated the effect of just CA and KA, so that link should have been hard to measure! One element of explanation for why this movement in US Treasury holding effect has not been prevalent could be in Brad Setser's "tracking" of the missing reserves from the PBoC, since Q2-2018. Indeed, a hypothesis is that the PBoC stopped buying Treasury bills, and "delegated" the reserve accumulation role to State banks, for various reasons. Therefore, the effects of PBoC reserves on US inflation should only reflect the ↑ arrows, as described in equation 1 and 2 at the start, with a (here statistically significant) positive coefficient in front of PBoC reserve change in the US inflation regression.



(f) Regression 3: Japan holdings of US Treasury vs US inflation, 2000-2009 - (an attempt at) directly measuring foreign holdings of Treasury effect on US inflation

I perform the same VAR, except that I replaced PBoC reserve data with Japanese holdings of US Treasury data (from treasurydirect.gov instead of FRED)

I apply the same constraints in the VAR:

I can now observe that between 2000 and 2009, there's a slight Granger causality between US inflation and variation in Japanese holdings of US Treasury. And, of more interest for our study here,

this correlation/(Granger)-causation totally disappears after 2010, with a break in the coefficients of the regression (that can be tested with a Chow test). See the 2 Granger causality table before and after 11/2009 below, to see the difference in explicative power of Japanese holdings of US Treasury vs US inflation.

Before 11/2009 :

```
. vargranger
```

Granger causality Wald tests

Equation	Excluded	chi2	df	Prob > chi2
InflationlessFo~y	ChangesInEffect~s	.28073	2	0.869
InflationlessFo~y	ChangeJapaneseH~s	5.3889	2	0.068
InflationlessFo~y	MOMChangesInEne~y	6.8329	2	0.033
InflationlessFo~y	ChangeInInflati~C	2.4521	2	0.293
InflationlessFo~y	ALL	14.641	8	0.067
ChangesInEffect~s	InflationlessFo~y	.51481	2	0.773
ChangesInEffect~s	ChangeJapaneseH~s	.	0	.
ChangesInEffect~s	MOMChangesInEne~y	.6816	2	0.711
ChangesInEffect~s	ChangeInInflati~C	1.7681	2	0.413
ChangesInEffect~s	ALL	3.8738	6	0.694
ChangeJapaneseH~s	InflationlessFo~y	.34826	2	0.840
ChangeJapaneseH~s	ChangesInEffect~s	.54366	2	0.762
ChangeJapaneseH~s	MOMChangesInEne~y	2.4017	2	0.301
ChangeJapaneseH~s	ChangeInInflati~C	7.4764	2	0.024
ChangeJapaneseH~s	ALL	11.043	8	0.199
MOMChangesInEne~y	InflationlessFo~y	.10004	2	0.951
MOMChangesInEne~y	ChangesInEffect~s	3.8717	2	0.144
MOMChangesInEne~y	ChangeJapaneseH~s	2.2062	2	0.332
MOMChangesInEne~y	ChangeInInflati~C	.91419	2	0.633
MOMChangesInEne~y	ALL	6.6174	8	0.578
ChangeInInflati~C	InflationlessFo~y	7.1812	2	0.028
ChangeInInflati~C	ChangesInEffect~s	.02665	2	0.987
ChangeInInflati~C	ChangeJapaneseH~s	.	0	.
ChangeInInflati~C	MOMChangesInEne~y	6.2127	2	0.045
ChangeInInflati~C	ALL	12.078	6	0.060

After 11/2009 :

```
vargranger

Granger causality Wald tests
```

Equation	Excluded	chi2	df	Prob > chi2
InflationlessFo~y	ChangesInEffect~s	1.0787	2	0.583
InflationlessFo~y	ChangeJapaneseH~s	1.1063	2	0.575
InflationlessFo~y	MOMChangesInEne~y	5.5714	2	0.062
InflationlessFo~y	ChangeInInflati~C	.46731	2	0.792
InflationlessFo~y	ALL	9.0424	8	0.339
ChangesInEffect~s	InflationlessFo~y	.72568	2	0.696
ChangesInEffect~s	ChangeJapaneseH~s	.	0	.
ChangesInEffect~s	MOMChangesInEne~y	2.6245	2	0.269
ChangesInEffect~s	ChangeInInflati~C	.17529	2	0.916
ChangesInEffect~s	ALL	4.6202	6	0.593
ChangeJapaneseH~s	InflationlessFo~y	9.9409	2	0.007
ChangeJapaneseH~s	ChangesInEffect~s	10.227	2	0.006
ChangeJapaneseH~s	MOMChangesInEne~y	1.8216	2	0.402
ChangeJapaneseH~s	ChangeInInflati~C	2.5679	2	0.277
ChangeJapaneseH~s	ALL	25.783	8	0.001
MOMChangesInEne~y	InflationlessFo~y	9.8283	2	0.007
MOMChangesInEne~y	ChangesInEffect~s	1.7002	2	0.427
MOMChangesInEne~y	ChangeJapaneseH~s	.28366	2	0.868
MOMChangesInEne~y	ChangeInInflati~C	12.293	2	0.002
MOMChangesInEne~y	ALL	24.053	8	0.002
ChangeInInflati~C	InflationlessFo~y	2.2136	2	0.331
ChangeInInflati~C	ChangesInEffect~s	.70366	2	0.703
ChangeInInflati~C	ChangeJapaneseH~s	.	0	.
ChangeInInflati~C	MOMChangesInEne~y	7.0156	2	0.030
ChangeInInflati~C	ALL	9.5888	6	0.143

One potential explication, following the framework I have applied so far, is to say that since the Bank of Japan was purely accumulating US Treasury reserves until 2009-2010, but then started managing its reserve following other rules. For instance, it could have started to buy and ALSO sell significant amounts of them after the great financial crisis, vs only buying before - which then mitigates the effects from Japanese CA and KA on US inflation after the GFC. We would thus be in the blue case described earlier.

Japanese reserve

Chapter 10 – our policy proposals, and implementation of our encryption and mechanism design schemes

(a) Executive summary

Mundell's redundancy (or n-1) problem illustrates how international finance can be viewed as a zero-sum game, with many prisoner's dilemma problems. Until now, international monetary agreements have relied on specified external anchors (gold, USD, bancor) to facilitate coordination and commitment- indeed, if one views the results of monetary negotiations as a Nash Demand Game with irrevocable commitment from all players to follow, then defining an external anchor is a way to surely enforce this contract. However, that anchoring process creates lengthy, hazardous and always inopportune international negotiations. I will therefore offer in this paper a protocol to improve such negotiations around anchoring. In fact, one of the main insights of the model exposed in Chapter 9 is that simple forms of privacy-preserving aggregate demand and supply estimation could lead to more flexible forms of anchoring. I derive an illustrative example built on currently mature such privacy-preserving technologies and providing a concrete implementation of the previously theoretic "planner" dear to mechanism designers - here to guarantee flexibility in the anchoring, and thus long term international monetary and financial stability. For that, I go to great length to make sure such flexible monetary anchoring performs better not only facing "the three inescapable problems" associated with changes and transitions in monetary systems: "the disruption of foreign exchanges and the collapse of monetary and credit systems", "the restoration of foreign trade", and "the supply of the capital that will be needed virtually throughout the world for reconstruction, for relief and for economic recovery" (White,

1942, in his drafts for the Bretton Woods conference), but also during periods of stability, by providing parameters through which control the path of global natural rates.

(b) A role for market design in international macro-finance design

The village economy analogy I used in the motivation of our model exposed in Chapter 8 naturally calls for game theory models, such as those underpinning the contract theory, borrowing and lending and insurance literature exposed in Chapter 4 (Part I). I started with the basic building block of Bogolmonaia and Moulin (2001)'s cake-eating game, which I believe that this model provides a close analogy to real life operations by central bank officers, and illustrates in a different fashion than existing models such as Mundell-Fleming how safety considerations are being carried out in real life, along with risk vs returns logics. Furthermore, this highly abstract model can merge well with existing macroeconomy models, by determining more accurately calibration values in existing models (curves' slopes, elasticities...). Indeed, I believe that the superposition of games with incentives on top of existing models are not competing but complementary views, just as Roth's suspension bridge building analogy illustrates how in addition of "simple, beautiful and indispensable physics", "bridge design also concerns metal fatigue, soil mechanics, and the sideways forces of waves and wind". International macroeconomics also unfolds within a game of economic competition and collaboration, whose rules - which "might even be impossible to be answered analytically" - must still be explored, especially on how they interact with that part of the physics captured by the simple model", to allow "bridges designed on the same basic model to be built longer and stronger over time, as the complexities and how to deal with them become better understood" (Roth, 2002).

(c) The economic consequence of Bogolmonaia and Moulin's non strategy-proofness

Let's first observe that the original Bogolmonaia and Moulin's good assignment game I used in Chapter 8 mainly concerns itself mainly with what axiomatic properties such a game has. Notably that it is ordinally efficient, fair (i.e. if everyone prefers his or her assignment to the assignment of anyone else with respect to the reported preferences) but not strategy proof (i.e. agents might try to manipulate the game - for instance if too many people like the second choice of an agent as their first choice, then this agent may be better off if he starts eating from his second choice instead of his first choice). Furthermore, they proved that there is no mechanism that satisfies ordinal efficiency, strategy-proofness and equal treatment of equals. What do these imply for our adaptation in monetary anchoring? Let's first note how the entire language around" manipulating one's exchange rate" hints at such market design considerations. Indeed, if one combines a non strategy proof mechanism with the long-term incentives of a repeated game based on this mechanism leading to a" winner takes all" reserve currency (and economy), then any agent will have incentives to try to manipulate the game to try to be better off in the resulting distribution. Bogolmonaia and Moulin's scheme's ordinal efficiency is not that important in our case, since there are secondary markets on which countries' debts can be acquired at any points in time - even though potentially at a higher price. What Bogolmonaia and Moulin's model was used to highlight was indeed rather to decide which countries' debts will NOT be fully endorsed by the end of a round. And since this is the only case incurring a" penalty" to countries in our model, let's examine what factor can play there (hence which levers of" manipulation" countries have).

Let's also note here that it is the approach we are following so far that is of interest - the specific model and incentives analysis indeed might change in the future, but hopefully many bright minds from market design and contract theory will contribute in examining the monetary anchoring supergame, so that the world comes ready when a new Bretton Woods will be called, and that the contingencies at that time do not dictate its outcomes. So where are the" tension points" in our game?

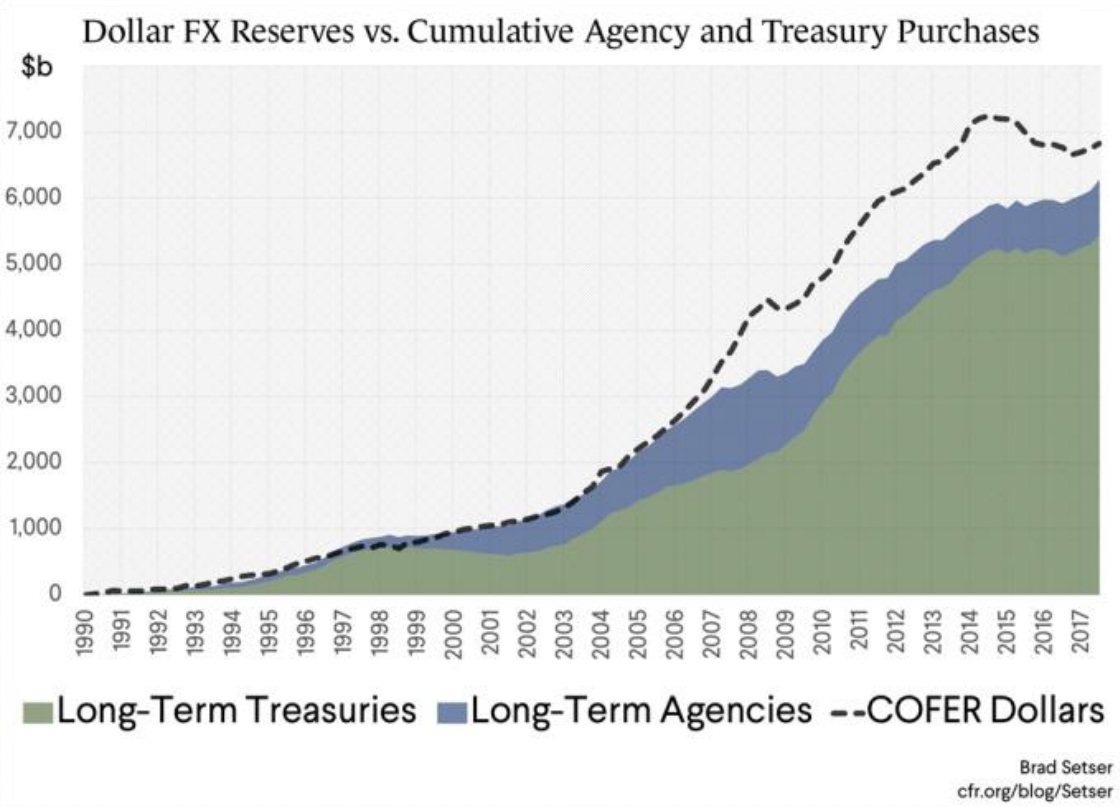
Let's first note where a country can intervene (the size of the cake it issues at the beginning of each round, its interest rates, its eating speed during each round, and its preference ranking), and where it cannot (the same parameters for every other country, plus inflation rates for all countries). Then where privacy intervenes - the cake sizes and eating speeds are known by all at the start of a round, but each country's ranking lists remains in practice private (so in our game the sizes of the cakes issued at the beginning of each round do not factor in the potential rankings). Let's recall there the application of the literature on optimal borrowing lending - and how privacy-preserving technologies can now allow implementations of some schemes designed in the 80s (Townsend 1982, and how technology lowered the costs became interesting enough to use these more complicated form of contracts).Then how do countries potentially improve their lot through interactions with other countries (one could call that manipulating the game - though what I mean here is more on how to interact with other countries so that in the same rules of the same game your outcome improves) ? It has to deal with the private information part of the game, since if known then a country could just adapt its own parameters accordingly (for instance if known all what other countries will eat, with what speed and in what time, one could know until what cake size he'll be able to issue successfully this round). Also looking in more details in how these eating order ranking done by each country s made - we can note that trade partnerships at least intervene in most of the different modeling of how the ranking is done (one could also imagine military alliances, size of countries' economies...). And what is the best way to gain more trading partners? By producing more goods, of better quality, or cheaper. So we can relate here this fact from the" exchange rate manipulation" language noted earlier. Hence, a better monetary anchoring game for us will consist in both giving better information to each country about the aggregate other countries' private rankings, so that it can better decide on the size of the cake/debt it issues at a given round/quarter, all the while ensuring that competitive devaluations are avoided.

So, any optimal monetary anchoring scheme has then to be both an exchange rate stabilization scheme (that still allows to allow for exchange rates to help mitigate unforecasted shocks, and to account for cultural differences among countries - as some exporting countries might agree to finance more importing countries) and a privacy-preserving demand aggregation scheme. And this on a multilateral scheme rather than on networks of bilateral trading partners - as for us only a truly flexible reserve composition and global governance and negotiation platform can lead countries to compete fully on economic terms with less incentive to wage war.

(d) Toward a multipolar monetary scheme : forex volatility as a starting point for cooperation

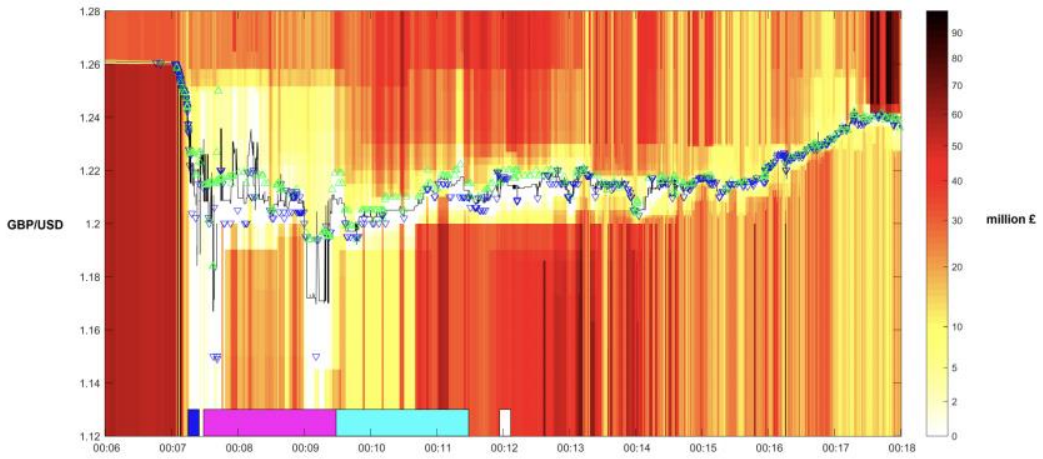
An extensive literature has documented the negative impacts of exchange rate volatility on a country's economy, its trade (Rose, 2000, updated in 2016) and its growth (Aghion, Bacchetta, Ranciere and Rogoff, 2009). These considerations are being reminded to policymakers', as emerging markets' volatility is rising compared to other financial variables. Furthermore, t this trend is likely to deepen as the contest between the US and China intensifies, as digital forms of national currencies and competing payment systems are introduced(Honohan, 2007a), and as "any transition path from a dollar-centric monetary system to a multipolar world is likely to be disorderly with increased speculation and volatility" (Farhi at the IMF's Bretton Woods at 75seminar).Consequently, a good starting point for us to derive our proposed system will be built on the existing policy debate regarding the management of forex reserves, on recent theoretical findings supporting and laying out "optimal" interventions, and from empirical observations on how these are already being systematically conducted (Frankel, 2019). Our specific form of currency intervention is thus aiming at embedding the existing unilateral forms of systematic managed float(ibid) into multilateral agreement, that will let each central bank bring volatility to the level it desires and in accordance with others' targets - while optimizing returns from their reserves. Our methods also further decouple exchange rate

determination from measures targeted at inflation - a separation that might prove useful if, as in Rogoff(2003)'s hypothesis, deglobalization leads to a significant return of inflation. Indeed, the theoretical advancements on exchange rate determination now put the emphasis on market frictions caused by the few risk-bearing financial intermediaries' shifting perceptions and acceptance of currency risks, whose multi-currency balance sheets readjustments thus constitutes "first-order determinants of exchange rates and their volatility"(Gabaix, Maggiori 2014). The level of exchange rate volatility can then be viewed as deter-mined by the policy trade off of how much of these shocks are to be absorbed into central banks reserves, and how much are let into exchange rate fluctuations. Frankel (2019) il-lustrates how some central banks are guided by internal systematic rules concerning such trade-offs, and how reserve management objectives can be an important term in the equation. However, if Gabaix and Maggiori (2014)'s main bearers of the risks resulting from international imbalances are the "highly concentrated, few large financial players ranging from the [former] proprietary desks and investment management arms of global investment banks to macro and currency hedge funds, active investment managers and pension funds", empirical data show evidence that these actors are only bearing the marginal currency risks, while central banks are bearer "to the first order of approximation of all net foreign demand for 'safe' US assets from 1990 to 2014" - (see figure 1 below from cfr, February 16, 2018,echoed by Alessandro Dovis discussing GaMa models at the NBER Monetary Economics Meeting of March 7, 2014).



This observation is then prompting us to reconsider whether the aforementioned policy trade-off (between absorbing shock into reserves or letting it increase the exchange rate volatility) is veritably a trade-off, or in reality an unilateral policy forfeiture - since it seems that excessive volatility is the result of excessive concessions made to private agents that are, after all, only marginally concerned with the underlying risks. With consequences such as flash crashes - resulting first from very short span imbalances in order books (see figure 2 below from the Bank Of England's Staff Working Paper No. 687, October 2017). The 2016 sterling crash is an extreme case, on one of the most liquid currency pairs, but that is reproduced daily on the more exotic and less traded currency pairs.

Figure 1: The limit order book for the GBP/USD pair on the Thomson Reuters platform



- The black line shows midpoint between best bid and ask during the interval.
- Triangles show individual transactions: those in blue pointing down indicate transactions that involve the sale of sterling, and those in green pointing upwards indicate those to buy.
- Coloured regions in the graph show the cumulative quantity of limit orders to sell and buy between a given price and the best bid/ask price. Coloured regions under/above the black line indicate the quantity of limit orders to buy/sell sterling.
- The rectangles at the bottom of the chart show periods when trading was restricted on the CME.

These are therefore the arguments advocating for - and hinting at the potential efficiency of - active, systematic and continuous market-making style intervention by central banks to reduce the volatility of their currencies. Our proposal thus builds on the empirical findings of Frankel (2019), bringing convincing elements supporting the efficiency of currency interventions and displaying evidences "of a systematic effort to dampen volatility of the exchange rate". I will thus examine how to extend and assist systematic managed floating in a multilateral setting to further control exchange rate volatility, composing with each central bank's secret preferences and varying commitment levels. Then, introducing the conceptually useful use of options (which might not be needed in a real implementation) I will derive the accountability and potential profitability of such forms of intervention. Lastly, options will also illustrate how, from a safety-net point of view, such a mechanism designed ex-ante(resulting for instance in automatic forex intervention if a currency fall more than X%) can have a huge prevention effect in avoiding further market panic.

(e) Enforcing stabilization and safety nets on all currency pairs at once, at lower to no reserve costs

At the core of our proposal resides the multi-currency nature of the market making activity of international banks, which I aim at replicating at a central bank level. A first underlying reason would be that of collection of risk - in the line of bigger risks for higher returns. Additionally (and that is a second reason for emphasizing the multi-currency aspect) in our case the additional risk is that of adding on more exotic currencies such as the South East Asian ones in a reserve basket previously not containing them - that could thus act as an additional cushion to mitigate external shock on them.

It is then possible to see that for such a multi-currency reserve balance sheet the profit objective of traditional private market maker is here also aligned with the volatility stabilization objective of the central banks involved, and that the mechanisms underlying these forms of interventions would be conceptually the same as the ones through which financiers' alterations to their balance sheets affect both the level and volatility of exchange rates.

The design question then, critical to the feasibility of such a multi-exotic currencies account, is on how to create and foster this form of collaboration among different central banks.

- **Computing these multilateral balance sheets, through privacy- preserving methods**

The privacy-preserving methods like multiparty computation (referring to the financial adaptation of Abbe, Khandani, Lo, 2012, which build on Yao 1982; Goldreich, Micali, and Wigderson 1987; Ben-Or, Goldwasser, and Wigderson 1988; Chaum, Crepeau, and Damgard 1988; Beaver, Micali, and Rogaway 1990; Cramer et al. 1999). are optional extensions that can help jump-start institutional discussions, and provide a clear and useful framework on which to reach agreement on the different exchange rate objectives pursued by respective central banks. This is why this section will build on the language and framework of these privacy-preserving methods - which again don't have to be actually implemented for the interventions to be conducted.

Let's examine indeed how different central banks from the Chiang Mai Initiative would proceed to build such a common balance sheet, and conduct market making operations. They would first each allocate some funds denominated in their national currencies, plus portions of their reserves in each of the currencies they would like to stabilize their exchange rates with. They would then set-up the daily volatility bands they want their national currencies to stay in, which proportion of reserves they are ready to commit to the operation, and what amount of risk or leverage they are ready to bear on any derivative instrument used in the process (for convenience let's imagine the updates are only feasible at a regular interval - for instance once a day or once a week. We are then in a discreet time setting). These three points are where privacy-preserving methods might be applied, since participant central banks wouldn't want for instance the entirety of the reserves they engaged in that fund to be potentially used to defend the currency of another participating country - thus a daily total amount of reserves committed to each currency could be computed for instance using the aforementioned methods, without individual inputs from each central bank being revealed). Note that the viewing of the results of these computations can also be restrained so that each central bank only sees the pooling of reserves allocated to him - and not that allocated to others. In this fashion, both inputs and outputs of these forms of computations have modular privacy settings, that can be deployed according to participants preferences.

The previous paragraph described mostly a pooling of reserves, quite similar to what already exists in the Chiang Mai Initiative, but applied on a continuous and systematic basis rather than just during times of extreme stress (in fact one of the goals of this automatic and systematic market smoothing is to potentially provide in-commensurable psychological relief and precious time for governments to avoid times of extreme stress). However there are other benefits to having a common multicurrency account: first, the mechanisms derived to stabilize a currency vs the international currencies part of the reserves portfolio can now also be used to also stabilize more exotic currency

pairs (but among natural trading partners) such as the MYR/IDR, to avoid the flash-crash like features presented below (fetch from Google on October 10th, 2019 - the pikes are probably coming from data collection related issues on Google's side, illustrating even further the array of challenges raised by the Correspondant Banking System for FX markets, especially on emerging market currencies).

Second, adjusting flows among multiple currencies that were previously not part of re- serve composition can also turn what is currently a reserve costly operation into potentially profitable currency intervention strategies:

Indeed, having the mandate and now the means to stabilize the volatility on a currency pair thus allow the participating central bankers through this common market making fund to apply short straddle type of strategies, to commit to maintain the volatility within a cer- tain band. There can of course be more sophisticated strategies, but the straddle example is sufficient to illustrate how such types of currency interventions could be less costly in terms of reserves, and could build future credibility for participating central banks and discourage speculative trading firms - and this without hampering the set of tools to fight inflation, thus effectively decorrelating the two issues.

- **On the use of options to build commitment and credibility**

Strong commitment and use of options in the early periods of such an implementation could contribute to anchoring investors' expectations as described in Krugman (1992), potentially automating market reactions without the need of this fund actually buying options and intervening.

The commitment among different central banks will have to be coordinated and enforced, but this is also where the privacy-preserving methods provide a framework to better define (potentially in real time) objective measures, quantified commitment, and all that in a flexible frame that does not extend invitation to speculators to test a public rigid band.

(f) Additions to the current international monetary system

- **A systematic safety net against currency crisis**

The automatic smoothing of exchange rate volatility derived in our protocol provides a safety net against currency crashes, without introducing the moral hazard of a fully specified guarantee (since other participants can withdraw their support to the smoothing at the next time allowing update of their preferences). Indeed," people infer estimates of changes in 'fuzzy' lifetime incomes from perceptions of the sustainability of current spending rather than, as in conventional economic models, the other way round." (Mervyn King. The end of alchemy: Money, banking, and the future of the global economy, WW Norton Company, 2016, p312).

- **Including more currencies in central bank safe asset reserves**

A first observation concerning the "safe asset shortage" and related to how I propose to strengthen the existing monetary system through application of privacy-preserving technologies such as multiparty computation is to link that shortage to the existing literature on information asymmetry. Indeed, if I assume for now for simplicity (the condition will be relaxed in the following paragraph) that all exchange rates are fixed, so that any adjustment of their parities would come unilateral decision from one of the involved parties, then the safest decision for any of the players would be to convert

whatever savings they have into a historical, already implemented, safe asset - the USD - even though its return would be lower than holdings in other currencies. Furthermore, this individual rational optimization taken collectively leads to even lower world interest rates, further diminishing returns on reserves denominated in USD.

One could for instance derive a small adaptation of a Nash Demand Game, in discreet time, two agents, with each player i potentially devaluating following its arbitrary probability $\mathrm{D_i}$ at each time step t - which would give him a one time gain of $\mathrm{d_{i_t}}$, before the other player also devalue at the following time step t+1, bringing back equilibria. Further assume that there is a total final gain of $\mathrm{G_0}$ to be shared between the two players at the end of the game, that decreases to $\mathrm{G_t}$ every time any of the agents devalues. Under full private information with none of the players disclosing its probability to devalue D_i at each time step t, then if the total duration T of the game is long enough so that T*(*what the player i believes the other player j's behaviour* $D_j * d_{j_t}$ will be}) > (the final gain G_0), then the rational behaviour of the agent i not knowing agent j's parameters to entirely discard the final gain of G_0 and devalues whenever it should deem necessary. Now extending this simple model to N players then reveals that none of these N players will adapt the currency of any other players in this game as a reserve safe asset, since it will fear - justifiably - a devaluation that will reduce the value of its savings in this currency. Revealing some information on the probability to devalue D_i , (or at least, on the average, or the uppermost value of all the D_i) will, on the other hand, set a upper bound on the belief from any player i on what the parameters of the other players are. Revealing information about $D_j * d_{j_t}$at any time step t can also enable the "optimal single period borrowing and lending contract" as described in Townsend (1982), to protect the final gain of G_0 from a temporary need for one of the players that another could potentially solve. Implementing these borrowing and lending contracts also further reduces the probability of devaluating from all players, thus increases the chance of their

currencies attaining a central bank reserve status (especially if the borrowing and lending contract enforces some swap between the two legs of a currency pair, as described in our protocol previously). The final remark here will concern the relaxation of the fixed exchange rate regime assumption - indeed, the deterministic probabilities to devalue D_i in the previous simple model then become truly uncontrolled probability probabilities D_{i_t} resulting from, we have seen in Chapter 8, shifts in risk appetite from all the private financial intermediaries bearing the risks of the immediate imbalances in international flows. This additional uncertainty weights further on the left hand term of the inequality on what the player i believes markets will inflict to the player j's exchange rate D_{j_t} ,resulting in non-cooperative behaviours. Thus I further advocate here the implementation of currency intervention agreements - not just from a trade or safety net point of view now, but also to contribute to balancing the asymmetry in the current dollar-centric system, by internationalizing more currencies.

Let's note that our proposed framework would also further extend the existing institutional (or rather non-instutionalized) framework through which current-account surplus countries finance current-account deficit countries. By adapting the previous model we could also argue here that any framework that would lead to more explicit forms of external constraints for deficit countries (if surplus countries want to stop accumulating one specific currency they can just lower the proportion from their own reserve committed to help stabilize that currency) would also increase the long-term gains of all the parties involved - including that of the country currently in a temporary current-account deficit.

- **An additional lever to enforce systematic capital controls**

Under our proposal, the increased share of transactions conducted by central banks to absorb shocks and ease exchange rate fluctuations among themselves would be an implementation of the "optimal capital controls, that should lean against the wind by requiring a temporary tax on inflows

and a subsidy on outflows (if dealing with sudden inflows, the opposite if dealing with a sudden stop)" from Farhi and Werning (2013).

(g) Existing ground for implementation

An interesting observation is to compare the "decline in access to correspondent banking services in emerging markets" (title of a series of World Bank studies and reports from 2015 onward), to the efforts by the People's Bank of China to internalize the RMB through bilateral swap lines with its trading partners, intended mainly at reducing transaction costs of cross-border exchange for local firms, instead of the traditional in crisis liquidity providing swaps. These swap lines, which are likely to increase in number and in size in the future, could provide the ground on which to build such a multilateral market maker.

- **An update of the European Exchange Rate Mechanism**

Readers might remember the history and failures of the European Exchange Rate Mechanism, which ultimately rushed EU members into adopting a common currency. The proposal here is not without parallel, since both goals are aiming at integrating a region to facilitate trade and foster shared growth and stability. However, the new theories, practices and technologies are now allowing adjustments in real-time of exchange rates and their volatility bands (potentially under privacy-preserving methods), i.e. less incentives for speculation and more flexibility to defend against attacks. Furthermore, the common pooling and commitment of reserves - once again adjusted in real-time - offers a discreet form of fiscal control tied to the usage of the pooled reserves, that was and is still lacking on the Euro- pean side. Thus, rather than "crossing the river in one leap", we are here offering additional "stones in the river" to be tested and relied upon, after the failure of the European Exchange Rate Mechanism also buried the discussions on a common currency for the ASEAN.

- **A corrective for the Euro**

Another Chinese idiom emphasizes that while "the sea of bitterness ahead has no bounds, turning back one can still see the shore". In fact, should the eurozone's citizens find the constraints of the necessary political union too binding, the mechanisms laid out here offer a new and smoother transition path out of the single currency. Furthermore, if I consider the parallel discussions on central bank digital euros, along with all the additional markers or interest differential they would be capable of bearing, a symbolic unique Euro could still be preserved among European consumers, while a marker on the digital token specifying whether that token is a French digital Euro, a German digital Euro or a Spanish digital Euro would allow different nationalities' tokens to be exchanged at different exchange rates on global FX markets. That setting would thus correspond to a system with different European currencies and monetary policies, but with each of the European government subsidizing intra-Eurozone cross-border consumer spending to preserve the symbol of an unique currency. Accordingly, a French person traveling to Germany could then just spend his French-Euros on German-Euro labelled hostels, food and entertainment, as if they were the same, with the clearing system automatically billing the Banque de France (or the Bundesbank) and compensating the German sellers (or vice versa) of the exchange rate differentials. The underlying transfers between the respective central banks could here again be implemented following the mechanism described in this paper, to guarantee smooth exchange rate fluctuations and constantly adjusted agreement on the sharing of imbalances and reserves. The specific sectors for which currency parities are maintained through subsidies can be decided and adjusted through time, as the current unique currency acts as if governments are subsidizing all sectors of the economy to maintain parity. A gradual path out of the Euro could thus involve gradually removing these subsidies across more and more sectors.

- **Pareto improvement of the existing monetary system**

Similar to the argumentation in the previous paragraph, I can emphasize here that implementing the proposed protocols on top of the existing monetary system only adds positive

features - the smoothing of exchange rate volatility and coordination of interest rates (see below) - to the current zero cooperation situation. In fact, under the proposed protocol, countries eventually deciding to stop cooperating with others just return to the current non intervention in exchange rate practice. Thus, if the cost in terms of reserves (the only costs in the proposed protocol) are rightfully shared between the two participants of a currency pairs, and potentially compensated through mutual swap agreements, then the protocol de- livers a net improvement in the stability of participating currencies and monetary policies.

One could argue that a country which would wish to exit this protocol after potentially accumulating under it foreign liabilities, could be in the position to seriously disrupt these foreign currencies by massively using the reserves at its disposal (one of the fears to- day concerning China holding massive US debts). To this I would first argue that the transition from the current situation, in which a few countries have been piling up reserves in just three or four ”safe” currencies, to a multilateral version in which all participating countries are exchanging reserves denominated in currencies from all of each other, would considerably reduce the aforementioned risk. Second, the smoothing and safety net engaged (potentially through financial options - which mark strong commitment) around currencies still remaining in the protocol should contribute in mitigating them from the impact of the unloading of their currencies by the exiting country. The same argument - that all other countries could also unload their reserves denominated in the currency of the country leaving the protocol - should also contribute in holding the multilateral protocol together, so that all transitions happen within the consensus bandwidths (which are regularly adjusted for each currency pair) and the shocks (including resulting from these readjustments) can be smooth and controlled.

(h) Results from the post-covid 19 simulations

I use the simulations described in Chapter 8, and implemented in https://mybinder.org/v2/gh/NicolasXYZ/MPC_experiment/master?filepath=second_notebook.ipynb. There, one can run the exact coding to see the current results, and modify the code at will to test out new ideas.

These simulations of extra Covid debts show that :

- in the case of everything constant (pre Trump US and China trade relations) debts are overall sustainable, with adjustments in reserve levels and contraction of countries' economies depending on how affected by the crisis they were.

- similar results in the case of everything constant, with just additional reliance on trade with China (for instance for masks, medical supplies etc). The economic contraction is smaller, and the global reserve contraction as well. This could be interpreted by the fact that the additional trade with China is flushed in its reserve (the increase can be seen in the graph below), used to acquire other countries' debt (inferred from the lowering of global interest rates) and thus sustaining economic activity

- in the case of everything constant among all countries except China and US, who in that scenario stop trading with each other, they are small probabilities of a global contraction (less reserves, less debts, less GDP growth) that preserves the overall shares of each country in the global economy - except for China in the global economy which suffers more. However in these small probability event the US go through an initial bubble fueled by the decrease of China, that then collapses back to the initial level (and note that after this collapse China's share is also back to the initial level - but with the cost of a global contraction, especially for all EM markets). And with the caveat provided just above that this debt model doesn't take into account other incentives and consequences created by such dynamics - small probabilities in economic contraction in one country might leading to escalating tensions on other dimensions as well

- in the case of stopping trade between China and the US AND additional reliance by other countries on China, there is high probability for a sudden takeover of the role of the US as reserve currency China, accompanied by strong contraction for every other country. Again, with the previous caveat of unaccounted destabilizing geopolitical consequences.

- finally, in the case of our proposed stabilization scheme the effects of all above scenarii are smoothen, with much more balanced reserve currencies (at least 3 currencies accounting each more than 20% of the global share of reserves, with the exact currencies - most often Germany ie the Euro, or the JPY - switching depending on the random shocks, but without adverse effects on all countries - including on the US even though the dollar loses its monopoly as reserve currency).

(i) A step further: interest rate agreement

- **Harmonizing interests earned on FX reserve following countries' targets, and steepening yield curves accordingly**

The protocol derived above distributes forex reserves to central banks according to their preferences. These reserves are however usually invested in bonds issued by each one of these countries, whose interest rate policies might therefore impact the others' preference in holding these currencies and bonds. A mechanism for each participating country to harmonize the exchange rate volatility considerations above and interest rate policies has then, and can, be derived using the same privacy preserving methodology. This harmonization process consists indeed for each participating country to specify privately its interest rate targets on its own currency-denominated bonds, and to specify its returns targets on each of the other participating currencies. The "planner" can then solve this optimization problem, without any of the participant accessing

others' preferences, and distribute the amount of each currency to be held by each central bank to the closest of its preference.

Let's note that introducing the above protocol for each maturity of each currency-denominated bond can also provide central banks with an additional tool to influence the yield curve - for instance by setting the interest rate target 30 year bonds higher (respectively, lower) than the average return target of the other central banks to lead them to buy (respectively sell) bonds at these maturities; similarly with 10 year bonds then, and 7 year bonds after, etc.

- Harmonizing world interest rates

Rising interest rates in a low interest rate world is a typical prisoners' dilemma, as described in Mervyn King's the End of Alchemy: "If all countries had set higher interest rates, then it is possible that the resulting slowdown would have changed the narrative guiding expectations and spending both in countries with deficits and those with surpluses. But no single country seemed able to achieve that. Each central bank acting on its own was faced with the invidious choice between raising interest rates sufficiently to dampen the level of domestic demand, knowing that the likely result would be a recession at home, and continuing on a path that would in the end prove unsustainable and lead to an even bigger recession." Thus he wonders - "Were there other policy instruments, unavailable to central banks, which might have resolved those coordination problems, and would they contribute to the healing process today? Or are we headed for another crisis?" (p332-333) The protocol I explicated in this paper can also include a privacy-preserving computation at each update time t for central banks' desired targets at t+1, for them to coordinate among themselves without revealing any private preference or target.

(j) Conclusion

I presented here the benefits and implementability of multi-currency balance sheets among different central banks or institutions, that can reduce volatility independently from inflation targeting measures. I further explored how these forms of cooperation could be derived from existing institutions and technologies, and how they would affect the current international monetary system. It is our hope that this article could provide the basis for discussions that would extend and filter the numerous calls and proposals for reforms of the IMF, linking them to the existing technological and political possibilities of our time.

Future work would consist in first extending the modelling done in Chapter 8, by linking this high level game theoretic model with other macroeconomic models (new Keynesian, and even IS-LM – indeed the incentives introduced by this central bank level village economy made affect different countries' IS and LM curve slopes differently). Junction could also be made with safe asset models such as that of He et al, AER 2020.

Second, parallel between our proposed scheme and an extended version of the hybrid contract described in Part I, Chapter 6, and in Townsend, JME 1988, could be made and formalized. Indeed, central banks are indeed agents with multitemporal tie-ins with each other, with unforecastable shocks occurring differently to each other. Lending reserves to each other would be a way to mitigate these shocks, and this hybrid between pure insurance and pure borrowing-lending fits well the framework of Townsend, JME 1988 (but in a multiagent framework, focused on currency and banking shocks).

Appendix for Part II: the exact procedure followed in the empirical testing of foreign central bank influence on US inflation rate (along with Stata logs) :

I follow the Toda-Yamamoto (1995) procedure to test for Granger-causality. Please note that one could bootstrap to improve the asymptotic validity of the tests - however it is not trivial for dependent data. So I'll work on it separately, while the results here - which still exhibits the breaks quite distinctly - will already give a "taste" of the findings used above.

1. First I test each separate time series involved in the VAR for their order of integration. The stata log of that process can be seen there : https://github.com/NicolasXYZ/MPC_experiment/blob/master/IntegrationOrderTests.pdf (using both ADF and KPSS tests to cross-check)

I can see there that US monthly inflation change is stationary at all points in time, similarly to all other time series involved in this regression, except for month to month change in US GDP (consistently with theory) and for Chinese reserve change - which is stationary, except during the January 2012 - October 2015 period where it might exhibit an unit root. I also test that US GDP and Chinese reserve change (2012-2015) are not I(2).

Then the *maximum* order of integration for the group of time-series, noted *m,* is m=1.

2. I then set up a VAR model in the *levels* of the data, regardless of the orders of integration of the various time-series. The choice of the appropriate maximum lag length for the variables in the VAR is based on the usual information criteria, such as AIC, SIC - but as it can be seen in the stata log there increasing or decreasing it doesn't change the result too much.

Stata log for the 2012-2015, 2018-2020 (contrasted with other time periods) regressions : https://github.com/NicolasXYZ/MPC_experiment/blob/master/VARandGrangerChina.pdf

I do make sure that the VAR is well-specified, ie the residuals are not correlated, normally distributed…(tests can all be seen in the stata log above)

3. For the Granger-causality test I now fix the Wald test statistics so that it will be asymptotically chi-square distributed with p d.o.f., under the null (as some of the data are non-stationary, then the traditional Wald test statistic *does not follow its usual asymptotic chi-square distribution under the null).*

For that I take the preferred VAR model and add in *m additional lag (here m=1)* of each of the variables into each of the equations, and test for Granger non-causality as follows. If the VAR has two equations, one for X and one for Y (for illustration), I test the hypothesis that the coefficients of the first p lagged values of X are zero in the Y equation, using a standard Wald test. Then I do the same thing for the coefficients of the lagged values of Y in the X equation.

To "trick" Stata to not include the coefficients for the 'extra' m lags when I perform the Wald tests (as they are there just to fix up the asymptotics), rather than declare the lag interval for the endogenous variables to be from 1 to 3 (the latter being $p + m$), I'm going to leave the interval at 1 to 2, and declare the extra (3rd) lag of each variable to be an "exogenous" variable. The coefficients of these extra lags will then not be included in the subsequent Wald tests.

I find the Granger causality reported in the write-up above, one-way from Chinese reserve changes to US inflation changes (same stata log).

4. I test for cointegration between the timeseries of the VAR. For the 2012-2015 period both the Johansen's Trace Test, the Max. Eigenvalue Test and the information criterii indicate the presence of

cointegration between 2 of the time series, which are the month to month changes in US inflation and in Chinese reserves. I test cointegration between these two time series separately to confirm. There's no cointegration for the 2018-now period though - so no cross-check on the Granger causality for that period https://github.com/NicolasXYZ/MPC_experiment/blob/master/CointegrationTests.pdf . One could also have usee an ARDL bounds test here in case Chinese reserve change 2012-2015 do exhibit an unit root, for similar results.

I thus have cointegration and (Granger) causality from Chinese monthly reserve change to US inflation monthly changes at the 2012-2015 period (I may still be wrong about there being no causality in the other direction, but at least I have a cross-check on Granger causality in this direction). There's no cointegration cross-check on the 2018-now period however.

For the Japanese 2000-2009 vs 2009-2019 and vs 2000-20019 **regression :**

I follow the same process, replacing the Chinese reserve changes by Japanese holdings of US Treasury, monthly differentiated, collected from treasurydirect.gov and accessible here : https://github.com/NicolasXYZ/MPC_experiment/blob/master/foreignHoldingVSTreasuryForStata.xlsx.

I do the order of integration test for Japanese holdings of US Treasury changes (the test for the others have already been reported above), the VAR, Granger-causality test, postestimation checks and cross-checks in the following stata log. I can see that Japanese holdings of US Treasury changes is I(0). There is cointegration between US inflation and Japanese holdings of US Treasury changes between 07/2000 and 12/2007, and not after. There's also a one-way Granger causality between US inflation and

Japanese holdings of US Treasury changes between 07/2000 and 12/2007, even until 11/2009, but not after.

The stata logs are accessible there : https://github.com/NicolasXYZ/MPC_experiment/blob/master/JapaneseHoldingsChange.pdf

Bibliography

[1] Andrew K. Rose, 1999. ”One Money, One Market: Estimating the Effect of Common Currencies on Trade,” NBER Working Papers 7432, National Bureau of Economic Research, Inc.

[2] Aghion, Philippe Bacchetta, Philippe Ranci`ere, Romain Rogoff, Kenneth, 2009. ”Exchange rate volatility and productivity growth: The role of financial development,” Journal of Monetary Economics, Elsevier, vol. 56(4), pages 494- 513, May.

[3] Honohan, Patrick, 2007. ”Dollarization and exchange rate fluctuations,” Policy Research Working Paper Series 4172, The World Bank.

[4] Matteo Maggiori Emmanuel Farhi, 2015. ”A Model of the International Mon- etary System,” Working Paper 349586, Harvard University OpenScholar.

[5] Ricardo J. Caballero Emmanuel Farhi Pierre-Olivier Gourinchas, 2015. ”Global Imbalances and Currency Wars at the ZLB,” NBER Working Papers 21670, National Bureau of Economic Research, Inc.

[6] Kenneth S. Rogoff, 2003. ”Globalization and global disinflation,” Proceedings - Economic Policy Symposium - Jackson Hole, Federal Reserve Bank of Kansas City, pages 77-112.

[7] Gabaix, Xavier Maggiori, Matteo, 2014. ”International Liquidity and Exchange Rate Dynamics,” CEPR Discussion Papers 9842, C.E.P.R. Discussion Papers.

[8] Alessandro Dovis, discussion of Gabaix and Maggiori, International Liquidity andExchange Rate Dynamics at the NBER Monetary Economics Meeting of March 7, 2014

[9] Emmanuel A. Abbe Amir E. Khandani Andrew W. Lo, 2012. "Privacy- Preserving Methods for Sharing Financial Risk Exposures," American Eco- nomic Review, American Economic Association, vol. 102(3), pages 65-70, May.

[10] Jeffrey Frankel, 2019. "Systematic Managed Floating," Open Economies Re- view, Springer, vol. 30(2), pages 255-295, April.

[11] Chatain, Pierre-Laurent; Van Der Does De Willebois, Emile J. M.; Gonzalez Del Mazo, Ines; Valencia, Ricardo David; Aviles, Ana Maria; Karpinski, Karol; Goyal, Sameer; Corazza, Carlo; Malik, Priyani; Endo, Isaku; Eckert, Sue E.; Abel, Don. 2018. The decline in access to correspondent banking services in emerging markets : trends, impacts, and solutions - lessons learned from eight country case studies (English). FCI Insight. Washington, D.C. : World Bank Group.

[12] Emmanuel Farhi Matteo Maggiori, 2019. "China vs. U.S.: IMS Meets IPS," NBER Working Papers 25469, National Bureau of Economic Research, Inc.

[13] Markus K. Brunnermeier Harold James Jean-Pierre Landau, 2019. "The Dig- italization of Money," NBER Working Papers 26300, National Bureau of Eco- nomic Research, Inc.

[14] Abbe, E. A., Khandani, A. E., & Lo, A. W. (2012). Privacy-preserving methods for sharing financial risk exposures. American Economic Review, 102(3), 65–70. https://doi.org/10.1257/aer.102.3.65

[15] Abidin, A., Aly, A., Cleemput, S., & Mustafa, M. A. (2016). An mpc-based privacy-preserving protocol for a local electricity trading market. In S. Foresti & G. Persiano (Eds.), Cryptology and network security (pp. 615–625). Springer International Publishing.

[16] Albrecht, M., Chase, M., Chen, H., Ding, J., Goldwasser, S., Gorbunov, S., Halevi, S., Hoffstein, J., Laine, K., Lauter, K., Lokam, S., Micciancio, D., Moody, D., Morrison, T., Sahai, A., & Vaikuntanathan, V. (2018). Homomorphic encryption security standard.

[17] Asharov, G., Jain, A., López-Alt, A., Tromer, E., Vaikuntanathan, V., & Wichs, D. (2012). Multiparty computation with low communication, computation and interaction via threshold FHE. In D. Pointcheval & T. Johansson (Eds.), Advances in cryptology - EUROCRYPT 2012 - 31st annual international conference on the theory and applications of cryptographic techniques, Cambridge, UK, April 15-19, 2012. Proceedings (Vol. 7237, pp. 483–501). Springer. https://doi.org/10.1007/978-3-642-29011-4_29

[18] Bogdanov, D., Kamm, L., Kubo, B., Rebane, R., Sokk, V., & Talviste, R. (2016). Students and taxes: A privacy-preserving study using secure computation. Proceedings on Privacy Enhancing Technologies, 2016(3), 117–135. https://doi.org/10.1515/popets-2016-0019

[19] Bogetoft, P., Christensen, D. L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J. D., Nielsen, J. B., Nielsen, K., & Pagter, J. (2009). Secure multiparty computation goes live. 325–343. https://doi.org/10.1007/978-3-642-03549-4_20

[20] Boston University (n.d.). Accessible and scalable secure multi-party computation. https://multiparty.org/

[21] Brakerski, Z. (2012). Fully homomorphic encryption without modulus switching from classical gapsvp. Advances in Cryptology–CRYPTO 2012, 868–886. https://doi.org/10.1007/978-3-642-32009-5_50

[22] Corrigan-Gibbs, H., & Boneh, D. (2017). Prio: Private, robust, and scalable computation of aggregate statistics. 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17), 259–282. https://www.usenix.org/conference/nsdi17/technical-sessions/presentation/corrigan-gibbs

[23] Fan, J., & Vercauteren, F. (n.d.). Somewhat practical fully homomorphic encryption. ia.cr/2012/144

[24] Goldreich, O., Micali, S., & Wigderson, A. (1987). How to play any mental game. In B. Shriver (Ed.), Proceedings of the nineteenth annual acm symposium on theory of computing (pp. 218–229). Association for Computing Machinery. https://doi.org/10.1145/28395.28420

[25] Goldreich, O., Micali, S., & Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. J. ACM, 38(3), 690–728. https://doi.org/10.1145/116825.116852

[26] Ion, M., Kreuter, B., Nergiz, A. E., Patel, S., Raykova, M., Saxena, S., Seth, K., Shanahan, D., & Yung, M. (2019). On deploying secure computing commercially: Private intersection-sum protocols and their business applications. IACR Cryptology EPrint Archive, 2019, 723. https://eprint.iacr.org/2019/723

[27] Kamm, L., Bogdanov, D., Laur, S., & Vilo, J. (2013). A new way to protect privacy in large-scale genome-wide association studies. Bioinformatics, 29(7), 886–893. https://doi.org/10.1093/bioinformatics/btt066

[28] Lapets, A., Volgushev, N., Bestavros, A., Jansen, F., & Varia, M. (2016). Secure mpc for analytics as a web application. 2016 IEEE Cybersecurity Development (SecDev), 73–74. https://doi.org/10.1109/SecDev.2016.027

[29] Microsoft. (2020). Microsoft seal (release 3.5). https://github.com/Microsoft/SEAL

[30] Polyakov, Y., Rohloff, K., & Ryan, G. W. (n.d.). PALISADE lattice cryptography library. https://git.njit.edu/palisade/PALISADE

[31] Powers, M. R. (2007). Using aumann-shapley values to allocate insurance risk: The case of inhomogeneous losses. North American Actuarial Journal, 11(3), 113–127.

[32] Yao, A. C.-C. (1986). How to generate and exchange secrets. Proceedings of the 27th Annual Symposium on Foundations of Computer Science, 162–167. https://doi.org/10.1109/SFCS.1986.25

[33] Robert M. Townsend. (1994). The Medieval Village Economy: A Study of the Pareto Mappings in General Equilibrium Models. Princeton, NJ: Princeton University Press, 1993. Pp. xxi, 145. $35.00. The Journal of Economic History, 54(2), 451-452. doi:10.1017/S0022050700014662

[34] Robert M. Townsend. (1982) Optimal Multiperiod Contracts and the Gain from Enduring Relationships under Private Information. Journal of Political Economy 90(6), December 1982: 1166-1186.ˇ

[35] Robert M. Townsend. (1989) Currency and Credit in a Private Information Economy. Journal of Political Economy 97(6), December 1989: 1323-1345.

[36] Robert M. Townsend. (1988). Information constrained insurance : The revelation principle extended, Journal of Monetary Economics, Elsevier, vol. 21(2-3), pages 411-450.

[37] Stephen Morris & Hyun Song Shin, "undated". "Approximate Common Knowledge and Co-ordination: Recent Lessons from Game Theory," Penn CARESS Working Papers 72042421d029130510780dde2, Penn Economics Department.

[38] Kareken, John, and Neil Wallace. 1981. “On the indeterminacy of equilibrium exchange rates.” Quarterly Journal of Economics 96 (2): 207-222.