ARCHIVES OF ECONOMIC HISTORY

Volume XXXIII No 2 July – December 2021

ΑΡΧΕΙΟΝ ΟΙΚΟΝΟΜΙΚΗΣ ΙΣΤΟΡΙΑΣ

Τόμος XXXIII Τεύχος 2 Ιούλιος – Δεκέμβριος 2021

CONTENTS - ΠΕΡΙΕΧΟΜΕΝΑ

ATHENS - ΑΘΗΝΑΙ, 2021

ARCHIVES OF ECONOMIC HISTORY

84, Galatsiou Avenue, Athens – 111 46, Greece, tel. +30 210 2934916 / +30 6937 244739
e-mail: akiohos@otenet.gr • www.archivesofeconomichistory.com

The Democratization of the Banking Monetary System so as to Grant the Free Basic Income Without Debt Crises. Alternative Solutions Through Decentralized Digital Currencies

K. KYRITSIS* T. PAPPAS**

Abstract

In this article we analyze the ability of the monetary-banking system, to support the free basic income that eliminates poverty without creating periodically debt-crises. We discover 5 toxic anti-democratic functions of the banking monetary system that create periodically debt crises. The free basic income is unfortunately not possible to derive from taxes only as it is a too large expense for Governments, so it has to be derived directly from currency issuing by the central bank. By democratizing top-down the monetary system not only periodically debt-crises are not created but also the free basic income can be granted. Alternatively, the poverty may be eliminated with the free basic income through bottom-up alternative decentralized non-banking digital local or global currencies. We state the necessary principles for such currencies (governmental or not) and we give 2 examples of them which are fully taxed within the old banking currencies.

JEL Classification: G21, G28, H30

Keywords: Banking monetary system, free basic income, poverty, debt crises, alternative digital currencies.

1. Introduction

The United Nations in the recent years has declared a planetary scale campaign to eradicate poverty from the planet. This cannot happen without changing the banking monetary system in the economies. The main function of money here is as right to access basic goods in the planetary life. With the current monetary and banking system the basic income is not possible to be granted through taxes by the politicians, and so the poverty as an epidemic will rise and lead many people to commit suicide, end in mental hospitals, die earlier or live in permanent depression and poor health. In this way the impersonal system becomes the big predator that as lion of colosseum with the early

* Associate Professor, Department of Accounting and Finance, University of Ioannina, Ioannina, Greece, e-mail: ckiritsi@uoi.gr

** Laboratory Lecturer, Department of Accounting and Finance, University of Ioannina, Ioannina, Greece, e-mail: thpappas@uoi.gr

Christians, or as a modern minotaur devours the men in poverty. A clear case of a regressive rather than progressive economy.

The monetary system if cured from its current toxic and antidemocratic functions can solve this major indirect evil on our societies (significant percentages of poverty). It can be cured either top-down through join political power or bottom-up through the initiative of the majority in new concepts of money, crypto-currencies etc.

In the next 2 paragraphs we will discover the basic 5 toxic, poverty creating and anti-democratic functions of our monetary system that characterize our economy and our civilization. Their toxicity is relative to an ethical economy dedicated to serve the evolution of the human immortal soul.

The next 5 toxic and non-democratic functions of the banking monetary system, are the main factor behind all other catastrophic events in the present economy as we live not in capitalism (that was before 1690) but in the capital debtocracy. It is the main factor that makes our economy a regressive rather than progressive economy. This factor is the main factor behind the periodic debt crises, massive bankruptcies, high percentage of poverty, lack of basic income, unhappiness and financial misfortune of the majority of the economic organizations the last 3 centuries

These toxic and non-democratic functions of the banking monetary system lead to the lack of the ability by the governments to grant the basic income to the citizens, which is the most obvious large-scale phenomenon of economic half-slavery. The basic income is a basic economic human right. And as in the ancient Roman civilization the most obvious evil was the existence of slavery, so in the modern civilization the most obvious evil is this economic half slavery. This half-slavery due to lack of basic income as main source of misery unhappiness and poverty, is our blind point in perceiving our civilization. This in its turn creates permanent large percentages of the population being in poverty which characterizes our civilizations almost as an evil civilization. And it is so because it is not a result of meritocracy, (people with virtues will never be poor) but as if in a large scale statistical Russian roulette, it is a systemic crime. Even if all people were identical clones of the same person, all of the same abilities, this phenomenon of high percentage of poverty would still happen

For an evolution of our civilization to a more human civilization which would support as a priority the evolution of the immortal human soul consciousness, it is critical to invent and discover new concepts and functions of money, much better that the current function of money issued by central banks. In the same paragraphs we describe the top-down resolution of these toxic and anti-democratic functions The 3rd paragraph describes new concepts of money

including the digital currencies with technologies like the blockchains or other that may heal in a bottom-up way the toxic and anti-democratic functions

2. Collective majority's good in a democratic economy that serves the evolution of the human immortal soul.

Here we set the standards of 1) democratic principles and the 2) priority of the social good in favor of the partial and minority profit of the selfish individual entrepreneurship. Moreover, we reassure the value of personal and social freedoms and reduced social inequalities compared to intensified inequalities and the recession of the latter. Hundreds of statistical analyses originating either from Universities of from the UN (see [1] Richard Wilkinson: How financial inequalities harm societies), prove that the significant economic inequalities and the lack of the free basic income severely affects society and increases:

a. Criminality,
b. Suicides and mental illness,
c. Severe anxiety and desperation
d. The reduction among the young members of society the ability to learn,
e. The decay of the ability of collaboration in the production sector.
f. Also, the increase of inequalities according to statistical analyses in several countries, is related with reduction of GDP (see [2]) and, in general, a reduction of speed of evolution while, a significant part of the population is not appropriately contributing due to social exclusion.

Additionally, we should note here that while the belief that the major goal of each individual is social status improvement and money or, possibly, social reputation is central, the real long-standing value is the 3) serving of the soul consciousness evolution rather than the access to social power.

Finally, in nowadays society where everything is access only through the right of money, there is no notion of individual freedom when income money is absent and in particular in the absence of the free basic income. Individual freedom would begin from an undeniable human economic right to a minimum free and life-long basic income (or survival subsidy), much like social health insurance. However, nothing similar exists and it is impossible to be granted by the politicians through taxes (vary large sum of annual expense), while the unavoidable resorting to the issuing of currency is blocked by the despotism of the monetary banking system. *In this way, amidst the last 21 century financial crisis like the current one (2009-2021), a long-term unemployed individual*

(especially in poorer countries with one only year only unemployment subsidy), must choose between recruited to criminality or resort to a gradually trapping and bankrupting, bank debt.

Living in a society without free basic income is like walking unarmed in the jungle, while living in a society with free basic income is like walking in a civilized park.

Is the social economic ontology also the social economic deontology? Or in other words, is the way that the monetary banking system functioning (ontology) also the deontology (meritocracy) and monetary optimality? As we shall present in this article it is not at all so.

There is a duality of regressive and progressive function of our institutions and economy.

In our civilization, the conduction of institutions, and exercise laws, rules, sciences, and arts are, supposedly, in the name of social good. However, based on the key principles we mention and especially that of the serving of the evolution of the human soul consciousness, the actual result is, oftentimes, social harm, existential trauma, and the violation of the above-mentioned principles. This may be called the regressive exercise of the institutions as compared toa progressive exercise of the institutions. Given the principle of the benefit of the majority, that we mentioned we may diagnose as regressive act of an institution, science or art if it is done for the benefit of a minority oligarchy and against the benefit and well-being of the majority and the overall social good, even if the usual legal formal procedures are used.

It is important to note how regressive practice of institutions, sciences and arts may occur under a typically legal framework, either due to the law themselves being inappropriate and unfair or because there are not yet notions and laws that protect such sides of social good. E.g., the notion of a financial crime is relatively new and, hence, there are not yet sufficient laws that clearly define all its forms. As a result, a large financial crime may be conducted totally respecting the current laws. Such is e.g., according to this study the blocking in the financial system of the ability to grant the free basic income.

3. The three pathologically toxic and anti-democratic functions of the national central bank.

In this paragraph we describe three pathologically toxic and anti-democratic functions of the central bank. The term “toxic” financial product or service is widespread in financial analysis. The same banks characterize red loans as toxic products. The term” pathologically toxic” is also used quite often. E.g.,

in one of his speeches, Loukas Papademos, the former president of the European Central Bank, in 2011 in the Greek Parliament, used this term describing the situation of the economy in the current crisis.

Most of the national central banks in the Eurozone are public, except that of Italy, Greece and possible very few other countries. But even when public banks they have by laws special independence in d3ecisions about from the Government and the parliament.

The independence of ECB is guaranteed by article 130 of TFEU (Treaty on the Functioning of the European Union, former article 101 of TES, see [9]), which states that

"During the exercise of power and fulfillment of duties and obligations assigned under the Treaties and the habitude of ESCB and ECT, neither the European Central bank nor the national central banks nor any other member of the decision-making modules of these institutions should not be given or accept guidance from other institutions or organizations or from the government of a member-state or any other organization."

Here is therefore the root of anti-democratic despotism, and lack of wisdom in the monetary decisions, as the collective intelligence of the Universities, parliaments, governments etc. of the eurozone is by far a superior intelligence expertise and wisdom compared to a tiny minority of bureaucrats of the central bank. We enlist her the 3 the toxic anti-democratic functions of the central bank.

1. Monetary Despotism or forced pre-emptive control of money issuing

The governments have lost their decision-making ability as far as currency issuing is concerned. Not only the can't take decisions so as to issue currency according to investment demand or other social demand (e.g. basic income) but they are also obliged to borrow it from the central bank either it is private or a public bank! The central bank essentially supplies money based only on the demand for debt, nor for investments or other social issues (thus very often the term debt-currency)

The central organization that issues money, is a bank and not a not-for-profit organization, that is it only lends money and demands it to be returned to its hands which has been issued and, necessarily, lent to the society. This and only central monopoly demand of return all the active money is pathologically toxic and creates a vast central dependence of the entire economy from one and only monopoly bank! However, here we focus in the fact that a very small number of employees and bureaucrats decides upon money, its issuing, the lending rate of interests and their circulation as if they knew about the social

good better than the collective intelligence of the society, its universities, its parliaments and its governments.

Here is a list of financial-monetary decisions which a government has, lost the right to take, either due to a local national private central bank or due to the Maastricht Agreement, after its inclusion in the EU.

a. It cannot decide when and how much money to issue.

b. Either the central bank belongs to the state (public central bank) or not (private central bank), the government must borrow the issued money and, actually, return it to the central bank which is like it does not belong to the state or the people.

c. It cannot – and has not a right of to determine the borrowing rate of interests of the issued and borrowed money.

d. It cannot issue money and channel it to the society without debt, e.g., with by subsidizing or investments.

e. The monetary system with central bank and not a central not-for-profit organization is from the beginning non-solvent and condemned to lead periodically to debt-crises.

This twisted toxicity of the public borrowing the public money is like the Greek proverb *"Come on grandpapa, I will rent to you your own lands to cultivate, but do not worry, I will give you dividend from the rents that you give me"*

Let us see a numerical example. The central bank issues e.g. 10 billions of a currency. The state has a need of 5 billion which is needed for new social investments and is obliged to borrow it from the central bank (even if it is a state and not a private one). Thus, it is charged with 5 billion which it is obliged to return to the central bank through taxes etc. While the alternative, would be to issue money, by a not-for-profit public organization which falls under to Ministry of Finance which would issue these 5 billion that would belong to the state without any borrowing, zero interest rate and return obligation. Obviously, the first scenario is not of the state's benefit! It is even worse when the central bank is private and issues currency for which the rule of gold is not into effect, which could easily be issued by the Ministry of Finance. The issued currency does not belong, not even typically, to the state but to publicly unknown individuals who, thus, have power onto the state and the national economy, as a whole. Obviously, that is against the national benefit and, as a result, since 1974, when the rule of gold was abandoned, such a private central bank (e.g., the bank of Greece, in Greece) violates article 102.6 of the Greek constitution. This article states that

"Private economic initiative shall not be permitted to develop at the

expense of freedom and human dignity or to the detriment of the national economy".

Similar articles exist in the Italian constitution and of other countries, except …the German constitution! It is even more scandalous when a private central bank (like n Greece and in Italy) even as an private but privileged enterprise has also the right to issue laws of the state about the banking sector and the public finance!

The same applies to the case when ECT, the central bank of euro, which is, in a way, affiliated to the Bank of Greece, up to a percentage, when it issued during the Quantitative Ease, 80 billion per month out of zero.

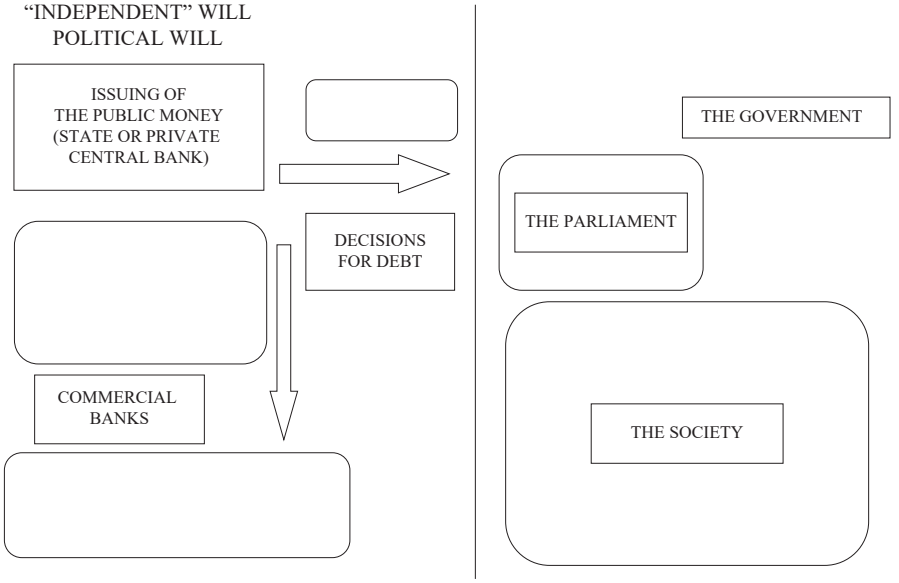
The central bank does issue currency only during Quantitative Ease. It does issue currency almost automatically when ever the current years demand for debt by the commercial banks is higher compared to the previous year. And this is apparent by the diagrams of the volume of Euro, in the publications of the ECB, which was continuously increasing before Quantitative Ease. This is essentially the inflation character of our monetary systems. This applies similarly to the US dollar too.

Someone might wonder if this was always so since the ancient times e.g. in the Roman empire and ancient Greek Athens. It was not so at all! Public currency was issued only by the public or the ministry of economics never private or public banks! It was essentially an unfortunate historical occasion of English state bankruptcy of 1694.

This pathologically toxic function of central banks appeared for the first time in the history of contemporary western civilization in 1694, in England, when, due to the 50-year war with France, the gold of the state had been exhausted and England was, practically in bankrupt. Despite king's Charles and his daughters, Maria Stuart, objections, Cromwell managed to pass, after their death, a law in the parliament to enable individual bankers to issue the English state currency though their own gold, (see [4). To avoid a further social turmoil, this private central bank was named "Bank of England". The same happened within a century to most of the European countries, under several underground pressures.

After World War II, the state of England, fortunately, took under its control the issuing o the currency and turned the "Bank of England" into an independent authority public bank. Unfortunately, however, currency is not being issued by the Ministry of Finance, but, by a bank ("Bank of England") which is "independent". That is, the problem has not been completely corrected. The same applies to the most European countries. However, Greece and Italy still have private central banks.

Diagram 1.1: Forced Preemptive Control of Money Issuing (Monetary Despotism)



Here are some opinions of great presidents of the United States about this issue.

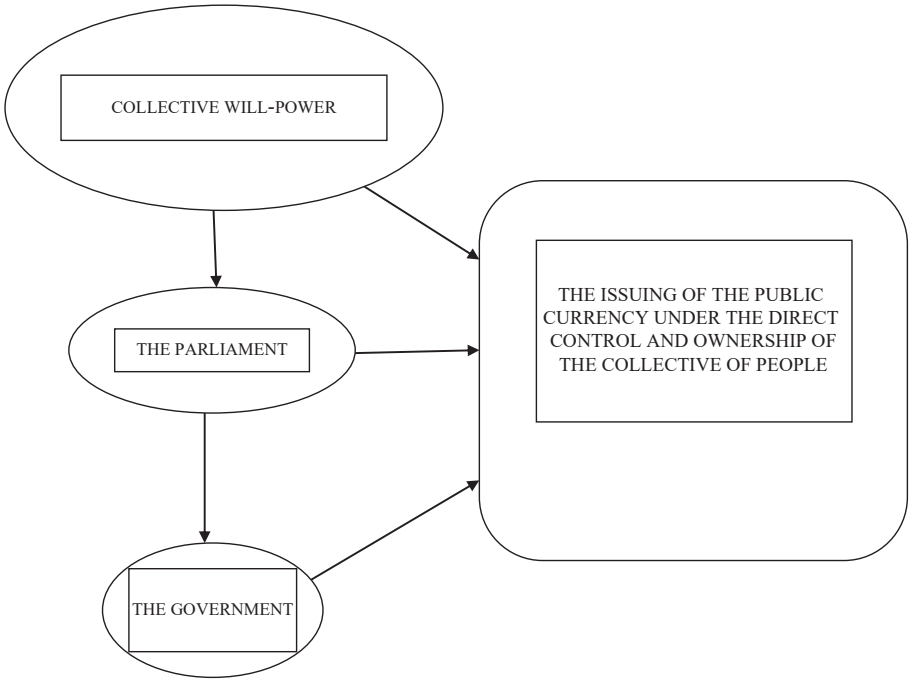
In the United States, Abraham Lincoln, after his win in the civil war and the liberation of black people, wanted to establish a public central bank which would issue state dollars. But he was murdered.

"The government should create, issue and administrate all of the currency and the credits needed to fulfill the purchasing power of both the government and the consumers. With the adoption of these principles, the taxpayers will save large amounts of money and money itself will stop being the governor and ruler of humanity and it will become a servant of it." Abraham Lincoln.

The next presidents, such as Roosevelt and Johnson were against the establishment of a private central bank which would issue the dollars, despite the pressure to do so, due to the obvious reason of it being non-profitable for the state. Notably, a failed murder attempt took place against Johnson, who, as per his words, was proud to have set an obstacle against the establishment of such a private bank.

Diagram 1.2: Top-Down Resolution of the Forced Preemptive Control of Money Issuing, or Monetary Despotism

(In this way the basic income becomes feasible, so the main indirect evil of poverty in the society can be resolved)



"Currency minting should be assigned to the central government and be protected from the rule of Wall Street. We are opposite… to any law that would let our currency and financial system in individuals." Theodore Roosevelt.

However, the next president, Wilson, accepted this and at 1913 the major private central bank of dollar, Federal Reserve, was founded (see [7], and [8]). The federal reserve bank is related to banks of the states, in a similar way that the ECB is related to the national central banks, in the eurozone. The agreement of the establishment of the Federal Reserve Bank is similar to the Maastricht agreement.

As Wilson he stated, a little before his death, he considered this to be his life's greatest sin.

"I am a vastly depressed person, I have, unwittingly, destroyed my homeland. A big industrial nation (the US) is now under control of the financial system which has been centralized. The development of the nation and all our activities are in the hands of some men, these of the bank system. We have become one the worst governed nations, one of the most controlled governments in the civilized world. This is not, anymore, a government with free will, but a government under the will and power of a small group of dominating men of the financial system." Woodrow Wilson

Also, note that even the popular figure of the Italian fascism, Benito Mussolini, agrees. He was someone who of course knew very well what fascism means.

"Fascism should be, more accurately, named private-partnership, since it is the partnership between the state power and the power of the private enterprises." Benito Mussolini.

This is what the wise writer Tolstoy once said:

"Money is a new form of slavery, which differs from the previous one only in the fact that it is impersonal – that is, that there is no human relationship between the ruler and the slave." Leon, Tolstoy.

2. The monopolistic pre-emptive propriatisation of the issuing of the public currency.

The toxic and anti-democratic function refers o private central banks. Normally, when money was issued before 1694, it was a public good and it belonged to the state, that is, equally to all! And this is a socially and macro-economically right. For the central bank to be private is like all the military weapons of a country being property of a private company… independent of the government and the parliament. So, whether there is a war or not is being decided by this company based on its financial benefit!

Today, the central banks of Greece and Italy are private, while these of Germany, France, England and Spain are public.

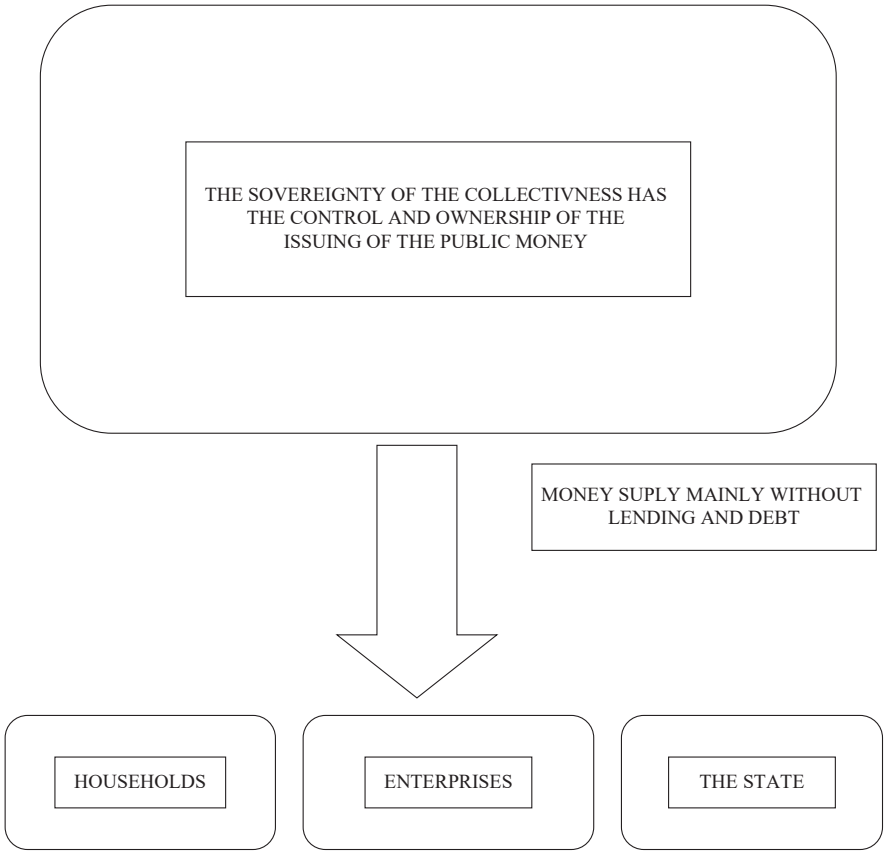
It is also obvious how private central banks violate the European legislation about monopolies (in the US it is called legislation about trusts), since they are private monopolies (of lending the issued money). Even if their functioning was for the nation's benefit, they would violate this name excluding exceptions. With the same logic, every branch could allow for the exceptional existence of a monopoly in it, which is of course unacceptable.

When the central bank issues new currency, it records it to the accounting system in its assets when it is lent to another commercial bank and is also recorded to its liabilities as if it does not own it and is borrowed from non-one

("to the bearer of the bill"). Since the bearer of the bill is, again, the borrowing side, it means either that no one has to payback the debt or that the central banks is in debt to the totality of the people. We must not forget that there is no rule of gold in issuing currency. This is crucial and we will, return to this point in the toxic functioning of commercial banks of money-issuing middleman role in the next paragraph.

Schematically, the solution of this pathologically toxic function of the private central bank is described in the diagram 2.1.

Diagram 2.1: The Top-Down Resolution of the Forced Proprietary Monopoly of the Issuing of the Public Curency



3. Macroeconomic forced debt

It refers to the fact that the central organization which issues money is not a not-for-profit but a profit-seeking bank and, indeed, a non-investment bank, that is, in order to let the money it issues to circulate, it has to and is obligatory to lend it to some organization! It is very important to disciminate that this necessity lies only on a macro-economic and statistical scale and not in a personal individual scale.

Banks, however, cover that, often claiming that debt is only optional and only if one wants and is capable of engaging. It is optional only at the individual level of the borrowing organization, while it is imperative in the overall statistic of the society and the economy for the issued money to circulate, due to the monopoly nature of the banknotes issuing by the central bank and the fact that its only lends as a bank.

This pathologic toxicity is clearly seen e.g., in the case of the first totally private National Bank of Greece which, at 1842, began issuing for the first time drachmas in banknotes, which never existed before, as the country was newly established. E.g., let's say that is issued the first billion of drachmas in banknotes, which, in order to circulate in Greece, should be offered as a loan to the Government and the rest of the individuals, e.g. with an interest rate of 2%, that is, it asks a return of 1.02 billion drachmas. How will these 0.02 billion drachmas = 20 million drachmas will be found since only the National Bank could issue money based on gold? Obviously, the monetary system is non-solvent from its very beginning. Accounting currency will be created, that is, accounting claims records (currency M1, M2, M3) which are more as an amount compared to the amount of the banknotes in circulations in drachmas and, at some time, the system ends up collapsing, the financial enterprises even the public economy bankrupts and the with the red non-served loans appear.

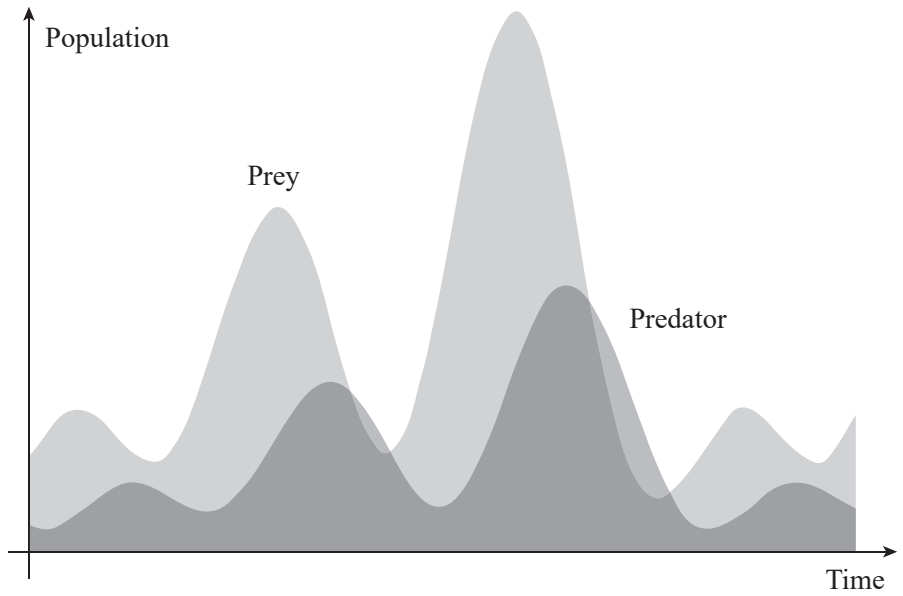
This macroeconomic forced debt leads the European enterprises to have, in average, 60%-66% of their assets in borrowed capital from banks, that is, double from their own equities capital (see Financial administration II, G. P. Artikes [14]). This means that they own their enterprises, only typically, while, from a financial viewpoint, the enterprise to the borrowers and the banks. It also means that they become financially unstable, like paper tower of bank-contracts, which in the first financial earthquake, due to changes in economy, they will collapse and bankrupt in the form of financial debt crises.

German mathematicians, using computer simulations, have proved that, indeed, such a banking monetary system collapses periodically, enforcing enterprises, households and states to go bankrupt (see [15], Gradido currency,

Bernd Hückstädt (Author) while other forms of non-banking monetary systems are stable.

Because of the forced debt the Governments are not able to grant free basic income for the citizens. The taxes only by far are not sufficient. And as we mentioned this is the main evil characteristic and half-slavery of our economic system. The main indirect source of unhappiness, misery, suicides, mental illness, poverty, non-contributing talents in the society, reduction of productivity, psychological cruelty, less number of families less number of children, deceleration of civilization evolution less innovation and existential traumas.

The bank system, through debt acts as a parasitic or ravenous population (predator) with its prey being the rest of the economy. For such interactions between population, the Lotka-Volterra equations do hold (see [16]) which forecast the periodic destruction of the host (the rest of the economy) as well as the parasite (the commercial banks).



Therefore, the appearance of red loans as a significant proportion of the economy is an actual statistical fact for which the bank-monetary system is responsible, even if at the individual scale the debt remains an uncertain event. It is like an epidemic. We may forecast the percentage of people affected per year, but not if an individual will be affected or not.

Diagram 2.2: Macroeconomic Forced Debt

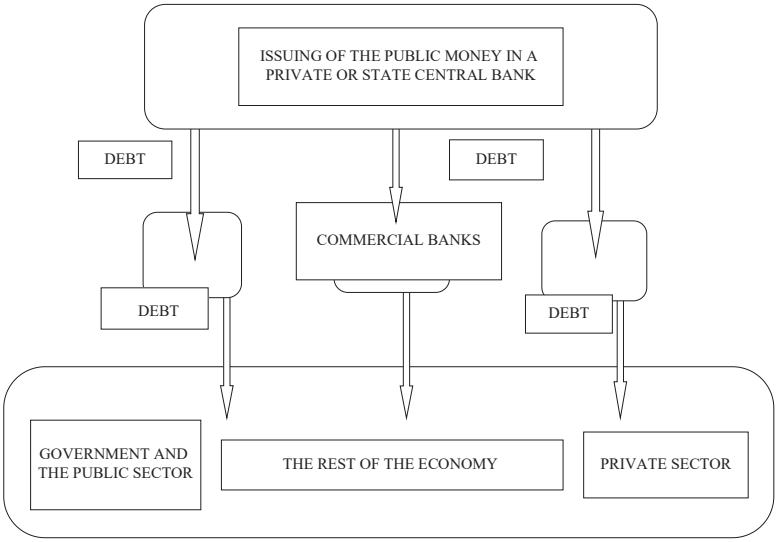
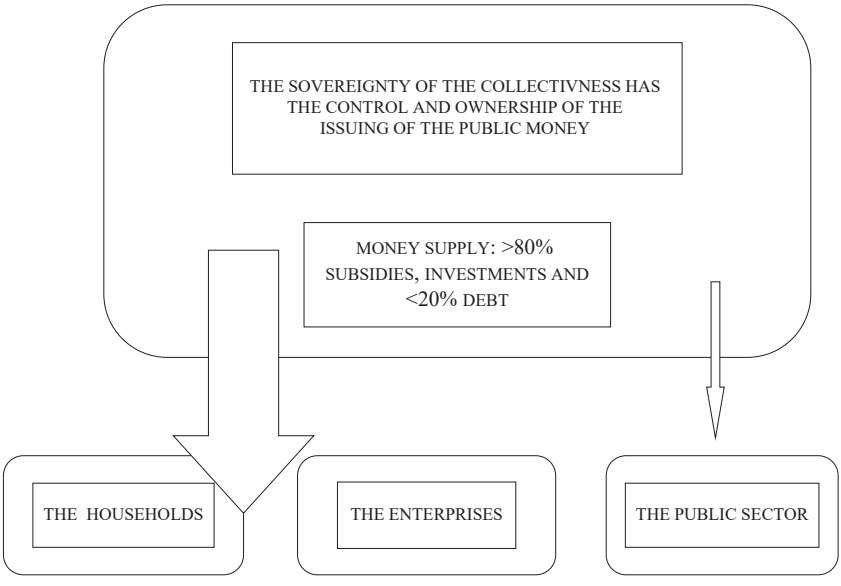


Diagram 2.3: The Top-Down Resolution of the Macroeconomic Forced Debt (in this Way no Debt Crises are Created Periodically)



Thus, judges for red-loans in such debt crises should not hasten and blame the borrowing side in cases of red loans, with the thinking such as "it was the borrowers's fault and bad management of risk". On the contrary, they should lay the blame on the banks. As industries polluting the environment with toxic waste are required to pay penalties, the same should apply to banks, which pollute the economy as a whole with excessive forced debt.

Unfortunately, these pathologically toxic functions of the bank monetary system are not, anymore unavoidable evil, after the abolition of the rule of gold, but, they are simply bad collective financial habit of the society.

The next table 1 analyzed the mainstream believes about the central banks and the underlying reality.

Table 1: Central Bank

Major believes about the central bank	**The reality of the central bank's functioning**
1. The way central banks function is the perfect, for the benefit of the majority, and it has been decided by the government	The way central bank functions is pathologically toxic and anti-democratic for the majority but vastly beneficial for an oligarchic minority and has been determined by tragic historical circumstances against the power of the governments, while staying mostly unchanged in the centuries after.
2. The central bank stabilizes the economy	The central bank sustains only the pathologically toxic and anti-democratic function of the bank-monetary system, which periodically creates debt crises.
3. The most important task of the central bank is to determine interest rates	The most important task of the central bank is to issue banknotes.
4. The central bank, either private or public, should be an independent authority relative to the Government(s) and decide autonomously, since government(s) and the parliament are not capable of making good monetary decisions.	Decisions regarding the monetary system and banknotes issuing should be taken by the government(s) and the parliament(s) after consulting experts. The collective intelligence is superior to that of some employees and bureaucrats.

Major believes about the central bank	**The reality of the central bank's functioning**
5. The central bank should be a strictly lending bank and not an investment bank, since, if there is no organization that controls through debt the society, there would be chaos.	If the central bank also offered the issued money through investments and not only via debt, it would better. It is the right rules that ensure a smooth functioning of the economy and not that the issued money is supplied only through debt.
6. Banknotes are being issued by the central bank only during Quantitative Ease.	Banknotes issuing takes place at any moment and automatically, whenever debt demand exceeds the previously issued currency supply. This is regulated by the fractional reserves rule or available liquidity of commercial banks, to which the central bank has committed itself, voluntarily.
7. The currency is issued by the central bank under certain rules, as a proportion of the GDP or the total wealth.	The currency is issued by the central bank according to the demand for debt by the commercial banks or during Quantitative Ease.
8. The central financial organization that issues money should be a bank.	The main financial organization that issues money should be a non-profit organization and not a bank. It became a private bank "temporarily" for the first time in England during 1694, since England had gone bankrupt due to 50 years of war.
9. Issuing currency that is not backed up by gold is a pathologically toxic function.	The value of gold is conventional, as well. Currency should be issued on the base of the size of the population and human productive ability (GDP). This is healthy and fair (Πάντων χρήματων μέτρον άνθρωπος=For all Money the measure is the human factor)

2. The three pathologically toxic and anti-democratic functions of the commercial banks

Passing now to commercial banks, the forced-debts, always at a macro-economic level and not an individual one, is a common pathologically toxic functioning of them, as well as of the central banks, which leads, with statistical certainly, to a periodic collapse of the financial system and the appearance, again with statistical certainly, of debt-crises and red-tape borrowers. The Commercial banks are also exhibit, however, two new pathologically toxic functions.

1. Empty-lending. (the same banknote is being lent simultaneously to up to 100 borrowers while it actually remains at the bank)

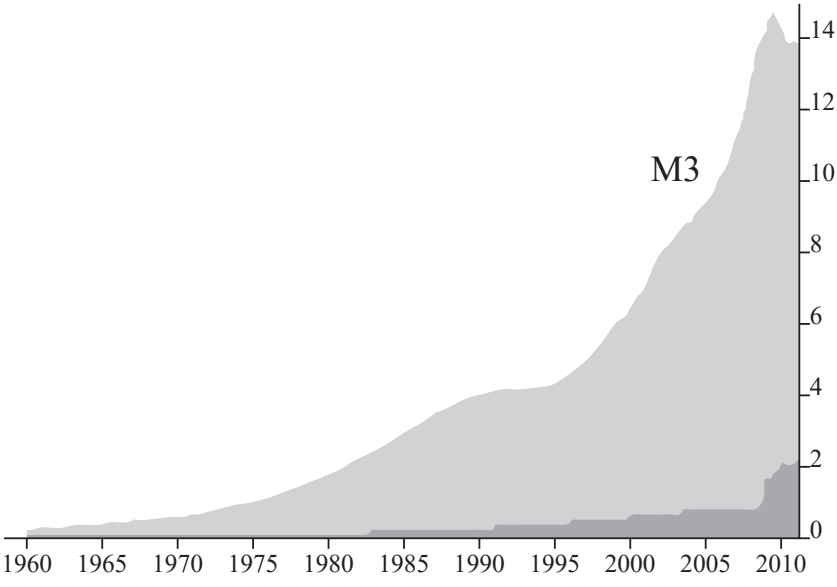
As we have written above, when, some centuries age, the fraud of goldsmiths and loan sharks, who were lending at the same time the same ounce of gold that had been trusted to them by depositors, was discovered, after hanging some of them, finally, governments were convinced, due to the lack of enough gold, to legalize issuing multiple receipts of gold deposition lending for the same ounce of gold, which were used, at that time, in the role of banknotes. Thus, today's rule of fractional inventories used by commercial banks, had been born, which, at our time, is called rule of liquidity (see [11], "Eurozone, Money and Financial System", Gikas

G. Hys A. (2017) rule of liquidity for ECT.). According to this rule, the same banknote which statistically remains at the treasury of a trade bank can be lent to up to a hundred borowers (rule of liquidity of 1% of the total depositions in Eurozone). That is, commercial banks at a 99% rate lent "void" and not actual banknotes. Thus, commercial banks create "accounting money" M1, M2, M3 (se e.g. [11], [12], [13], [14]) which are simply claims of money in accounting records and they depict the money flow in the society rather than the banknotes flow themselves. This should be seriously taken into account by judges in cases regarding banks and red-tape borrowers that they cannot serve their debt, in times of debt-crises. E.g. if in the treasury and liquidity accounts of a bank contain only 100 euros, the bank has the right to lent up to 10,000 euros which, in fact, it does not possess in banknotes. Thus, is has the right to ask for a loan from the Central Bank while this 1% rule is being reserved. The central bank usually considers this lending its obligation. And, if there are no banknotes stocks in the Central Bank available, and it is an excess money demand, in order for the central bank to meet this demand with money supply, it can issue currency and banknotes under an automatic procedure, without this being considered a Quantitative Ease. Currency and banknote issuing is called

Quantitative Ease when it is done after a decision of the Central Bank, without any excess debt demand by the commercial banks. It is know that during 2016-2018 the ECB issued 80 billion euro per month, out of nothing, simply typing these amounts into its computers, which have no value in gold.

Money issuing, without it corresponding to gold, is not considered pathologically toxic in the current bank-monetary system. For the same reason, however, digital currency issuing such as with Bitcoin and other crypto-currencies via mining by computer algorithms, should not be considered a pathologically toxic either.

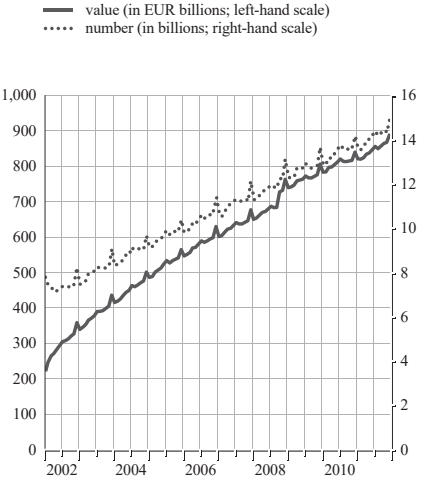
The well-known industry car manufacturer Henry Ford used to say, already during the previous debt-crisis of 1920-1930, that, "if the average American citizen knew the way the bank system works, there would be a revolution the day after it". But, even almost a century after and in the middle of the second large debt- crisis, average people, as if they have been hypnotized, do not understand the actual way that the bank- monetary system functions. Indeed, in a gallop in Switzerland regarding a possible Referendum regarding whether the state would continue allowing banks' "void-loaning" and the creation of logistic currency M1, M2, M3 or not, only 8% of the population understood which subject that the referendum referred to.



The diagram above depicts the way the accounting currency M3 is decreasing in the US (the line above) while the number of issued banknotes is increasing, since they were issued by the central bank of dollar.

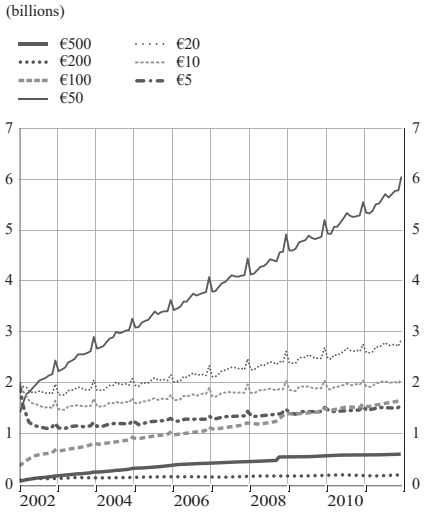
This leads, of course, banks to have a large leverage ratio, which is the bank's assets divided by the bank's own funds (which is above 10). After the abandoning of the rule of gold, there is no actual reason for this to happen, apart from banks' profits. The leverage ratio in the rest of the private sector is just about 3, that is assets/own funds=3. High leverage ratio means larger profits as a percentage of own funds but also larger instability risk in possible bankruptcies or crises. A leverage ratio of 3 is, already, rather high for enterprises, and it is a result of the forced-debt that has been described above, and is also the reason why they go bankrupt in a crisis like the current one. Not to mention of the >10 leverage ratio of banks, which led some commercial banks in Iceland, Cyprus and Greece immediately to collapse. The reduction of leverage ratio for the banks, in the form of a higher percentage of capital adequacy, is suggested in the guidelines of "Basel I, II, III" (see [17],) which are rules for the better functioning of banks. However, the suggested reduction is rather very low, lower than 2-3 percentage points.

Number and value of euro banknotes in circulation



Source: ECB.

Number of euro banknotes in circulation by denomination



Source: ECB.

The above constitute the pathological toxicity of "void-loaning" which is described in the next diagram while it cure is describe in the right next one.

Diagram 3.1: Empty Lending

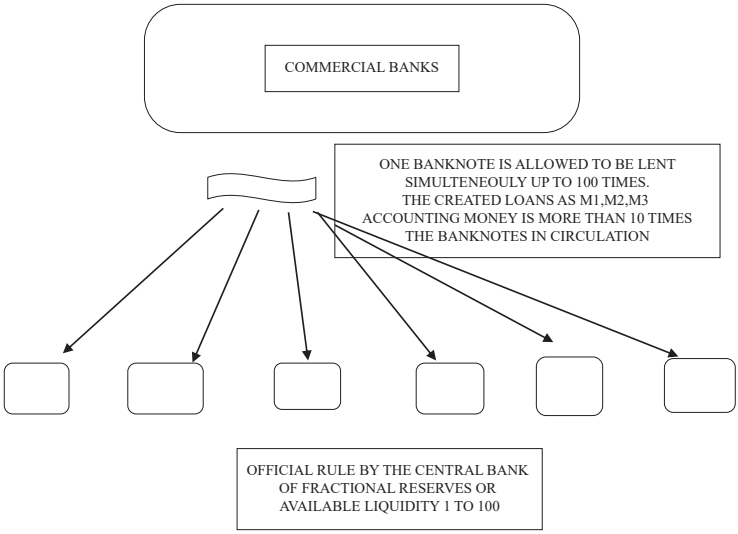
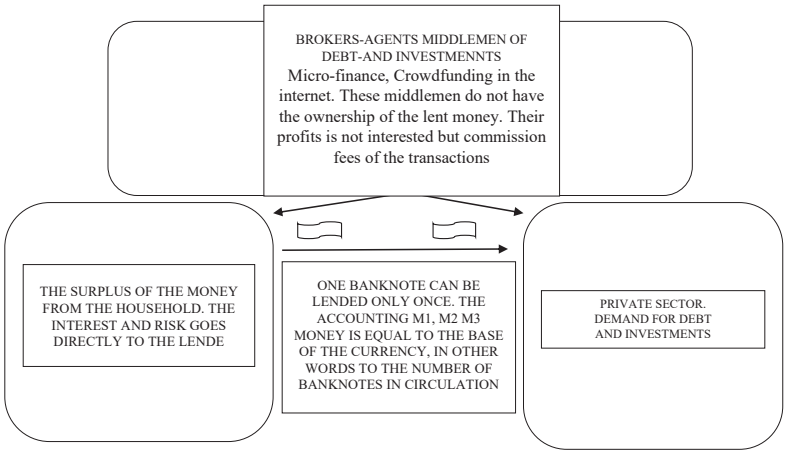


Diagram 3.2: The Top-Down Resolution of the Empty Lending



2. Currency-issuing middleman role of the commercial banks

If we ask an average citizen or a traditional economist about the reason of the existence of the commercial banks, they will both answer that they exist so as to offer to the economy the service of collecting of surplus money from households or other financial units and channel it through debt to the private sector enterprises in order to facilitate the needed production within the society.

Is this, however, what commercial banks actually do? Or the will to profit through debt, almost at every cost, reverses and changes this role?

A brief look at the balance sheets and other financial reports of the main) system) banks in Greece reveals that, often and for some banks, even systemic ones, their main role is different and it could be called "Currency-issuing middleman role". We see this e.g. in the balance sheet of Eurobank (see [27]).

During 2011, loans towards/and demands towards clients divided by the other credit institutions (the cheapest currency) divided by the loans by/and secured dues to the central bank and give ratio 74.69%.

Take into consideration, however, that, in general, in balance sheets, the actual influx of surplus capitals from households through deposits is much less than deposits because loans that the bank provides are also recorded as deposits.

During 2012, for this bank this ratio was 73.7%. During 2014, it was 54.42%. During 2016 it was 78.3%.

It is obvious now that this bank does not have the role people think it has, but it is simply a middleman in the currency currently issued by the central bank of euro (ECB)

As far as Alpha Bank is concerned, we see in its site ([29] l) and its published balance sheets that: During 2012, this ratio was 78%.

As far as Piraeus Bank is concerned, we see in its site ([30]) and its published balance sheets that: During 2007, this ratio was 61%. During 2015 was 68%. During 2016, it was 56%.

The above constitute the pathologic toxicity of "Currency-issuing middleman role of the commercial banks " which essentially states that in most banks in most of the years the majority of the money that the lent does not come from deposits but from borrowing from the central abnks as the Katter is cheaper money. In the next diagram we visualize it while its cure is described in the right next one.

It is significant for us to notice that these 5 toxicities of the banking system are not a necessary evil but more of a bad financial habit of the economy (much like e.g. smoking and smoke industries, metaphorically speaking).

Diagram 3.3: Middle Man Role of the Commercial Banks in the Money Issuing by the Central Bank

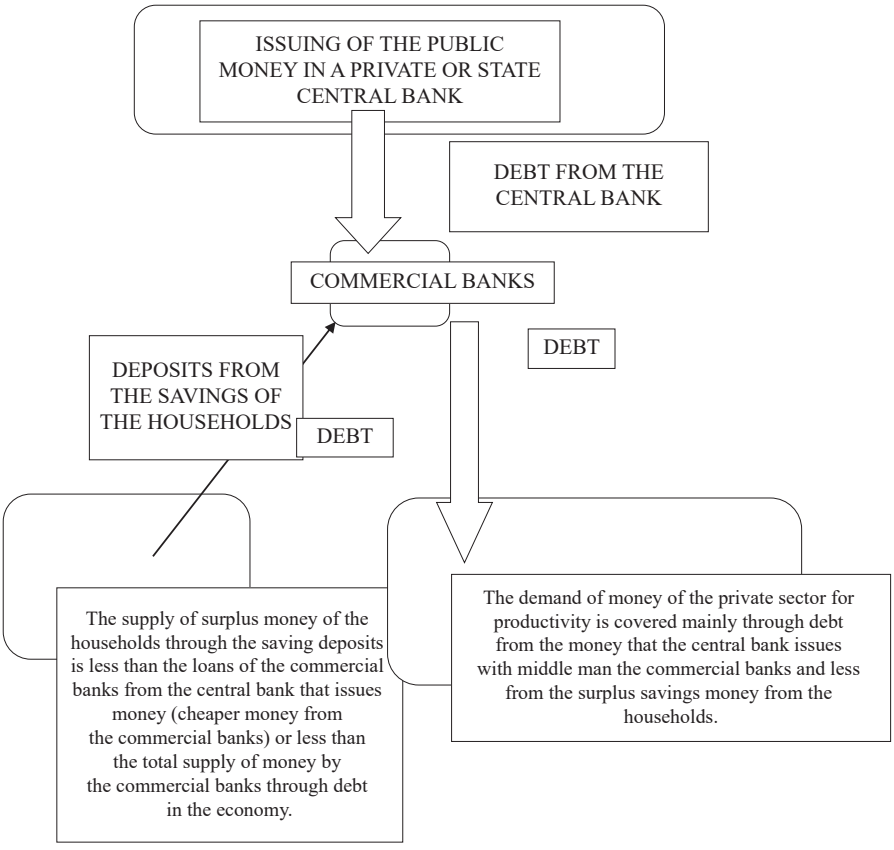
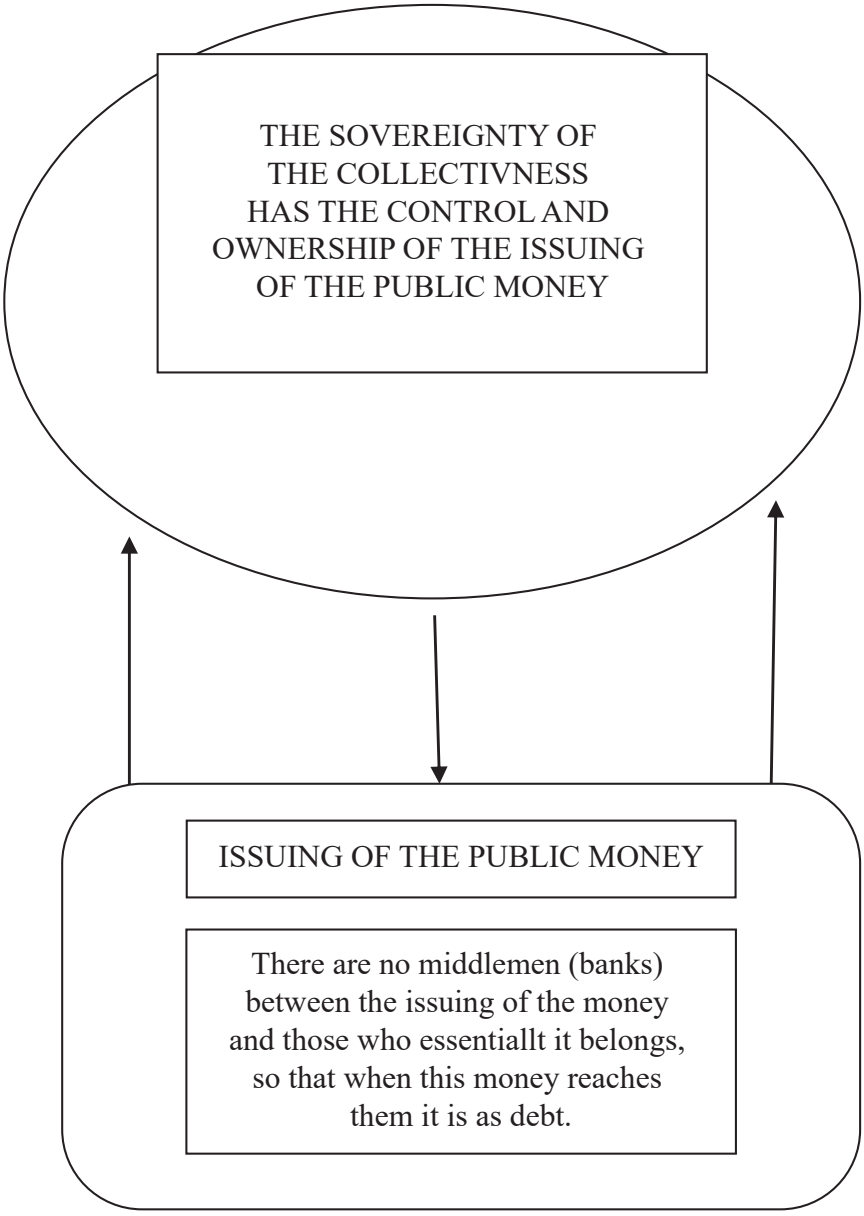


Diagram 3.4: The Top-Down Resolution of the Middle Man Role of the Commercial Banks in the Money Issuing by the Central Bank



Especially in Greece there is an extreme scandalous situation with the commercial banks which was mention in 2015 by the prime Minister Tsipras in a speech in the European parliament. He mentioned that more than 60% of the debt of Greece through the memorandums, and in particular 203 billion were given to the 4 big (systemic) private banks to stabilize them instead of being used for the public economy. The memorandums required that these 4 banks have now new owners that are outside Greece. This grant of 203 is more than double the red-tape non-serviced debt to the banks so it was an out of proportions act. Furthermore, the banks did not erase the red non-serviced loans to people and still liquidate even their only house they live. The 203 billion were given as follows

1. By law 3723 φεκ 250 2/12/2008 during the government of K Karamanlis 23 billion
2. Then during the government of G. Papandreou with laws N. 3845 ΦΕΚ 65 6/05/2010 15 billion
3. N. 3864 ΦΕΚ 119 21/06/2010 10 billion
4. N. 3872 ΦΕΚ 148 3/09/2010 25 billion
5. N. 3965 ΦΕΚ 113 18/05/2011 30 billion
6. Π. Νομ. Περ. ΦΕΚ 203 14/09/2011 30 billion
7. N. 4031 ΦΕΚ 256 09/12/2011 30 billion
8. 19/04/2012 40 billion ΦΕΚ ΑΡ. φ. 94

In total 203 billion

The next table 2 analyzed the mainstream believes about the commercial banks and the underlying reality

Table 2: Commercial banks

Major believes about commercial banks	**The reality of commercial banks**
1. The way the commercial banks function is perfect and beneficial to the majority.	The way commercial banks function is pathologically toxic and non-democratic for the benefit of the majority. It aims at the owners profit and because of this, they should not have that much power within the economy and the society.

Major believes about commercial banks	**The reality of commercial banks**
2. Commercial banks always lend money to the enterprises as if the own it, which the mainly they derive from households though deposits.	As can been seem in their balance sheets, of the commercial banks, at least in Greece, they lend money to enterprises, as if they own it, and most of the banks and most of the years, they lend money borrowed from the central bank or other sources because it has lower cost when compared to the one originating from the deposits of the surplus money of the households.
3. The commercial banks are comparatively the most stable financial institutions.	The commercial banks have the highest leverage ratio (>10) amongst enterprises (which have a leverage ratio of about 3), so, they have the largest profit but also the largest instability.
4. The commercial banks, in the way they function, are the motor power of the economy and their existence is needed.	The commercial banks after the elimination of the rule of gold, because of the debt that they force in the economy, drive the average enterprise to have an average debt capital equal to 60%-66% of their assets and, thus, they constitute an important impediment and danger for the economy and its development. Banks are not a necessary evil; they are a historically harmful habit of the past and misfortune for the economy.
5. Due to this specific instability, bank should be granted with more and more privileges and power in the economy.	Due to their actually parasitic profit through forced debt and their instability, the banks should be deprived of some privileges and new rules should be imposed while, gradually, they should be set aside as institutions.
6. It is more important that the banks are saved rather than public economy, enterprises and households, thus in the bailout of Greece 210 billion, that is more than 60% of the memorandums' funds lent in Greece, were given to them.	The example of Iceland shows that it is more important to save households, enterprises and public economy with new forms of economy, against saving the banks and the old forms of debt economy.

Major believes about commercial banks	**The reality of commercial banks**
7. Deposits in the commercial banks' balance sheets account for the influx of money from households and clients towards the banks.	Deposits in commercial banks' balance sheets do not account for the influx of money from households and clients since as such are often recorded banks' loans towards their clients which are an outflow towards the clients.

3. The Bottom-up cure of the 5 toxic and anti-democratic functions of (central also) banks that can also provide the free basic income and eradicate poverty with new uprising institutions of digital currencies and new local or global currencies.

Digital currency

On October of 2017 the IMF director confessed that the future of the global globalization of currency is crypto-currencies with blockchains such as, e.g. Bitcoin etc. Monetary systems with digital crypto-currencies such as Bitcoin do not suffer from the 5 pathologically toxic functions of bank currencies.

That is:

1. They are not issued under monopoly by a central bank, so they do not suffer from forced antidemocratic despotism.

2. From the moment they are issued (e.g. mining for Bitcoin) their supply does not have to necessarily pass through the "gate" of loaning to meet the demand, that is, they do not suffer from "forced-debt".

3. Since, theoretically, anybody can issue crypto-currency though mining, they do not suffer from the abusive proprietary monopoly of their issuing.

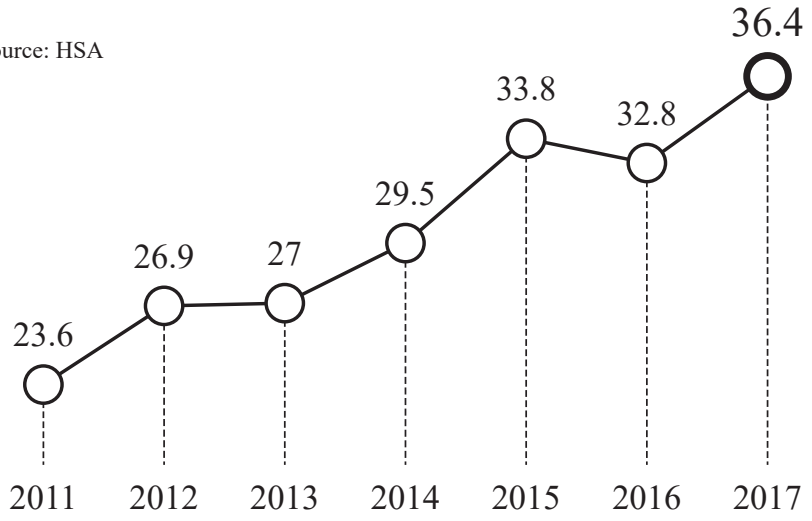
4. Since they are not offered to the society strictly through banks, they do not suffer from empty- lending.

5. Since no bank interferes in a monopolistic way from their issuing until the cover of their demand from the society, the do not suffer from forced money-issuing middle man role.

6. Other benefits of them are that they are faster in currency transfers and remittances on the internet and in transactions, since no bank is needed to mediate with a 1-2 days valeur. But this advantage is the less important and if the central abnks issue digital euro and digital dollar, it will not exist as advantage.

Diagram 3.5: Percentage of population that makes buyments online (2011-2017, 1st term)

Source: HSA



Of course, digital crypto-currencies are not the only forms of digital currency that does not suffer from the 5 pathologically toxic functions we have described. Probably, the biggest benefit of humanity from the spreading of digital crypto-currencies is that they have made the average citizen aware of the abovementioned 5 toxic functions of bank currencies, from which they do not suffer. In the diagram below we see the increase of the transactions in digital currencies even if transactions are currently made, mainly, with bank currencies rather than crypto-currencies.

[20] Use of e-commerce. [21]

The next is a table that discover hidden believes about money as compared with the reality.

Table 3: Money and Society

Major believes	The reality
1. Society cannot function without the current concept and function of money	It is known by the theories of social systems in sociology, that money is necessary only when there is the private property whose value must measure, and that social systems without private property do not need money to function. Nevertheless money is not a single concept and function and there a lot of different types of money relative to its effect in the society and the inequalities. As in the civilization, due to lower frequency and level of evolution or development, there is an excess of negative will within the symbolic duality of prey-predator, then the way to mix it and convert it to will for good, is through private property and enterprise and the completion of productivity and power through capital accumulation, as in the private sector. Large enterprises with size above the median contribute usually to the increase of economic inequalities. Their products reflect the rather negative will of power accumulation through money, in their designed programmed obsolescence for reasons of money. Small size of enterprises on the other hand contribute to the decrease of the economic inequalities and the main concern of their owners, besides offering with their products or services, is to survive or keep a decent level of well-being. It is a challenge to re-design the function of money so that it reduces inequalities and grants also the basic income to the citizens.
2. Economic inequalities reflect the meritocracy among people.	This is partially only true. The economic inequalities reflect the meritocracy of special type of skill, that of becoming rich. In the great picture of society, money is the main tool for creating in a statistical way inequalities. And the inequalities are also source of injustice and unfairness in the fate of human beings that may be more advanced souls that those with the privilege of being rich.

	The initiators of many religions is an example. Or many heroic figures in sciences and arts, that have advanced the civilization but they did not acquire neither sufficient money neither sufficient fame when they were living. These are not merely the exceptions in statistical rule, as money has a statistical property similar to the inherited royal aristocracy in this sense that in order to get the privilege of becoming rich one must adopt and repeat the same type of strategies under similar principles and values as the already rich did to become rich (Skill to become rich).
3. The economy cannot function without the current banking-monetary system of money supply after issuing it, exclusively through lending.	The emergence of the digital (crypto) currencies seem to suggest that in a few decades they will make the banking system (which is responsible for the repeating debt crises) almost obsolete, as Monarchies and Aristocracy became in politics. If national currencies will remain, they should be issued from public not-for profit organizations that should circulate the issued money mainly not through debt.
4. Money is neutral in creating inequalities in societies.	Money is not only a neutral tool as means of exchange. Its statistical function is also a tool to create the economic inequalities, and has become a tool to exercise non-democratic power from small minority groups to the majority
5. Money is a positive tool in the social functioning	Money is good only as lesser semi-random evil, compared to direct brutal military or monarchic based, totalitarianism, in creating inequalities based on direct force by weapons or based on racist principles.

In the next we present principles and rules for general local or global digital currencies with or without the block chain technology that can solve the great indirect evil in our civilization which is large percentages of poverty. This poverty is not due to lack of good and resources but mainly a systemic crime based on the distribution and circulation of the money without a free basic income. A planet like earth can comfortably support up to 10 billion people if the right to access the goods (money) is appropriately distributed (free basic income). We are at the moment a bit more than 7,5 billion people. This poverty can be eliminated through the free basic income, which unfortunately cannot come

entirely from the taxes as it us a too large expense, but only directly through the money issuing,

We describe general new principles t design new types of healthy money and present rules how such local currencies that provide a free basic income can function within the old forms of banking currency.

The next rules and principles for local digital currencies are variations and synthesis of similar rules of the local currency of Woergle in Austria in the decade of 1930, and of the modern Sardex local currency in Italy. (see [8])

The rules lead also to a parallel local currency to that of the dominant (US dollar or Euro etc) which is not inflation based, it includes the basic income and all the taxes are paid in full to the dominant currency (US dollar or Euro etc)

Let us put some terminology to ease the discussion Let us consider 2 properties of money

1. Unit of measurement of value of other goods (This aspect of money does not require the existence of private property in the social system)

2. Store of value (This aspect of money is usually linked with the existence of private property in the social system)

If both hold for a currency let us call it 1st generation money, while if only the 1st property holds and not the second let us call it 2nd generation money. 1st generation money can be bought and sold and borrowed with interest, but 2nd generation money cannot (it has no interest rate too).

Also for the 1st generation money if in order to issue it one requires collateral (to be backed up with e.g. gold or a basket of goods and services) let us call it collateral based money, while if it is possible to issue it without corresponding to an already existing good zero-generated money or currency. For example the current banking money is zero-generated money. Obviously the bitcoin is not 2nd generation money and zero-generated, while complementary credit currencies like Sardex is 2nd generation money but also collateral money. Also the internet currency gradido (by Bernd Huckstadt, http://gradido.net/en/Book/c/1/book) is 1st generation money too but also zero-generated.

Now what are the desired experience for money that we would like so as to improve social life and the existential experience of it? In my psychology and perception the next would be the desired properties

1. We want money that frees from financial slavery (e.g. minimum free basic income).

2. We want money that everybody can issue and is not the privilege to few only

3. We want money that provides capital (equity not debt) to anyone who want to make a growing business

4. We want money that is not tied directly to private property, as few only have sufficient large private property

5. We want money that its rules allow the decrease of private property inequalities.

6. We want money that is closer to the functions of the free flowing information of the web, rather than money tied to static private property.

Therefore under these desired properties, we should favour

1. 2nd generation money versus 1st generation money

2. And from 1st generation money, the zero-generated versus the collateral based money.

We do live in a world of 1st generation and zero-generated money, which is more intangible, than the collateral money which is more hard materialistic. I believe we should no go back to collateral money. People trading in stock exchanges (when they do not lose massively money) experience the idea of making money from nothing. Although this may seem and may be parasitic, we can convert this feeling to something fruitful for the productive economics. We should take the zero-generated money and transform it or the sake of liberating financial the majority and reducing economic inequalities. It seems to me more spiritual, more charming and with more degrees of freedom to define what we want with money.

General Principles of Local or Global or Digital Currencies
(The principles are desired, but not all principles are realized by the rules)

1. Principle of democratic equality

Whenever new currency is issued, it belongs to the collective equally to all. All members are equal with respect to the rules of the currency. The value of the currency corresponds to the productive and wealth creating ability of the people as individuals and collectively. Every situation and intention for productivity by a person or group of persons that will be good for the collective, and if the lupper limit of percentage of money to the non-money wealth of the society is nor surpassed, is a good reason for issuing of money to create more than 80% equity capital (and not borrowed liability capital) to support the productivity.

2. Principle of consistent inheritance of the civilization to all

Every person has the birth right till the end of his life to basic goods and services for good survival. This is done through the minimal subsidy or free basic income of survival, which defines a non-zero-sum periodic residual for every person

3. Principle of non-proprietary money (2nd generation money) and proprietary money (1st generation money)

The 2nd generation money is only abstract units of measurement of economic subjective value, therefore it cannot be property of anyone. Currency cannot be bought sold, lent, or borrowed, on an interest rate. Instead of owning amounts of currency, there is the almost equivalent concept of temporary credit from the collective to any member of the collective, for any goods and services that the collective can provide, measured in units of economic value. If the local central authority itself owns such "money" units, then it means that it is inversely a temporary credit from the members of the collective to the collective, for goods and services that the collective can provide, measured in units of economic value. The value of the currency corresponds to the productive and wealth creating ability of the people as atoms and collectively. 1st generation money has the properties 1) portable for purposes of means of exchange and transactions 2) Its units of value that measure the value of goods 3) It is the store of value. But 2nd generation of money has the properties 1) 2) but not 3) as it is not store of value. Therefore, here we are taking about 2nd generation money. Modern 1st generation money that are also store of value, most probably should be a fixed basket of goods and services. E.g. the unit could be a basket of goods and services that an average person needs for a decent life during one month. Non-proprietary money (2nd generation) can be converted to proprietary 1st generation money according to in advance decided and agreed rules.

4. Principle about the amount of currency

The amount of existing currency at each time is related in a monotone increasing way to the a) size of the population b) volume of activities c) Volume of tangible wealth or assets, locally produced or imported. For small collectives, that the accounting and evaluation of the assets is difficult the dependence of the amount of currency on the 3rd factor of assets is not used.

The rules are such that for constant population, volumes of activity and tangible wealth, the amount of currency is asymptotically constant (so no inflation is created by the rules of the currency itself). For example, if only the c)

factor of the volume of tangible wealth or assets, a suggested of corresponding size of money amount would be 66% (=2/3). This is as percentage about the percentage of water in the biomass.

5. Principle of reduction of inequalities

The collective network puts rules of the currency, so as to reduce in a consistent way the financial inequalities.

(The principles are desired, but not all principles are realized by the rules of the currency)

6.1. Principle of the central local authority (case of public authority issuing the currency)

The collective network has privilege as far as issuing, and distribution of the currency compared to the members, only so as to serve the totality of the members and the environment.

6.2. Principle of non-central authority. (case of private enterprise issuing the currency)

The administrators of the collective network have no privilege as far as issuing, and distribution of the currency compared to the members.

7. Principle of non-debt society.

The issued currency is circulating from the issuing agency to the collective mainly (e.g. suggested at least by 4/5) with other ways than debt.

8. Principle of economic autonomy

The rules are such that the collective can sustain itself economically for an indefinitely time under normal conditions. This means that exports and imports both for tangible goods and intangible services are not non-balancing in systematic way in such amounts that supersede the ability of payments by the collective.

Local (City) Government Currency Within the Old Banking Currency Rules of the Network

The members of the local currency can be physical persons, enterprises and the local city government itself.

The percentages x%, y%, z%, 1% reduction monthly etc are universal constants and parameters of the local currency.

1. Rules of issuing and distribution of the currency (Population, assets and volume of activities

1.1. Every month the local (city) government is issuing and is giving a constant amount per each person-member of the network as survival subside(e.g. 1000 equivalent to euro). The issued currency has a date of birth in the computer system. This covers the principle 2, and that the amount of circulating currency depends only on the number of individuals in the population as backed-up by the intangible assets of productivity of the individuals of the population. Alternatively it depends both on the number of individuals in the population plus as percentage of the value of the total assets-wealth of the population both tangible in t% and intangible in i% and also as percentage of the volume of productive activities (local group GDP) p%. It also covers the principle 5 of reduction of inequalities.

1.2. But at the same time, when 1.1 is applied the local government is issuing 2 times the same amount for each member, so that half of it serves as the taxes, corresponding to that person, and the other half, for the ecological environment and foreign (to the collective) transactions with other collectives. We notice here that although there is "taxation" for persons there is no for organizations. As economic organizations reflect also economic inequalities, this means the local government does not have advantage in the taxes by higher economic inequalities.

1.3. At each indented transaction between two members of the local currency, x% (e.g. 10%, but it maybe agreed to be 100% also) of its value is done in the local electronic currency (possibly after issuing automatically by the local government the necessary local currency), for the buying side, which is received by the selling side. The issued currency has a date of birth in the computer system.

1.4. For small collectives of local currency the dependence of the issued currency on the existing wealth does not apply, for reasons of non-available information and the principle 5. But if it does apply, then there is a one time initial issuing and granting of an amount of local currency at the subscription of the member in the local currency proportional to the size of its assets with a coefficient equal for all members.

2. Rules of currency withdrawal from circulation for asymptotic constant amount of currency

2.1. Any amount of local currency as a kind of automatic tax that does no go to anyone though not even to the local government, or withdrawal from circulation, decreases its value, by 1% monthly (in general y% monthly), and

in general proportionally in time with the above rate, according to its date of birth. The 1% is set so the annual rate of decrease is close to the rate of a low taxation, thus familiar. Otherwise higher rates, would make the local currency undesirable to store economic value compared to the old banking currency (e.g. Euro). Furthermore this rule of simple proportionality can be improved (relative to the principle 5) to be with an increasing percentage to the size of the amount of currency according to an agreed table exactly as it is down in the taxation in the current banking currency (e.g., euro) This rule of depletion of the value of the currency are set so as to have asymptotically constant amount of circulating currency relative to population, and thus no inflation due to the issuing of new currency.

Alternatively to this rule is that the currency does not lose money by time, but at the death of a person all the currency that he/she poses is annihilated. Again for constant population and length of life, this creates a constant amount of currency which therefore is not inflationary.

2.2. Alternatively to 2.1, at each transaction, as a kind of automatic tax that does no go to anyone though, there is a subtraction of the part of the value, of the transaction in the local currency by 12%. which is charged equally as 6% to the buying and selling sides. Furthermore this rule of simple proportionality can be improved (relative to the principle 5) to be with an increasing percentage to the size of the amount of currency according to an agreed table exactly as it is down in the taxation in the current banking currency (e.g., euro This rule of withdrawal of currency from circulation is set so as to have asymptotically constant amount of circulating currency relative to the volume of activities, and thus no inflation due to the issuing of new currency.

2.3 Receipts and other accounting documents are produced for every transaction as if it was carried out in full value in the old banking currency. National taxes are paid also in full in the old banking currency, by both sides.

3. Rules of authority responsibilities and economics

3.1. The local (city) that runs the network of the local currency through the internet, acts as a not-for- profit organization. The accumulated funds in the local currency, by the "taxation" (rule 1.2) are utilized exclusively for the common good, of the collective, and only after appropriate direct-democratic voting (through the internet) and financial auditing, of the members to the administrators of the local (city) government.

4. Rules of correlation of the local currency with the old banking currency.

1.1. The cross exchange rate of the local electronic currency to the parallel global banking currency (e.g. euro) is determined either in a semi-fixed rate adjusted by a political decision after a voting of all members of the network, or it is left free-floating defined daily by the free market of exchanges.

1.2. Any person, enterprise, or other organization that becomes a member of the local currency is committed to provide at least z% (e.g. 10% as in Sardex) of its sales, if there is demand for it, by other members of the local currency, to be carried out in the local currency. This includes both tangible goods and intangible services and salaries (as long as both the organization and the employee are members of the local currency).

1.3. Any transaction between two members of the local currency must be done in at least x% of its total value, in the local currency (e.g. 10% or 100%). But there is a veto option for the member-buyer to have it 100% in the local currency. This veto option of the buyer cannot override the veto option too of the seller not to make available more than z% (e.g. 10% as in Sardex) of its sales in the local non-banking currency.

5. Rules of economic autonomy

The details of the rules so as to have economic autonomy as in the principle 8, are left open.

Private Enterprise Local Currency Within the Old Banking Currency. Rules of the Network

The members of the local currency can be physical persons, enterprises or the local city government itself. The percentages x%, y% (or 1% reduction monthly), z%, etc are universal constants and parameters of the local currency.

1. Rules of issuing of the currency and distribution (Population, assets and volume of activities)

1.1. Every month the network is issuing and is giving a constant amount per each person-member of the network as survival subside (e.g. 1000 equivalent to euro). The issued currency has a date of birth in the computer system. This covers the principle 2, and that the amount of circulating currency depends only on the number of individuals in the population as backed-up by the intangible assets of productivity of the individuals of the population. Alternatively it depends both on the number of individuals in the population plus as percentage of the value of the total assets-wealth of the population both tangible in t% and intangible in i% and also as percentage of the volume of productive

activities (local group GDP) p%. It also covers the principle 5 of reduction of inequalities.

1.2. At each indented transaction between two members of the local currency, x% (e.g. 10% or even 100%) of its value is done through the electronic local currency (possibly after issuing the necessary local currency), for the buying side, which is received by the selling side. The issued currency has a date of birth in the computer system.

1.3. For small collectives of local currency the dependence of the issued currency on the existing wealth does not apply, for reasons of non-available information and the principle 5.

2. Rules of taxation or currency withdrawal from circulation for asymptotic constant amount of currency

2.1. Any amount of local currency as a kind of automatic tax that does no go to anyone though, or withdrawal from circulation, decreases its value, by 1% monthly (in general y% monthly), and in general proportionally in time with the above rate, according to its date of birth. The 1% is set so at the annual rate of decrease is close to the rate of a low taxation, thus familiar. Otherwise higher rates, would make the local currency undesirable to store economic value compared to the old banking currency (e.g. Euro). Furthermore this rule of simple proportionality can be improved (relative to the principle 5) to be with an increasing percentage to the size of the amount of currency according to an agreed table exactly as it is down in the taxation in the current banking currency (e.g., euro) This rule of depletion of the value of the currency is set so as to have asymptotically constant amount of circulating currency relative to population, and thus no inflation due to the issuing of new currency. *Alternatively to this rule is that the currency does not lose money by time, but at the death of a person all the currency that he/she poses is annihilated. Again for constant population and length of life, this creates a constant amount of currency which therefore is not inflationary.*

2.2. Alternatively to 2.1, at each transaction, as a kind of automatic tax that does no go to anyone though, there is a subtraction of the value, of the transaction in the local currency by 12%. which is charged equally as 6% to the buying and selling sides. Furthermore this rule of simple proportionality can be improved (relative to the principle 5) to be with an increasing percentage to the size of the amount of currency according to an agreed table exactly as it is down in the taxation in the current banking currency (e.g., euro) This rule of withdrawal of currency from circulation is set so as to have asymptotically

constant amount of circulating currency relative to the volume of activities, and thus no inflation due to the issuing of new currency.

2.3. Receipts and other accounting documents are produced for every transaction as if it was carried out in full value in the old banking currency. National taxes are paid also in full in the old banking currency, by both sides.

3. Rules of network administration reward

3.1 The private enterprise that runs the network of the local currency through the internet, should be preferably but not necessarily a not-for-profit organization. The covering of the costs of this organization is through monthly fees, that are z% (e.g. 10%) in the local currency and 100%-z% in the old banking currency (e.g. euro). The organization that coordinates the local currency has the same rights and privileges as any other member organization of the local currency.

4. Rules of correlation of the local currency with the old banking currency

4.1. The cross exchange rate of the local electronic currency to the parallel global banking currency (e.g. euro) is determined either in a semi-fixed rate adjusted by a political decision after a voting of all members of the network, or it is left free-floating defined daily by the free market of exchanges.

4.2. Any person, enterprise, or other organization that becomes a member of the local currency is committed to provide at least z% (e.g. as in Sardex 10%) of its sales, if there is demand for it by other members of the local currency, to be carried out in the local currency. This includes both tangible goods and intangible services and salaries (as long as both the organization and the employee are members of the local currency).

4.3. Any transaction between two members of the local currency must be done in at least x% (e.g. 10% but also maybe 100%) of its total value, in the local currency. But there is a veto option for the buyer to have it 100% in the local currency. This veto option of the buyer cannot override the veto option too of the seller not to make available more than z% (e.g. 10% as in the local currency of Sardex) of its sales in the local non-banking currency.

5. Rules of economic autonomy

The details of the rules so as to have economic autonomy as in the principle 8, are left open.

4. Conclusions

We summarize the conclusions of this article's analysis in a short list of 4 points

1. The exercise of substantial constructive justice and ethics in the financial decision making should be based on the principles of evolution of the soul consciousness and collective social good of the majority and not on the interests of a privileged financial oligarchy against the many. Otherwise, it is an exercise of destructive, short-sighted, bureaucratic regressive justice and economy.

2. Poverty is the main system evil of our economy and it can be cured through the free basic income. But unfortunately the free basic income cannot be derived solely from taxes, as it is a too large expense. It has to come directly from the money issuing organization.

3. We discover 5 toxic anti-democratic functions of the banking monetary system that create periodically debt crises. These functions originate during the gold standard an as the gold standard has been abandoned, so we can also correct them through top-down democratization of the banking monetary system. In this way poverty can also be eliminated as the free basic income can be derived now directly from money issuing.

4. Alternatively, the poverty may be eliminated with the free basic income through bottom-up alternative decentralized non-banking digital local or global currencies. We state the necessary principles for such currencies (governmental or not) and we give 2 examples of designs of them which are fully taxed within the old banking currencies.

References

Richard Wilkinson, How financial inequalities harm societies. https://www.ted.com/talks/richard_wilkinson?language=el

A Statistical Analysis of the Expenditures on Research and Development and the Increase of Gross Domestic Product: an sensible way for Easing the Effects of Greek Economic Crisis https://www.researchgate.net/publication/319220589_A_Statistical_Analysis_of_the_Expenditures_on_Resear ch_and_Development_and_the_Increase_of_Gross_Domestic_Product_an_sensible_way_for_Easing_the_Effe cts_of_Greek_Economic_Crisis

Over-debt Monetary system http://overdebtmonetarysystem.blogspot.gr/2012/04/6-how-central-banks-violate- us.html http://www.quirinale.

it/qrnw/statico/costituzione/pdf/costituzione_inglese.pdf, http://www.tribunalconstitucional.pt/tc/conteudo/files/constituicaoingles.pdf
Bank of England, Wikipedia https://en.wikipedia.org/wiki/Bank_of_England
Banking in Europe https://wiki.mises.org/wiki/History_of_money_and_banking
Constitution, laws and bank money minting. http://accfin.teiep.gr/eclass/modules/document/file.php/TMA242/%CE%9C%CE%9F%CE%A5%CE%9A%C E%91%20%CE%A3%CE%A4%CE%91%CE%9C%CE%91%CE%A4%CE%99%CE%91.pdf
Woodrow Wilson https://en.wikipedia.org/wiki/Woodrow_Wilson
Over-debt Monetary system Conclusions http://overdebtmonetarysystem.blogspot.gr/2015/02/9-conclusion.html https://crisismonetarysystem.blogspot.com/2015/02/74.html
Independency of ECB. https://www.ecb.europa.eu/ecb/legal/pdf/c_32620121026el.pdf
Collateral Accounts https://www.youtube.com/watch?v=1ML3hEcSKgc&t=283s, https://www.youtube.com/watch?v=1ML3hEcSKgc, https://www.bibliotecapleyades.net/sociopolitica/sociopol_globalbanking96.htm
"Money and financial system", Gikas G., Hyz A. (2017), rule of liquid inventories, Briken Hill publications.
"Introduction to Bank economics and capital markets:, Syriopoulos Constantine, Papadamou Stefanos, Utopia publications, 2014.
Money, Credit, Banks, Kiochos P. – Papaniklolaou G., published by Kiochou Eleni publications. [14] Financial-economic administration I, II, G. P. Artikes, 2013
Gradido currency, Bernd Hückstädt (Author) https://www.amazon.com/Gradido-natural-economy-Bernd-H%C3%BCckst%C3%A4dt/dp/1291004610
Lotka-Voltera https://en.wikipedia.org/wiki/Lotka%E2%80%93Volterra_equations
Basel III, https://en.wikipedia.org/wiki/Basel_III
ECB Annual reports https://www.ecb.europa.eu/home/html/index.en.html [19] The Location of U.S. Currency: How Much Is Abroad? https://www.federalreserve.gov/pubs/bulletin/1996/1096lead.pdf
Use of e-commerce, http://www.statistics.gr/el/infographic-ecommerce-2017
Crypto currencies https://en.wikipedia.org/wiki/Cryptocurrency
Crowdfunding https://en.wikipedia.org/wiki/Crowdfunding
Microfinance https://en.wikipedia.org/wiki/Microfinance [24] Poverty, money and love https://www.ted.com/talks/jessica_jackley_poverty_money_and_love

Financial mathematics, Petros Kiochos, Apostolis Kiochos, Interbooks, 2nd edition.
Xafa, M. (2014) "Sovereign Debt Crisis Management: Lessons from the 2012 Greek Debt Restructuring", CIGI Papers no 33.
https://www.eurobank.gr
https://www.hba.gr/Statistics/List?type=GreeceBrief
http://www.alpha.gr/
http://www.piraeusbank.gr

REAL PROPERTY TAXATION IN GREECE, THE EFFECTS ON THE REAL ESTATE MARKET AND ON THE ECONOMIC SYSTEM OF THE COUNTRY

E. CHRYSOGONIDOU* P. KYRMIZOGLOU**

Abstract

The purpose of this paper is to highlight the problems created by the sudden increase in real property taxation in the real estate market, the burden on the construction industry, the reduction of demand and therefore real estate prices, the pressure on the financial system of banks, but also the pressure this in turn has on the market by reducing funding.

JEL Classification: E62, H2

Keywords: Real estate, Property taxes, Real estate prices

1. Introduction

Property taxes are considered to be the least burdensome for development with the fewest distortions for the economy (Arnold, 2008). However, the effects of the imposition of high property taxes are not immediately perceptible. The real estate market is directly affected by the increase in taxation, construction activity shrinks, the banking system and other macroeconomic performances of the economy are affected, ultimately creating a more unfavorable overall result in the course of development.

Through the empirical monitoring of transactions, macroeconomic figures and other short-term indicators, an attempt is made to record the effects of the tax increase in our country. While, through primary research, the evaluation of the tax system in terms of economic efficiency and justice in general, but also in particular the real property tax, as well as the return of investors was attempted. Determining the factors that affect the price of real estate also examines whether these changes affect the financial system. The current market situation is recorded and corrective actions made or discussed for the next period are evaluated.

* MSc Accounting and Information Systems, International Hellenic University, Thessaloniki, Greece.

** Professor, Department of Accounting and Information Systems, International Hellenic University, Thessaloniki, Greece, e-mail: pkirmiz@acc.teithe.gr

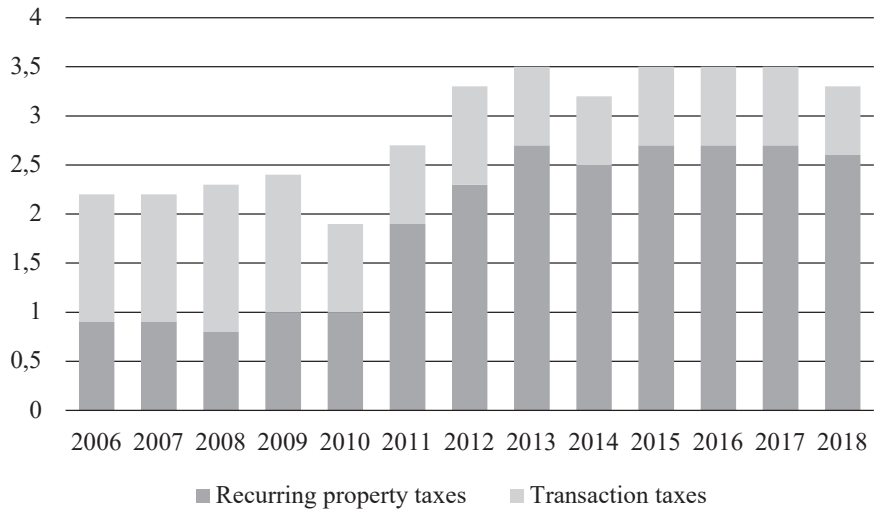
There are opinions arguing that real property taxation gives fiscal governments budgetary margins to make the tax system more efficient and equitable with the least possible distortions (Musgrave & Musgrave, 1989). Their use reduces the dependence of a tax system on income or consumption taxes (Trojanek & Kisiala, 2018). However, the real estate market is a very important sector of the economy with a multiplying effect on the course of the country's economy and the financial system (Maniatis, et al., 2019). High real property taxation can have adverse effects that are not immediately perceptible (Norregaard, 2013). Besides, the imposition of ENFIA failed to bring the expected tax revenues that had been set as a goal, instead it contributed to the deepening of the crisis and problems in the economy, further reducing the disposable income of citizens (Christelis, 2015).

2. Long-term and short-term sizes of the economy

Knowledge, determination and proper management of the tax base are a key factor in the effective imposition of taxes on real estate. Proper identification of

Chart 1: Property taxes as a percentage of GDP

Source: Taxation trends in the European Union, Luxembourg (2020)



the number, type and value of real estate as well as the best possible management of updates at regular intervals, are the crucial elements that make these taxes profitable.

In Greece, the positive effects they had on the overall economic development of the country are not obvious. Until 2011, revenues from real property taxes came mainly from transaction taxes and not from recurring property taxes (Rapanos & Kaplanoglou, 2014) and amounted to a total of 2.2% of GDP. From 2011 and on, the taxes from the transactions were reduced due to the reduction of the transactions in the real estate but also of the tax rates a

Table 1: GDP, house price Index and rent Index

Year	G.D.P.		House Price Index		Rent Index	Index P/R
	Current price (million)	annual change percent	nominal prices	annual change percent	annual change percent	
2007			100,00	5,90		
2008	241,990		101,70	1,70	3,90	97,90
2009	237,534	-1,84	97,90	-3,70	3,60	91,00
2010	224,124	-5,65	93,3	-4,70	2,40	84,70
2011	203,308	-9,28	88,20	-5,50	0,80	79,40
2012	188,389	-7,33	78,00	-11,70	-2,10	71,60
2013	179,616	-4,65	69,50	-10,90	-6,80	68,50
2014	177,349	-1,26	64,30	-7,50	-7,70	68,60
2015	176,110	-0,69	61,10	-5,10	-4,40	68,20
2016	174,237	-1,00	59,60	-2,40	-2,60	68,30
2017	177,152	1,60	59,00	-1,00	-2,20	69,20
2018	179,727	1,40	60,10	1,80	-3,20	72,70
2019	183,413	2,05	64,40	7,20		78,00

Source: Bank of Greece, ELSTAT

little later. Due to the large increase in recurring property taxes, total revenues from real property taxes increased, reaching 3.3% in 2018 (Taxation trends in the European Union, 2020). They continue to have a relatively small share in the tax revenues of the country since in 2019 they accounted for 5.4% of total tax revenues. (A.A.D.E., 2019).

With the imposition of high recurring property taxes, however, household disposable income already burdened by the financial crisis has shrunk even further, as has consumption, of course not in favor of savings which were moving negatively over the same period, while at the same time investments had been reduced to zero. In an attempt to maintain a level of consumption and meet basic needs on the one hand, or in an attempt to meet tax liabilities on the other, households used the already saved income.

Real estate returns fell, which led to a sharp drop in transactions. The market was frozen and this resulted in the inability of households to liquidate the real estate in order to cover the ever-increasing liabilities. Prices fell at a faster rate of change than GDP (table 1), especially after the imposition of recurring property taxes (Chart 2).

The construction industry was further burdened by the imposition of recurring property taxes. The imposition of VAT on real estate brought a drop in the issuance of new building permits initially with an average annual reduction of around 10% which however tripled in 2011 from the imposition of new property taxes, reaching 36% in 2012. Construction costs did not follow the same reduction in prices, therefore the return on investments for constructors decreased significantly.

Chart 2: GDP & H.P.I. (House Price Index) at nominal prices

Source: Bank of Greece, ELSTAT

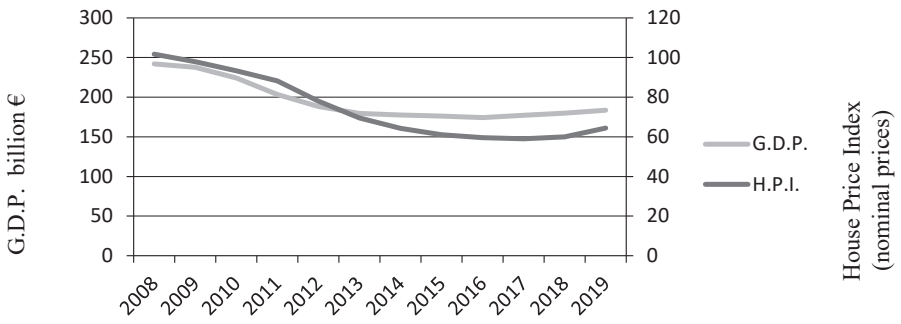


Table 2: Building Permits

	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Building Permits thousand	74	63	79	67	57	51	36	23	16	13	13	12,6	14	15	17
annual change percent		14,8	25,4	15,2	14,9	10,5	29,4	36,1	30,4	18,7	-	3,1	11,1	7,1	13,3

Source: IOBE, ELSTAT

3. Financial system

This situation logically affects the banking system as well. Banks also own real estate, so the value of their portfolio is directly affected by falling prices, but at the same time their credit risk is affected. The reduction of prices leads to a reduction of the return of the real estate; the liquidity of the consumers is limited so there are difficulties in the repayment of loans that have already been given. Also, the use of real estate as a guarantee for the provision of new financing can no longer achieve the same values, resulting in the reduction of financing, and therefore of the total liquidity in the market and households. This creates a vicious circle in the economy that simply feeds back the problem.

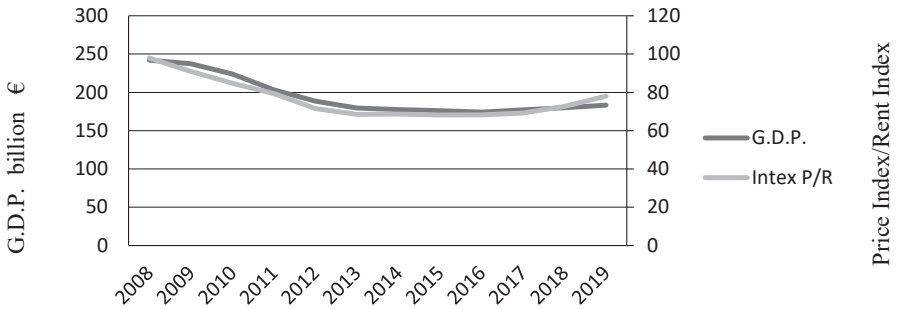
According to Chaliasos, (2012) Greece is a country where residents traditionally invest in real estate, which are by far the most important asset of households (over 80%), while on the other hand they have minimum liquid assets. Let us not forget that home ownership has very high levels in our country. Imposing a tax on real property was expected to put even more pressure on the already burdened disposable income and to bring worse results to the economy than expected. About 80% of the total bank deposits belonged to households (Chaliasos, 2012). In other words, the economic circumstances were such that the banking system was directly dependent on households, which presented marginal liquidity in the composition of their financial data. This fact in combination with the reduction of wages, uncertainty, unemployment led to the increase of the percentage of due loans from 5% in 2008 to 49% in the period 2016-17 (Bank of Greece, 2020).

The study and recording of changes in property prices has emerged in recent years as particularly critical. Indicators were created to monitor these changes as well as movements of this particular market. It is not uncommon for changes in the housing market to be used even as forecasts for future economic turmoil. Many argue that the abrupt fluctuations in the housing price index to rent may herald the existence of a bubble in property prices (Hardouvelis, 2009). It is worth noting that the recessions that follow such an abrupt change in prices are up to three times greater than recessions caused by other events (Praet, 2019). However, it is very difficult to diagnose this phenomenon at the time it occurs. In Greece, however, for the period under review, the above-mentioned index remained at expected levels without abrupt fluctuations, following almost completely the change in GDP (Bank of Greece, 2020) (Chart 3).

In recent years, efforts have been made to strengthen and stimulate this sector of the economy. The reduction of ENFIA rates, the suspension of VAT and the arrangements for strengthening the banking system, seem to have a positive effect in the end (ELSTAT, 2020). There is an increase in the issuance of building permits, a doubling of real estate transactions and an increase in prices as well as the demand for new building loans. Even foreign investments in high value real estate in Greece have increased significantly in recent years, accounting for 35% of the country's total foreign investment for 2019 (Mitrakos, 2020).

Chart 3: GDP & Price Index/Rent Index

Source: Bank of Greece, ELSTAT



4. Research

In the context of the present paper, an attempt was made to approach the issue with primary data that were collected. The purpose was to record the views of people involved in the real estate market, the problems they faced from the abrupt increase in taxation, but also their expectations for the future.

4.1 Planning and methodology

The issues that were examined are the feeling that exists towards the existing tax system, the factors that affect real estate prices, the interdependence with the banking system and the market movement as well. Finally, corrective actions of the state that were made or are being discussed in the future were evaluated.

It took place in October and November 2020 to a targeted audience, which deals with the real estate market. Specifically to Notaries, lawyers, engineers, real estate agents, civil and municipal employees (employed in real estate departments), as well as bank employees (employed in lending departments) in the Prefectures of Thessaloniki, Pella and Kilkis.

The questionnaire contained 24 questions. It was compiled and distributed electronically through the Google Forms platform and responses were collected, quantified and processed in Excel sheets.

4.2. Research results

The study involved 248 people, most of them with a university degree. It was considered important to find out whether the participants are also property owners or not. The majority of 41% have up to two properties, 28% have three to five properties, while 14% answered that they have more than six properties. In other words, in addition to their professional occupation with real estate, they themselves are burdened by the imposition of taxation.

The economic efficiency, the financial justice of the tax system, as well as the profitability of real estate investment were examined. The efficiency of a tax system is judged by its results, that is, whether it enhances growth by supporting the economic prosperity of citizens, entrepreneurship, work, by creating incentives and not restrictions. The country's tax system has failed to clearly convince citizens of its performance, with 36% saying they are a little convinced, and 16% not at all compared to those who think it is quite efficient (38%) and very efficient (10%). It fails much more to create a sense of justice

for equal treatment. 51% think it is a little fair while 29% say it is not at all fair. On the one hand, property taxation is considered a little (by 43%) fair and not at all fair by 23%, in the sense that owning real estate is an indicator of tax capacity but also a means of redistributing income from the richest, who are more burdened, to the weaker. But on the other hand there is a sense of injustice regarding double income taxation which has simply changed form without generating additional revenue. 45% of the respondents answered it is not at all fair and 39% that it is a little fair. After all, real estate cannot be a tax target by the state due to its immediate and easy identification.

Price pressure from imposing a new tax on already acquired property reduces its value, as well as its expected return. This, of course, affects the holder's behavior in terms of his disposable income or the amount he intends to spend. It is considered to be quite affected by 40% and absolutely by 11%. It is obvious that in case the property has been acquired with a loan, the owner is burdened even more, since the fall in property prices puts pressure on the banking system. On the other hand, the new buyer is indifferent (36%) to the imposition of a new tax. In order to proceed with the investment, the new charge on its return has been calculated, since it is integrated in the price and reduces it. The participants state that it is slightly affected in 29%, but also a 19% consider that it is affected enough. Obviously these answers concern the stability of the country's tax system, which makes the forecast for future returns more valid and secure. In an environment of instability, investors are more restrained because of the increased risk. However, the fall in prices after the imposition of a new tax has an impact on the supply of new real estate. Their construction costs remain at the same increased levels the selling prices are reduced, so the builders return also decreases, so the quantity of new real estate offered decreases, a fact which increases the prices.

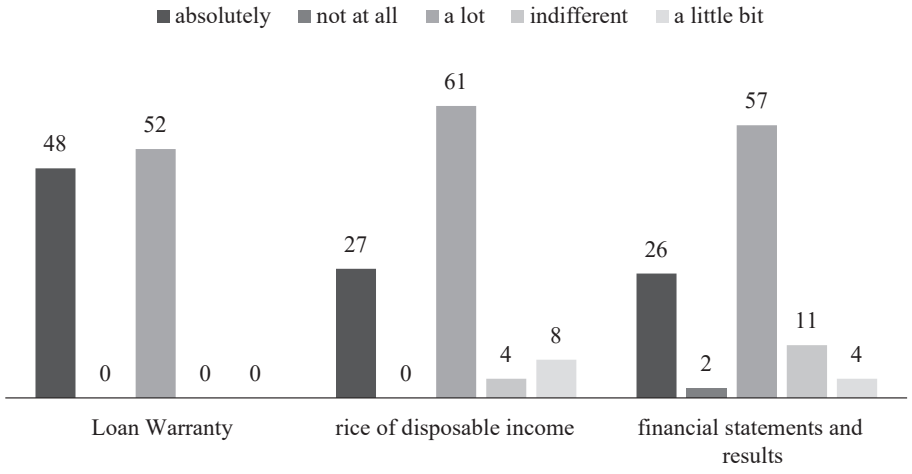
Some of the factors that determine prices, as well as the dependence of the financial system on them were evaluated. The utility of the property, its location as well as the factors of supply and demand and the coverage of needs are considered very important. However, the factor of disposable income, that is, the purchasing power of consumers, which is considered to completely affect prices by 49%, is considered even more important (table 3).

The problem that exists in our country regarding the monitoring and recording of changes in prices and the valuation of real estate according to market conditions, is of major importance and creates many problems in transactions (56% say enough and 39% absolutely). Even within the same services the set prices are different. In addition, the difference that exists between commercial and objective prices in Greece is considered to fully burden the transactions at

Table 3: Factors that determine prices (percentage %)

	Not at all	A little bit	Indifferent	Enough	Absolutely
Utility	6	6	4	68	20
Stock of real estate	2	15	22	47	14
Supply and demand		4		48	48
Special offers	3	12	18	58	9
Location		4	10	45	41
Coverage of needs	13	29	36	18	2
Disposable income		3	4	44	49

Chart 4: Dependence of the banking system on real estate prices (percentage %)



a rate of 48% and quite at 45%. This fact indicates the need for uniform legislation and treatment of the issue and systematic monitoring of real prices. The optimistic scenario claims that the completion of the Cadastre will help in this direction as well, in the aspect that it will greatly enhance the confidence of

investors in the market by 60% and 14% absolutely. At the moment there is no official public body to monitor and control the declared price of transactions. There is a feeling, however, that the transactions will be greatly facilitated (46%) and a very significant percentage of 38% believe that they will be completely facilitated by the completion of the cadastre.

Price stability is a factor that also plays an important role for a sound financial system. The financial statements and results of banks are directly and indirectly affected by the fluctuations, their decline leads to a reduction in financing with all that this entails for the economy and the vicious circle that is created. But also the uncontrolled rise, can lead to bubbles with catastrophic effects on the economy. The housing market is considered according to the research to be prone to bubbles and is affected very much by 60% and absolutely by 23%.

The results of the research regarding the dependence of the banking system on real estate prices are presented in detail in the following Chart 4

Factors that led the market to the current situation were examined while evaluating the corrective measures taken by the management or proposed for the future. The shrinking of disposable income mainly, the reduction of bank financing and the imposition of high taxation, were the main aggravating factors that led the market to this situation (Table 4).

The corrective measures taken in recent years by the state regarding banks and due loans, the suspension of VAT, but also the reduction of ENFIA rates, led to an increase in the return on investment in real estate, stimulated the domestic market, but strengthened foreign investment even more, which seems

Table 4: Factors that negatively affected real estate transactions (percentage %)

	Not at all	A little bit	Indifferent	A lot	Absolutely
Reduction of bank financing		12		59	29
Stock of real estate	1	12	7	63	17
Shrinking of disposable income		2		33	65
High taxation		3	15	48	31

Table 5: Factors that positively affect real estate transactions (percentage %)

	Not at all	A little bit	Indifferent	A lot	Absolutely
Settings on red loans	6	12	20	46	16
Suspension of VAT	5	14	13	55	13
Abolition of the supplementary EN.F.IA	3	11	9	58	19
Foreign investment capitals from abroad	7	18	18	15	42

to be at a percentage of 42% entirely responsible for improving the market image (Table 5). Also, a percentage of 58% of the respondents believe that the abolition of the supplementary EN.F.IA. will greatly strengthen this sector and a significant percentage of 19% that it will absolutely strengthen it.

The completion of the cadastre is expected to give a new impetus, as well as to improve the existing conditions, as there is a belief that it will secure the property by 36% absolutely and 47% a lot. However, regarding the fair distribution of taxes, there is a perception that the operation of the cadastre is indifferent at a rate of 43%. Another thing that is not expected to have such a big effect on the return of property taxes is the transfer of their management to the local government. Even though it may be more associated with exchanges that will be more immediate and visible to citizens.

Finally, an issue that was raised and requires immediate resolution and may be corrected by the operation of the cadastre and the intensification of inspections is the falsely stated price in the transactions. Tax evasion may not be accurately measured, but there are few cases where the declared price is the real one. Survey participants believe that the existing system ensures little (53%) or not at all (23%) the honest recording of the price in transactions and only 12% believe that it is captured sufficiently.

5. Conclusions

In our country, the imposition of high recurring property taxes further burdened the already reduced disposable income and consumption. Savings moved to negative levels and investments were eliminated. Real estate prices fell, driving investors' returns to zero and freezing the market. The possibility of liquidation of household real estate was non-existent. This whole situation put even more pressure on the banks, which on the one hand were unable to restore liquidity in the market and on the other hand reduced their financing even more, under pressure themselves, directly and indirectly, from falling prices. This created a vicious circle in the economy that merely fed back the problem.

Knowledge and determination of the tax base, in terms of the number of properties, their type and value, in combination with the financial level of their owners and their tax capacity, is a tool in the hands of the administration for effective fiscal policy. The unified calculation of the value of the properties based on their real market price and the constant monitoring of changes is a precondition for the development of the specific sector but also for the improvement of the tax efficiency. The strengthening of the state audit services as well as the upgrading of the computerization systems, certainly contributes in this direction. The abolition of additional ENFIA, which is considered the main deterrent for investors, could also create conditions for growth, not only of the specific sector of construction and the real estate market, but also of the entire economy of the country, boosting domestic investments while attracting capitals from abroad.

Bibliography

A.A.D.E. (2019). *Revenue Report.* Athens: AADE.

A.A.D.E. (2019). *Report on the evolution and fluctuation of tax revenues.* Athens: A.A.D.E.

Arnold, J. (2008). *Do Tax Structures Affect Aggregate Economic Growth? Empirical Evidence Form a Panel of OECD Countries.* Economics Department Working Papers. Paris: OECD.

Bank of Greece. (2013, 04). *bankofgreece.gr/realestate.* Recovery 08 10, 2020, from www.bankofgreece.gr

Bank of Greece. (2020). *Report on loans and arrears.* (B. of. Greece,) Recovery 11 20, 2020, from www.bamkofgreece.gr:

Bank of Greece. (2020, 01 21). *Bank granting research.* Recovery 04 30, 2020

Bank of Greece. (n.d.). *Real Estate Market Indicators.* Recovery 10 01, 2020, from www.bankofgreece.gr

Bank of Greece. (2020). *Summary of Main Available Short-Term Indicators for the Purchase of Real Estate.* Recovery 08 04, 2020

Christelis, D. (2015). Wealth Taxation of Real Estate During the Greek Crisis: The Perils of Ignoring Market Signals. *Vierteijahrshefte zur Wirtschafls-forschung*, σσ. pp. 61-83.

ELSTAT. (2020, 10 29). *Basic Macroeconomic Sizes.* Recovery 11 20, 2020, from www.statistics.gr

ELSTAT. (2020, 11 13). *Notary Works 2019.* Recovery 12 01, 2020, from www.statistics.gr

ELSTAT. (2020, 03). *Construction activity research.* Recovery 09 10, 2020, from www.statiticks.gr

ELSTAT. (2020). *The Greek Economy.* Athens: ELSTAT.

ELSTAT. (2020, 10 16). *Sizes Per Capita.* Recovery 11 20, 2020, from www.statistics.gr

EUROSTAT. (2020, 05). *Housing statisticks*. Recovery 10 01, 2020, from ec.europa.eu:

Haliasos, M. (2012, 12). Real estate as part of household property: International differences and the role of innovation. The Real Estate Market in the recent financial crisis, 16-20. Athens, Greece: Bank of Greece.

Hardouvelis, G. (2009, 04 27). The Importance of the Housing Market in the Economy. *"Real estate market: Recent developments and prospects"*, 13-58. Athens: Conference of the Bank of Greece.

Maniatis, G., & Pavlou, G. (2018, 09). *Real estate taxation and the future of the industry of constructions in Greece.* Athens: I.O.B.E.

Maniatis, G., Mitsopoulos, M., & Pavlou, G. (2019). *The developmental prospects of the construction industry in Greece.* IOBE, Collaboration with SEB. Athens: IOBE.

Mitrakos, Th. (2020). *euractiv.gr*. (Greece Investor Guide, Editor, & Greece Investor Guide,) Recovery 12 05, 2020

Mitrakos, Th. (2009). *Statistics and House Price Indicators : The new initiative of the Bank of Greece.* Athens: Bank of Greece.

Musgrave, R., & Musgrave, P. B. (1989). *Public Finance in Theory and Practice.* McGraw-Hill International Editions- Finanse Series.

Norregaard, J. (2013). *Taxing Immovable Property Revenue Potential and Implementation Challenges.* International Monetary Fund. IMF Working Paper.

Pavlou, G., & Maniatis, G. (2015, 03). The importance of development, the

obstacles and the future of the construction industry. (IOBE, Edit.) Athens: Institute of Economic & Industrial Research.

Praet, P. (2019, 02 21). *ecb.europa.eu.* Recovery 06 2020

Rapanos, V. Th., & Kaplanoglou, G. (2014). Taxation and economic development. The case of Greece. In the Collective Volume of the Hellenic Banking Association with topic "Competitiveness for Development. Policy Proposals" (pp. 609-638). Hellenic Banking Association.

Simigiannis, G. & Chondrogiannis, G., 2009. *Residential prices*: *The recent Greek experience*, Athens: Bank of Greece.

Taxation trends in the European Union, L. (2020). *europa.eu.* Recovery 09 17, 2020

Trojanek, M., & Kisiala, W. (2018). *Recurrent Property Taxes in Communal Budgets – Identification of Types of Communes and their Spatial Differentiation.* Real Estate Management and Valuation.

A SURVEY ON LATTICE-BASED BLIND SIGNATURES AND THEIR FEASIBILITY

D. PAPACHRISTOUDIS*

Abstract

Lattice-based cryptography has proved to be a very promising and versatile candidate for the post-quantum era. While it has been widely successful for more basic cryptographic primitives like digital signatures, much less progress has been made with more advanced primitives like blind signature schemes. This article provides a comparative overview of developments regarding lattice-based blind signature schemes in terms of security and feasibility. We review security flaws and potential attacks, bottlenecks in their performance, implementation issues, and the applicability of known impossibility results from the literature. A comparison is also made with alternative post-quantum proposals.

JEL Classification: O3, G2, M2

Keywords: Blind signatures, Privacy-oriented cryptography, e-cash, e-voting

1. Introduction

We live in the highly digitized Age of Information. The rise of the Internet heralded a major and rapid shift from the traditional industry towards an economy based upon information technologies. Indeed, all of us employ some form of electronic services in our daily lives (e-mail services, online banking, e-learning through various software, etc). Not surprisingly, there is great effort being put in the digital transformation of the global economy as evidenced by the high precedence set for it by administrative bodies such as the European Commission (EC, n.d.),the spread of Information and Communication Technologies across all business sectors as a means of enhancing productivity, and by the dramatic increase of cryptocurrencies in only a few years (Statista, n.d.). This Internet Economy (Carlsson, 2004) gives rise to a vast new array of opportunities for businesses, it boosts the development of trustworthy technology, it enables a sustainable and vibrant economy, and it fosters an open and democratic society. A major component of this new economy is the so-called *e-business infrastructure* (hardware, software, telecom, networks,

* Doctoral Candidate, Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece, tel.: (+30) 697 2162999, e-mail: dpapachristoudis@uom.edu.gr

etc). However,digital networks are susceptible to hacking, which creates the need for sophisticated cryptographic systems in order to secure transactions over insecure digital networks. On the other hand, it is well-understood that the amount of disclosed personal user information during any form of transaction should be kept at a *strict* minimum. In general, it is paramount for *every* publicly used digital system to strike the right balance between digital security and digital anonymity.

Digital signatures are a cryptographic primitive that enables one party, termed the *signer*, to issue signatures on messages or documents, validating their authenticity to some other party, termed the *user*. Such schemes primarily safeguard against attempts of impersonation, repudiation, and message tampering. However, forfeiting the confidentiality of the message-to-be-signed becomes problematic for privacy-oriented applications in which the message needs to remain unintelligible to the signer. For example, in an e-voting scenario, it would be highly undesirable for a voter to have to reveal the contents of his ballot to the authority responsible for validation. Similarly, in an e-cash context, a digital coin should mimic the properties of a physical coin. In particular, it should refrain from exposing its serial number on creation time as this would provide insight to the bank w.r.t. where its owner opted to spend it.

Blind Signature schemes (BS) are a variant of digital signatures, pioneered by D. Chaum in 1982 (Chaum, 1983) in an effort to create an electronic version of conventional cash. Since their original conception, they have found a myriad of applications in electronic voting (Kumar et al., 2017), e-cash (Chaum, 1983), anonymous authentication via digital credentials (Baldimtsi and Lysyanskaya, 2013) like Microsoft's U-Prove (Paquin and Zaverucha, 2013), wireless sensor networks (WSN) (Zhang et al, 2012), blindly signed contracts to ensure anonymity and fairness in cryptocurrencies (Heilman et al., 2016), to name a few. The key idea in blind signature schemes is to separate the party owning the message from the party issuing signatures. This is done by allowing the owner of the message to interact through a cryptographic protocol with the signer in order to obtain a signature on it, but in a way that does not expose the message to the signer's view. The resulting signature can still be verified against the signer's public key, just like with typical digital signatures. However, nobody –not even the signer– can link a message-signature pair to a signing transcript. There have been numerous BS proposals in the literature, including early work by (Chaum, 1983; Chaum, 1984) and later advances (Okamoto, 1992; Camenisch et al., 1995; Nyberg and Rueppel, 1993; Schnorr, 1990; Pointcheval, 1998; Fan and Lei, 1998; Hauck et al., 2019). However, all are based on number-theoretic assumptions, such as the hardness of factoring

large integers, computing discrete logarithms, or the quadratic residuosity problem. Unfortunately, the security assumptions underlying these schemes are known to be vulnerable to quantum attacks thanks to Shor's algorithm (Shor, 1997). As a result, they are ill-suited candidates for the post-quantum era. There also exist BS schemes from general complexity assumptions (Döttling et al., 2017; Fischlin, 2006; Juels et al., 1997) but their efficiency under standard assumptions poses an exceptionally difficult task.

By now, lattice-based cryptography is one of the most versatile approaches for constructing provably secure, efficient, and highly parallelizable cryptographic primitives that can withstand attacks even by quantum computers. This is apparent from the number of lattice-based candidates in the third round of NIST's post-quantum cryptography standardization process (NIST, n.d.). In addition, lattice-based cryptography offers the unique feature of allowing for worst-case to average-case reductions (Ajtai, 1996; Regev, 2005; Micciancio and Regev, 2007; Peikert, 2009; Langlois and Stehle, 2015), which is *needed* for cryptographic applications. This not only allows us to harness the hardness of worst-case lattice problems, but it also greatly simplifies key selection.

2. Preliminaries

In this section, some basic definitions are given which are required for understanding the remainder of the paper.

2.1. Notation

We will write $x \leftarrow_{\$} S$ if x is sampled uniformly from a finite set S. We denote the uniform distribution over the set S by Unif(S). In general, if D is an arbitrary probability distribution, we write $x \leftarrow_{\$} D$ to denote that x is sampled from D. Sampling can be made deterministic by specifying the randomness ρ that will be used. We denote this by $x \leftarrow_{\rho} D$, where $\rho \in \{0,1\}^*$. We will denote vectors in n dimensional space with bold, italic, lower-case letters. Matrices are denoted by bold, straight, upper-case letters. If $\mathbf{A}$ is an $m \times n$ matrix, we denote its *transpose* by $\mathbf{A}^T$.

Throughout this paper, λ will be used to denote the main security parameter. In order to formally define blind signatures, we adopt the following notation from (Fischlin and Schröder, 2009). Let $\mathtt{X}$ and $\mathtt{Y}$ be two algorithms. We denote by $(a, b) \leftarrow \langle \mathtt{X}(x), \mathtt{Y}(y) \rangle$, the joint execution of $\mathtt{X}$ and $\mathtt{Y}$ in an interactive way with private inputs x and y, respectively. The respective private outputs are a for $\mathtt{X}$ and b for $\mathtt{Y}$. If $\mathtt{A}$ is a probabilistic algorithm, we will write $y \leftarrow_{\$} \mathtt{A}$ to

denote that the output of A is assigned to y, and that A is running with randomly chosen coins. All logarithms are considered to be base 2. A positive function $f(\lambda)$ is called *negligible* in λ if for any polynomial $p(\lambda)$, there exists a $\lambda_0 \in \mathbb{N}$, such that $f(\lambda) \leq 1/p(\lambda)$, $\forall \lambda \geq \lambda_0$. A positive function $f(\lambda)$ is called *noticeable* (or *non-negligible*), if there exists a positive polynomial $p(\lambda)$ and a $\lambda_0 \in \mathbb{N}$, such that $f(\lambda) \geq 1/p(\lambda)$, $\forall \lambda \geq \lambda_0$. A function $f(\lambda)$ is called *overwhelming* if $1 - f(\lambda)$ is negligible. By $[n]$ we denote the set $\{1, \ldots, n\}$, where $n \in \mathbb{N}$. An algorithm is considered *efficient* if it runs in probabilistic polynomial time (PPT). For asymptotics, we assume the standard Landau notation (Cormen et al., 2009).

2.2. Linear Hash Function Families

A *linear hash function family* LHF is a tuple of algorithms (PGen, F). On input the security parameter, the randomized algorithm PGen returns some parameters par, which implicitly define sets: $S = S(\mathsf{par})$, $\mathbb{D} = \mathbb{D}(\mathsf{par})$ and $R = R(\mathsf{par})$, where S is a set of scalars and $\mathbb{D}$ and R form modules over S. Implicitly, par defines filter sets:

$S_{xxx} \subseteq S$ $(xxx \in \{\beta, c, c'\})$ and $\mathbb{D}_{yyy} \subseteq \mathbb{D}$ $(yyy \in \{sk, r, s, s', \alpha\})$

If the linear hash function family has perfect correctness (Hauck et al., 2019), then the filter sets are trivial, i.e., $S_{xxx} = S$ and $\mathbb{D}_{yyy} = \mathbb{D}$. Algorithm F(par, ·) implements a mapping from $\mathbb{D}$ to R. F(·) is a module homomorphism, meaning that for any $x, y \in \mathbb{D}$ and $s \in S$: $\mathsf{F}(s \cdot x + y) = s \cdot \mathsf{F}(x) + \mathsf{F}(y)$. The main security property for a linear function family is finding a non-trivial collision x_1 , x_2 in some appropriately defined subset $\mathbb{D}'$ of its domain $\mathbb{D}$ with the properties $\mathsf{F}(x_1) = \mathsf{F}(x_2)$.

Definition 1. Let LHF be a linear function family. LHF = (PGen, F) is said to be (ε, t)-collision resistant if for all adversaries A running in time at most t , it can come up with a pair x_1, x_2 in F's domain, s.t. $x_1 \neq x_2$ and $\mathsf{F}(x_1) = \mathsf{F}(x_2)$ with probability at most ε.

2.3. Merkle Trees

Let $\mathsf{G}:\{0,1\}^* \to \{0,1\}^{2\lambda}$ be a collision-resistant hash function. Given a set of values $v_o, \ldots, v_{l-1}$, a *Merkle tree* is constructed as follows: the leaves of the tree are simply the hashes of v_i under G. Every inner node y is constructed via y:= G(left child, right child). Using this construction, the values of all inner nodes are fully determined by the leaf nodes. The entire list of values is thus represented *by a single hash*. To prove the inclusion of a leaf node in a Merkle

tree, we use an *authentication path* which consists of the siblings of the nodes on the path from the bottom to the root of the tree. If v is indeed included in the tree and auth is an authentication path for v, then the verifier should obtain the tree's root node root by calculating successive parent nodes. The algorithms HashTree, BuildAuth, and RootCalc associated for a collision-resistant hash function G are described in Table 1. Algorithm HashTree takes as input a list of values $v_o, \ldots, v_{l-1}$ and returns a sequence of tree nodes, spanning the tree, along with the root of the tree. Algorithm BuildAuth takes as input an index, as well as a tree and outputs an authentication path auth. Finally, algorithm RootCalc takes as input a node and an authentication path auth and returns the root of a hash tree. Note that for all nodes $(v_o, \ldots, v_{l-1})$ and for all indices $i \in [l]$, we have RootCalc(v_i, auth) = root, where (root, tree) ← HashTree($v_o, \ldots, v_{l-1}$) and auth ← BuildAuth(I, tree).

2.4. Zero-Knowledge Proofs of Knowledge

Zero-Knowledge Proofs of Knowledge (ZKPoK) are a method by which one party (called *prover*) can prove to another party (called *verifier*) that a given statement is true, without revealing any information apart from the fact that the statement is indeed true. A zero-knowledge proof must satisfy three properties:

Table 1: Description of algorithms HashTree, BuildAuth, and RootCalc associated to collision-resistant hash function G

Algorithm HashTree($v_0, \ldots, v_{l-1}$):	**Algorithm BuildAuth(I, tree):**	**Algorithm RootCalc(v, auth):**

$h \leftarrow \lceil \log(l) \rceil$
for $j \in \{0, \ldots, l-1\}$:
$t_j^{(0)} \leftarrow \mathsf{G}(v_j)$
for $i \in [h]$:
for $j \in \{0, \ldots, 2^{h-i}-1\}$:
$t_j^{(i)} \leftarrow \mathsf{G}(t_{2j}^{(i-1)}, t_{2j+1}^{(i-1)})$
root $\leftarrow t_0^{(h)}$
tree $\leftarrow \left(t_0^{(1)}, \ldots, t_{2^{h-1}-1}^{(h)}\right)$
return (root, tree)
	$(t_0^{(1)}, \ldots, t_{2^{h-1}-1}^{(h)}) \leftarrow$ tree
	for $i \in \{0, \ldots, h-1\}$:
	$s \leftarrow \lfloor I/2^i \rfloor$
	$b \leftarrow s \pmod 2$
	if $b = 1$:
	$a_i \leftarrow t_{s-1}$
	else:
	$a_i \leftarrow t_{s+1}$
	auth $\leftarrow (I, a_0, \ldots, a_{h-1})$
	return auth
		$(I, a_0, \ldots, a_{h-1}) \leftarrow$ auth
		$b_0 \leftarrow \mathsf{G}(v)$
		for $i \in [h]$:
		$s \leftarrow \lfloor I/2^{i-1} \rfloor$
		$b \leftarrow s \pmod 2$
		if $b = 1$:
		$b_i \leftarrow \mathsf{G}(a_{i-1}, b_{i-1})$
		else:
		$b_i \leftarrow \mathsf{G}(b_{i-1}, a_{i-1})$
		return root$:= b_h$

- **Correctness**: if the statement is true, an honest verifier is always convinced of this fact by an honest prover.
- **Soundness**: if the statement is false, no cheating prover can convince an honest verifier that it is true, except with some small probability.
- **Zero-knowledge**: if the statement is true, no verifier learns anything other than the fact.

2.5. Homomorphic Encryption

A homomorphic encryption (HE) scheme is an encryption scheme that permits computations to be performed on encrypted data (i.e., decrypting is not required before performing the computations).

Definition 2. (Homomorphic Encryption Scheme) A homomorphic encryption scheme is a tuple of probabilistic polynomial time (PPT) algorithms HE = (HE.KeyGen, HE.Enc, HE.Eval, HE.Dec) defined as follows:

- HE.KeyGen(1^λ, 1^d): On input security parameter λ and a depth bound d, the algorithm outputs a pair of keys (sk, pk).
- HE.Enc(pk, msg): On input a public key pk and a plaintext message $msg \in \{0,1\}$, the encryption algorithm outputs a ciphertext ct.
- HE.Eval(pk, C, $ct_1, \ldots, ct_k$): On input a public key pk, a circuit $C: \{0,1\}^k \to \{0,1\}$ of depth at most d, and a tuple of ciphertexts $(ct_1, \ldots, ct_k)$, the evaluation algorithm outputs an evaluated ciphertext ct^*.
- HE.Dec(pk, sk, ct^*): On input a public key pk, a secret key sk and a ciphertext ct^*, the decryption algorithm outputs a message $msg^* \in \{0,1\}$ or $\perp$ (indicating failure).

Definition 3. (Correctness) An HE scheme is *correct* if for all λ, depth bound d, circuit $C: \{0,1\}^k \to \{0,1\}$ of depth at most d, and $msg_i \in \{0,1\}$ for $i \in [k]$, the following holds: for (sk, pk) $\leftarrow_\$$HE.KeyGen(1^λ, 1^d), $ct_i \leftarrow$ HE.Enc(pk, msg_i) for $i \in [k]$, $ct^* \leftarrow$ HE.Eval(pk, C, $ct_1, \ldots, ct_k$), we have Pr[HE.Dec(pk, sk,ct^*) = $C(msg_1, \ldots msg_k)$] = $1 - \lambda - \omega(1)$.

Definition 4. (Security) We say that an HE scheme is *secure* if for all λ and depth bound d, the following holds: for any adversary A with run-time $2^{o(\lambda)}$, the following experiment outputs 1 with probability $2 - \Omega(\lambda)$:

1. On input the security parameter λ and a depth bound d, the challenger runs (sk, pk) $\leftarrow_\$$HE.KeyGen(1^λ, 1^d) and $ct \leftarrow$ HE.Enc(pk, b) for $b \leftarrow_\$ \{0,1\}$. It sends (sk, pk) to A.

2. A outputs a guess b'. The experiment outputs 1 iff $b' = b$. Otherwise, it outputs 0.

Definition 5. (Circuit Privacy) An homomorphic encryption scheme HE is

semi-honest circuit private if for (sk, pk) ← HE.KeyGen(1^λ, 1^d), any circuit C: $\{0,1\}^k \to \{0,1\}$ of depth at most d, $msg_i \in \{0,1\}$ for $i \in [k]$, and $ct_i \leftarrow$ HE.Enc(pk, msg_i) for $i \in [k]$, the statistical distance between the distributions (HE.Eval(pk, C, $\{ct_i\}_{i\leq k}$), $\{ct_i\}_{i\leq k}$, pk, sk) and (HE.Eval(pk, C^0,$\{ct'_i\}_{i\leq k}$), $\{ct'_i\}_{i\leq k}$, pk, sk) is $2^{-\Omega(\lambda)}$, where $\{ct'_1\}$ = HE.Enc(pk, C($msg_1, \ldots, msg_k$)), ct'_i = HE.Enc(pk, 0) for $i \in \{2, \ldots, k\}$ and C^0: $\{0,1\}^k \to \{0,1\}$ is the circuit of depth d that simply outputs its first input (and ignores the rest).

If the above hold even for keys (sk, pk) and ciphertexts ct_i for $i \in [k]$ that were not generated honestly, then we say that the HE scheme is *maliciously circuit private*.

2.6. Blind Signature Schemes

In this section, we recall the syntax and security of blind signature schemes from (Chaum, 1983; Juels et al., 1997). A blind signature scheme is a tuple of algorithms (KeyGen, Sign =⟨S, U⟩, Ver), where Sign is an interactive protocol executed between a signer S and a user U. Their specification is the following:

- KeyGen is a probabilistic polynomial time (PPT) algorithm. On input a security parameter n, it outputs a key pair (sk, pk), where sk is the secret key and pk is the corresponding public key.
- Sign = ⟨S, U⟩ is an interactive and PPT two-party protocol between a signer S (who issues the signature), and a user U (requesting the signature) with a public key pk as common input. The private input of S is a private key sk, and the private input of U is a message msg. At the end of the protocol, U either obtains a valid signature σ as a private output or ⊥ in case the protocol fails.
- Ver is a deterministic polynomial time algorithm. On input a message msg, a public key pk, and a purported signature σ, it determines whether σ is a valid signature on msg with respect to public key pk. If it is valid, the algorithm outputs 1. Otherwise, it outputs 0.

According to (Juels et al., 1997), a secure blind signature scheme must satisfy the following three properties:[1]

- **Correctness**: If both the signer and the user comply with the signing protocol, then the produced blind signature is accepted as a valid signature by the verification algorithm except with probability p which denotes the scheme's correctness error. If p is 0, we say that the scheme has *perfect correctness*. Similarly, if p is negligible, we say that the scheme is *statistically correct*.
- **Blindness**: A signer S that issues signatures on two messages (msg_0, msg_1) of its

own choice to a user U, cannot determine the order in which it issues them. In particular, after interacting with two user sessions holding messages msg_b and msg_{1-b}, respectively (where $b \leftarrow_{\$} \{0,1\}$), S is given both resulting signatures $(\sigma_0,\ \sigma_1)$ (if either signing session fails to produce a signature, the signer is given $(\perp, \perp)$). The signer also gets to keep the transcripts of both sessions with U. The signer wins if it can correctly guess b with probability p s.t. $|p - 1/2|$ is noticeable. If $|p - 1/2|$ is 0, the scheme is called *perfectly blind*. If $|p\ -\ 1/2|$ is negligible, the scheme is called *statistically blind*. In this notion of blindness, the signer behaves "honestly" in the sense that it generates its keys using the blind signature scheme's key generation algorithm. A stronger "malicious" signer model was proposed in (Fischlin, 2006) in which the signer gets to choose its own keys.

- **Unforgeability**: One-more unforgeability ensures that an adversarial user is unable to produce even a single signature *without* interacting with the honest signer. In particular, if k interactions with the signer take place, then the user has to come up with at least $k + 1$ valid message-signature pairs (msg_i, σ_i), $i \in [k + 1]$ in order to win. Furthermore, all output messages need to be pairwise distinct. It should be noted that this definition for unforgeability *is not* meaningful for blind signature schemes with noticeable correctness error (i.e., schemes in which either party may abort with noticeable probability). If all pairs (msg_i, σ_i), $i \in [k + 1]$ are pairwise distinct, the blind signature scheme is said to be *strongly one-more unforgeable*.

2.7. Lattices

Lattices are sets of points in n-dimensional space with a periodic structure. A lattice is most easily described as the set of all *integer* linear combinations $\Lambda = \{\sum_{i=1}^{m} \mathrm{x}_i \boldsymbol{b}_i : x_i \in \mathbb{Z}\}$ of m linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{R}^n$. These vectors are called a *basis* for the lattice Λ and are often represented as a matrix $\mathbf{B} = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m] \in \mathbb{R}^{n \times m}$. We will write $\Lambda = \Lambda(\mathbf{B})$ to express this fact. We say that the *rank* of the lattice is m and its *dimension* is n. If $m = n$, the lattice is called *full-rank*.

Consider the quotient rings $R \coloneqq \mathbb{Z}[x]/\langle x^n + 1\rangle$ and $R_q \coloneqq \mathbb{Z}_q[x]/\langle x^n + 1\rangle$, where $n = 2^\kappa$, for some $\kappa \in \mathbb{N}$ and q is an odd prime number. Polynomials in R_q are of degree strictly less than n and have zero-centered coefficients, i.e., from the set $\{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\}$. For such coefficients, we abuse the notation mod to denote with $x = x' \pmod q$, the unique element x' s.t. for any integer k: $x' = kq\ +\ x$ and $x' \in \{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\}$. It is not hard to see that R_q^m is isomorphic to $\mathbb{Z}_q^{mn}$, $\forall m \in \mathbb{N}$, with vector addition corresponding to

polynomial addition, and matrix-vector multiplication corresponding to the convolution product $\sum_{i=1}^{m} \boldsymbol{a}_i \boldsymbol{b}_i$ (modulo $x^n + 1$ and q) of polynomials in R. We will thus identify any polynomial $\boldsymbol{x} \in R_q$ with its coefficient vector $\boldsymbol{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{Z}_q^n$ (i.e., we will treat polynomials of R_q and vectors of $\mathbb{Z}_q^n$ as equivalent). This is called *coefficient embedding*. Thus, polynomials in R_q will also be denoted by bold, lower-case, italic letters. Vectors of such polynomials are denoted with a hat. As such, we measure the size of an element $\boldsymbol{x} = x_0 + x_1 x + \ldots + x_{n-1} x^{n-1} \in R_q$ through its l_∞ norm$\|\boldsymbol{x}\|_\infty \coloneqq \max_i |x_i \pmod q|$. In rings R andR_q, $\|\boldsymbol{x}\|_\infty$ represents $|x_i|$ and $|x_i \pmod q|$, respectively. Similarly, for $\widehat{\boldsymbol{x}} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m)$, we define the l_∞ norm as $\|\boldsymbol{x}\|_\infty \coloneqq \max_i \|\boldsymbol{x}_i\|_\infty$. Furthermore, we define $\|\boldsymbol{x}\|_1 \coloneqq \sum_{i=1}^{n} |x_i|$ and $\|\boldsymbol{x}\|_2 \coloneqq (\sum_{i=1}^{n} |x_i|^2)^{1/2}$. For vectors of polynomials $\widehat{\boldsymbol{x}} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m)$,, $\widehat{\boldsymbol{y}} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m) \in R_q$, we define their *convolution product* as $\widehat{\boldsymbol{x}} \cdot \widehat{\boldsymbol{y}} \coloneqq \sum_{i=1}^{m} \boldsymbol{x}_i \boldsymbol{y}_i$, where the resulting polynomial is reduced *both*modulo q, and modulo $x^n + 1$. A lattice corresponds to an ideal $I \subset R_q$ iff every vector in it is the coefficient vector of some polynomial $\boldsymbol{f} \in I$. These structured lattices are called *ideal lattices* and will be our focus for this work.

2.7.1. Gaussian Distribution

For any vector $\boldsymbol{c} \in \mathbb{R}^n$ and any real $s > 0$, the Gaussian function with standard deviation s and center $\boldsymbol{c}$ is defined as $\rho_{s,\boldsymbol{c}}(\boldsymbol{x}) \coloneqq exp(-\pi \|\boldsymbol{x} - \boldsymbol{c}\|^2 / s^2)$, $\forall \boldsymbol{x} \in \mathbb{R}^n$. The Gaussian distribution is defined as $D_{s,\boldsymbol{c}}(\boldsymbol{x}) \coloneqq \rho_{s,\boldsymbol{c}}(\boldsymbol{x}) / s^n$, $\forall \boldsymbol{x} \in \mathbb{R}^n$. The discrete Gaussian distribution over a lattice $\Lambda \subseteq \mathbb{R}^n$, with standard deviation $s > 0$ and center $\boldsymbol{c}$ is defined as $D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x}) = \rho_{s,\boldsymbol{c}}(\boldsymbol{x}) / \sum_{\boldsymbol{v} \in \Lambda} \rho_{s,\boldsymbol{c}}(\boldsymbol{v})$, $\forall \boldsymbol{x} \in \Lambda$. We omit the subscript when $\boldsymbol{c} = \boldsymbol{0}$.

2.7.2. Hardness Assumptions

We first recall the (Ring) Short Integer Solution problem ($\mathrm{R-SIS}_{p,q,n,m,d}$) over R_q (Lyubashevsky and Micciancio, 2006; Peikert and Rosen, 2006) whose conjectured hardness is the basis for the security proofs of most proposed lattice-based constructions in the literature. The R−SIS problem asks, given many uniformly random elements of a certain large finite additive group, to find a sufficiently "short" nontrivial integer combination of them that sums to zero. More formally, we have the following definition:

Definition 6. (Ring Short Integer Solution ($\mathrm{R-SIS}_{p,q,n,m,d}$)) Given a uniform vector of polynomials $\widehat{\boldsymbol{a}} \leftarrow_{\$} R_q^m$, find a vector $\widehat{\boldsymbol{x}} \in R_q^m$, s.t. $\sum_{i=1}^{m} \boldsymbol{a}_i \boldsymbol{x}_i = 0 \pmod q$ and $0 < \|\widehat{\boldsymbol{x}}\|_p \leq d$. We call $\mathrm{F}(\widehat{\boldsymbol{x}}) \coloneqq \sum_{i=1}^{m} \boldsymbol{a}_i \boldsymbol{x}_i \pmod q$ the Ring SIS hash function.

A variant of SIS called the Ring k−SIS problem was introduced in (Boneh and Freeman, 2011a).

Definition 7. (Ring $k - \mathrm{SIS}_{p,q,m,\beta}$) For any integer $k \geq 0$, given a vector $\widehat{\boldsymbol{a}} \in R^m$

and a set of k short polynomial vectors $\hat{\boldsymbol{e}}_1, \dots, \hat{\boldsymbol{e}}_k$ s.t. $\hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{e}}_k = 0 \pmod{q}$, $\forall i \in [k]$, find a non-zero polynomial vector $\hat{\boldsymbol{v}} \in R^m$ s.t. $\|\hat{\boldsymbol{v}}\|_p \leq \beta$, $\hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{v}} = 0 \pmod{q}$, and $\hat{\boldsymbol{v}} \in R \backslash \mathrm{span}(\hat{\boldsymbol{e}}_1, \dots, \hat{\boldsymbol{e}}_k)$.

Finally, we recall the Ring Learning With Errors (LWE) problem, which is known to be at least as hard as other standard lattice problems in the worst case (Langlois and Stehle, 2015).

Definition 8. (Ring Learning With Errors ($\mathrm{R-LWE}_{q,\alpha,m}$)) Let q, α, m be functions of a parameter n and $B \in \mathbb{N}$. For a secret polynomial $\boldsymbol{s} \in R_q$ s.t. $\|\boldsymbol{s}\|_\infty \leq B$, the distribution $A_{q,\alpha,\boldsymbol{s}}$ over $R_q \times \mathbb{Z}$ is obtained by sampling $\boldsymbol{a} \leftarrow_\$ R_q$ and an $e \leftarrow_\$ D_{\mathbb{Z},\alpha q}$, and returning $(\boldsymbol{a}, \boldsymbol{a} \cdot \boldsymbol{s} + e) \in R_q \times \mathbb{Z}$. The (decisional) Ring Learning With Errors problem $\mathrm{R-LWE}_{q,\alpha,m}$ is as follows: for $\boldsymbol{s} \leftarrow_\$ \{-B, \dots, B\}^n \subset R_q$, the goal is to distinguish between the distributions:

$D_0(\boldsymbol{s}) := \mathsf{Unif}(\mathbb{Z}_q^{m \times (n+1)})$ and $D_1(\boldsymbol{s}) := \left(A_{q,\alpha,\boldsymbol{s}}\right)^m$.

3. Flawed Lattice-Based Blind Signature Schemes

In this section we describe a number of blind signature schemes in the literature, whose design has been shown to be flawed in one way or another. While their security is flawed (Hauck et al., 2020), we include them for completeness and because they each introduce new ideas that could potentially lead to either a revised security model for blind signatures, or to new more efficient blind signature schemes.

3.1. Rückert's Blind Signature Scheme

The first attempt towards constructing blind signature schemes from lattice-based assumptions was made in 2008 in the seminal work of M. Rückert (Rückert, 2010). Following a well-known pattern[2] found in many number-theoretic blind signatures (Okamoto, 1992; Pointcheval and Stern, 1996; Pointcheval and Stern, 1997; Schnorr, 1989; Pointcheval, 1998), (Rückert, 2010) uses Lyubashevsky's identification scheme (Lyubashevsky, 2009) as its basis (which itself relies on the SIS hash function) to construct a Fiat-Shamir-like blind signature scheme. However, because of a technique known as rejection sampling (which stems from the underlying hash function's enclosedness errors (Hauck et al., 2020)), there is no guarantee that any given protocol run will actually produce a valid blind signature for the user. The novelty introduced in (Rückert, 2010) to resolve this issue is to extend the standard 3-move protocol structure with an additional move, in which a user can prove to the signer that he failed to obtain a valid signature (when unblinding).

3.1.1. Construction

We now describe Rückert's blind signature scheme in detail. The parameter definitions are summarized in Table 2. The construction makes use of the following cryptographic components:

- the SIS linear hash function family $F(\hat{\boldsymbol{x}}) := \sum_{i=1}^{m} \boldsymbol{u}_i \boldsymbol{x}_i \pmod{q}$, $\hat{\boldsymbol{x}} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) \in R_q^m$, where $\hat{\boldsymbol{u}} \leftarrow_{\$} R_q^m$.
- a hash function $H: \{0,1\}^* \rightarrow R_q$ (modelled as a programmable random oracle),

Table 2: Parameter definitions for Ruckert's lattice-based blind signature scheme.

Parameter	Definition and Constraints
n	Main security parameter, integer power of 2
d_{sk}	Positive integer $< q/(4n)$
$\mathbb{D}_{sk}$	$\{\boldsymbol{v} \in R_q: \|\boldsymbol{v}\|_\infty \leq d_{sk}\}$
m	Positive integer $> \lfloor \log(q)/\log(2d_{sk}) \rfloor + 1$
$S_{c'}$	Challenge space $\{\boldsymbol{v} \in R_q: \|\boldsymbol{v}\|_\infty \leq d_{c'} := 1\}$
u, v	Positive integer constants ≥ 1
S_b	$\{\boldsymbol{v} \in R_q: \|\boldsymbol{v}\|_\infty \leq d_b := und_{c'}\}$
S_c	$\{\boldsymbol{v} \in R_q: \|\boldsymbol{v}\|_\infty \leq d_c := d_b - d_{c'}\}$
$\mathbb{D}_r$	$\{\boldsymbol{v} \in R_q: \|\boldsymbol{v}\|_\infty \leq d_r := vmn^2 d_{sk} d_c\}$
$\mathbb{D}_s$	$\{\boldsymbol{v} \in R_q: \|\boldsymbol{v}\|_\infty \leq d_s := d_r - nd_{sk} d_c\}$
$\mathbb{D}_a$	$\{\boldsymbol{v} \in R_q: \|\boldsymbol{v}\|_\infty \leq d_a := vmnd_s\}$
$\mathbb{D}_{s'}$	$\{\boldsymbol{v} \in R_q: \|\boldsymbol{v}\|_\infty \leq d_{s'} := d_a - d_s\}$
$\mathbb{D}$	$\{\boldsymbol{v} \in R_q: \|\boldsymbol{v}\|_\infty \leq d := d_s + d_a + nd_{sk} d_{c'}\}$
q	Prime s.t. $\geq 4dmn\sqrt{n}\log(n)$

- a statistically hiding, and computationally binding commitment function com: $\{0,1\}^* \times \{0,1\}^n \to \{0,1\}^n$.

Key Generation. On input the main security parameter n, the algorithm selects parameters as specified in Table 2.[3] KeyGen(1^n) samples polynomials $\hat{\boldsymbol{u}} \leftarrow_\$ R_q^m$ defining the homomorphic hash function F and $\hat{\boldsymbol{z}} \leftarrow_\$ \mathbb{D}_{sk}^m$. Finally, it sets sk :=$\hat{\boldsymbol{z}}$, and pk := F($\hat{\boldsymbol{z}}$), and returns (sk, pk).

Signing. The interactive signing protocol < S(sk), U(pk, msg)> works as follows:

1. **Signer**: At the outset, the signer samples a masking vector $\hat{\boldsymbol{r}} \leftarrow_\$ \mathbb{D}_r$ and computes a commitment $\boldsymbol{R}$: =F($\hat{\boldsymbol{r}}$). It sends $\boldsymbol{R}$ to the user.

2. **User**: The user receives $\boldsymbol{R}$ and samples its masking parameters $\hat{\boldsymbol{a}} \leftarrow_\$ \mathbb{D}_a^m$ and $\boldsymbol{b} \leftarrow_\$ S_b$. It samples randomness $\rho \leftarrow_\$ \{0,1\}^n$ and uses it to commit to the message-to-be-signed by computing $C \coloneqq \mathrm{com}(msg, \rho)$. It computes a "masked commitment" $\boldsymbol{R}' \coloneqq \boldsymbol{R} + \mathsf{F}(\hat{\boldsymbol{a}}) + \boldsymbol{b} \cdot \mathsf{pk}$ as well as its challenge $\boldsymbol{c}' \coloneqq \mathsf{H}(\boldsymbol{R}', C)$. Because $\boldsymbol{c}'$ will be part of the produced signature, it cannot be sent in the clear. The user "blinds" $\boldsymbol{c}'$ as $\boldsymbol{c} \coloneqq \boldsymbol{c}' + \boldsymbol{b}$. If $\boldsymbol{c} \notin S_c$ then $\boldsymbol{c}'$ "leaks" information about $\boldsymbol{c}$. Hence, to maintain anonymity, the user only sends $\boldsymbol{c}$ if it falls within S_c and repeats the entirety of step 2 from scratch otherwise. This rejection sampling step can be performed locally by the user without affecting the scheme's correctness.

3. **Signer**: Upon receiving $\boldsymbol{c}$, the signer computes its response $\hat{\boldsymbol{s}} \coloneqq \hat{\boldsymbol{r}} + \boldsymbol{c} \cdot \mathsf{sk}$. To make $\hat{\boldsymbol{s}}$ independent of the secret key, the signer rejection-samples it and only sends it to the user if $\hat{\boldsymbol{s}} \in \mathbb{D}_s^m$. Otherwise, the entire protocol restarts. This introduces an expected amount of correctness error of $1 - e^{-1/v}$ to the blind signature scheme.

4. **User**: Upon receiving $\hat{\boldsymbol{s}}$, the user checks if $\mathsf{F}(\hat{\boldsymbol{s}}) \neq \boldsymbol{c} \cdot \mathsf{pk} + \boldsymbol{R}$ and $\hat{\boldsymbol{s}} \notin \mathbb{D}_s^m$. If either condition fails, then the signer sent invalid data, and the user can trivially request a protocol restart. Otherwise, the user "unblinds" the response $\hat{\boldsymbol{s}}$ by computing $\hat{\boldsymbol{s}}' \coloneqq \hat{\boldsymbol{s}} + \hat{\boldsymbol{a}}$. A final rejection sampling step is necessary here in order to make $\hat{\boldsymbol{s}}'$ independent from $\hat{\boldsymbol{s}}$. Hence, the user outputs $(\boldsymbol{c}', \hat{\boldsymbol{s}}', \rho)$ iff $\hat{\boldsymbol{s}}' \in \mathbb{D}_{s'}^m$. Otherwise, the user reveals the blinding parameters $\hat{\boldsymbol{a}}$, $\boldsymbol{b}$, the challenge $\boldsymbol{c}'$ and the commitment to the message C (the user only withholds the decommitment parameter ρ to avoid having to reveal msg) to the signer and requests a restart. Notice that rejection sampling during this step further amplifies the blind signature scheme's correctness error by an additional factor of $1 - e^{-1/v}$.

5. **Signer**: The signer receives $\hat{\boldsymbol{a}}$, $\boldsymbol{b}$, the challenge $\boldsymbol{c}'$ and the commitment to the message C. These allow the signer to trace all computations performed on the user's side and ascertain if a restart is truly necessary. To this end, it computes the blinded commitment $\boldsymbol{R}' \coloneqq \boldsymbol{R} + \mathsf{F}(\hat{\boldsymbol{a}}) + \boldsymbol{b} \cdot \mathsf{pk}$, as well as $\boldsymbol{c}_1^*$: =H($\boldsymbol{R}'$, C) and

$\boldsymbol{c}_2^*$: =H(F($\hat{\boldsymbol{s}} + \hat{\boldsymbol{a}}$)−$\boldsymbol{c}'$ ·pk, C). If $\hat{\boldsymbol{s}} \in \mathbb{D}_s^m$, $\boldsymbol{c} - \boldsymbol{b} = \boldsymbol{c}'$, $\boldsymbol{c}' = \boldsymbol{c}_1^* = \boldsymbol{c}_2^*$, and $\hat{\boldsymbol{s}} + \hat{\boldsymbol{a}} \notin \mathbb{D}_{s'}^m$, the signer restarts the entire protocol. Otherwise, the user attempts to cheat by submitting an invalid "proof" and the signer simply dismisses the request.

Verification. On input public key pk, a purported signature $(\boldsymbol{c}', \hat{\boldsymbol{s}}', \rho)$ and message msg, algorithm Ver(pk,$(\boldsymbol{c}', \hat{\boldsymbol{s}}', \rho)$, msg) outputs 1 iff $\hat{\boldsymbol{s}}' \in \mathbb{D}_{s'}^m$ and H(F($\hat{\boldsymbol{s}}'$)−pk· $\boldsymbol{c}'$, com(msg, ρ)) = $\boldsymbol{c}'$. Otherwise, it outputs 0.

3.1.2. Claimed Security Results

While rejection-sampling can be used for tailoring the distributions of messages exchanged during the signing protocol, it comes at the cost of introducing a noticeable correctness error to the scheme:

Lemma 1. (Adapted from Theorem 3.3. of (Rückert, 2010)) The above blind signature scheme has a correctness error of $(1 - e - 1/v)^2$.

Moreover, because of its reliance on a commitment scheme, the construction of(Rückert, 2010) is only as blind as com is hiding.

Lemma 2. (Adapted from Theorem 3.5. of (Rückert, 2010)) If com is a statistically hiding commitment function, then the above blind signature scheme is statistically blind.

Finally, unforgeability relies on the collision resistance of the R−SIS hash function family, as well as the binding property of com:

Lemma 3. (Adapted from Theorem 3.8. of (Rückert, 2010)) If com is a computationally binding commitment function and the R-SIS hash function family is collision-resistant in $\mathbb{D}$, then the above blind signature scheme is one-more unforgeable.

3.2. BLAZE

BLAZE (Alkadri et al., 2020a) is a blind signature scheme, structurally similar to (Rückert, 2010). The signing protocol relies on rejection sampling with discrete Gaussian samples, instead of uniform, which allows for smaller key and signature sizes. Furthermore, the notion of signed permutations is introduced, which allows the scheme to avoid having to rejection-sample the challenge part of the signature (when unblinding), thus achieving a smaller correctness error.

Definition 9. (Adapted from (Alkadri, 2020a)) For the ring R_q, we define the set of signed permutation monomials as $\mathbb{S} := \{(-1)^s x_i : s \in \{0,1\}, 0 \leq i \leq n-1\}$.

In (Alkadri et al., 2020a), the authors prove that $\mathbb{S}$ forms a group under multiplication in R_q. Furthermore, if we define the challenge space $\mathbb{S}_\kappa^n$ as the set $\{\boldsymbol{v} \in R_q : \|\boldsymbol{v}\|_1 = \kappa, \|\boldsymbol{v}\|_\infty \leq 1\}$, then any polynomial $\boldsymbol{c} \in \mathbb{S}_\kappa^n$ can be partitioned

into a set of partitioning monomials $\{c_1, \dots, c_\kappa\}$ s.t. $\boldsymbol{c} = \sum_{j=1}^{\kappa} c_j$ where ^{c_j} contains exactly the j-th non-zero entry of $\boldsymbol{c}$ at the exact same position. Additionally, the following lemma shows that signed permutations can be used to (individually) mask each partitioning monomial. Consequently, this lemma is used within BLAZE to completely eliminate any protocol restarts due to the user's inability to unblind the challenge part of its signature.

Algorithm 1: Rejection_Sample$(\hat{\boldsymbol{z}}, \hat{\boldsymbol{c}}, \varphi, T; \rho)$	
01: $\sigma \coloneqq \varphi T; M(\varphi) \coloneqq e^{\frac{12}{\varphi} + \frac{1}{(2\varphi)^2}}$;	
02: if $\rho = \perp$ then:	
03: $u \leftarrow_{\$} [0, 1)$;	// Sample uniformly
04: else:	
05: $u \leftarrow_{\rho} [0, 1)$;	// Sample with fixed randomness
06: if $u \leq \frac{1}{M(\varphi)} e^{\left(\frac{-2\hat{\boldsymbol{z}} \cdot \hat{\boldsymbol{c}} + \|\hat{\boldsymbol{c}}\|^2}{2\sigma^2}\right)}$ then:	
07: return 1;	// Accept sample
08: return 0;	// Reject sample

Lemma 4. (Adapted from (Alkadri, 2020a)) Let $\boldsymbol{c} \in \mathbb{S}_\kappa^n$ be a polynomial and $\{c_1, \dots, c_\kappa\}$ be its partitioning set. Furthermore, let $p_1, \dots, p_\kappa$ be random signed permutations in $\mathbb{S}$ and $c_j^* := p_j^{-1} \cdot c_j$, $\forall j = 1, \dots, \kappa$. Then, for $c_j, c_j^* \in \mathbb{S}$, the following holds:

$$\Pr_{p_j \leftarrow_{\$} \mathbb{S}}[(c_1^*, \dots, c_\kappa^*) = (p_1^{-1} \cdot c_1, \dots, p_\kappa^{-1} \cdot c_\kappa) \mid \boldsymbol{c}]$$

$$= \Pr_{p_j \leftarrow_{\$} \mathbb{S}, \boldsymbol{c} \leftarrow_{\$} \mathbb{S}_\kappa^n}[(c_1^*, \dots, c_\kappa^*) = (p_1^{-1} \cdot c_1, \dots, p_\kappa^{-1} \cdot c_\kappa)] = \frac{1}{(2n)^\kappa}$$

3.2.1. Construction

We now describe the BLAZE blind signature scheme in detail. BLAZE makes use of the following cryptographic ingredients:

- a public (randomly chosen) deterministic function Expand: $\{0,1\}^\lambda \rightarrow R_q^m$ (instantiated for example with a PRF),
- a hash function H: $\{0,1\}^* \rightarrow \mathbb{S}_\kappa^n$ modelled as a random oracle,
- a statistically hiding and computationally binding commitment function com: $\{0,1\}^* \times \{0,1\}^\lambda \rightarrow \{0,1\}^\lambda$,

- functions Compress and Decompress for compressing (resp. decompressing) integers distributed according to $D_{\mathbb{Z},\sigma}$ (for implementation details cf. Table 3 in (Ducas et al., 2017)).

Algorithm 1 shows how rejection sampling is performed w.r.t. discrete Gaussian samples.

Key Generation. On input the main security parameter λ, algorithm KeyGen(1^λ) sets parameters according to the specifications of Table 3. It then samples a seed $\leftarrow_\$ \{0,1\}^\lambda$ and $\hat{\boldsymbol{z}}_1, \boldsymbol{z}_2 \leftarrow_\$ D^m_{\mathbb{Z}^n,\sigma} \times D_{\mathbb{Z}^n,\sigma}$. It expands the seed to a vector of polynomials by computing $\hat{\boldsymbol{a}} :=$ Expand(seed), and it also computes $\boldsymbol{b} := \hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{z}}_1 + \boldsymbol{z}_2 \pmod q$. It sets sk := $(\hat{\boldsymbol{z}}_1, \boldsymbol{z}_2)$, and pk := (seed, $\boldsymbol{b}$), and returns (sk, pk).

Signing. The interactive signing protocol < S(sk), U(pk, msg)> works as follows:

1. **Signer**: On input secret key sk, as well as seed, the signer samples masking terms $\hat{\boldsymbol{r}}^*_{1,1}, \dots, \hat{\boldsymbol{r}}^*_{\kappa,1} \leftarrow_\$ D^m_{\mathbb{Z}^n,s^*}$ and $\boldsymbol{r}^*_{1,2}, \dots, \boldsymbol{r}^*_{\kappa,2} \leftarrow_\$ D_{\mathbb{Z}^n,s^*}$ and computes commitments $\boldsymbol{R}_j = \hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{r}}^*_{j,1} + \boldsymbol{r}^*_{j,2} \pmod q, \forall j \in [\kappa]$. It sets $\hat{\boldsymbol{R}} := (\boldsymbol{R}_1, \dots, \boldsymbol{R}_\kappa)$, and it sends $\hat{\boldsymbol{R}}$ to the user.

2. **User**: On input seed, and a message $msg \in \{0,1\}^*$, and commitment $\hat{\boldsymbol{R}}$, the user computes $\hat{\boldsymbol{a}}$ = Expand(seed). It samples randomness $r, r', \rho, \rho \leftarrow_\$ \{0,1\}^\lambda$, signed permutations $p_1, \dots, p_\kappa \leftarrow_\$ \mathbb{S}$, and masking terms $(\hat{\boldsymbol{e}}_1, \boldsymbol{e}_2) \leftarrow_\rho D^{m+1}_{\mathbb{Z}^n,s}$ (notice that the random coins are fixed through ρ). It computes commitments $C_1 := \mathrm{com}(msg, r)$ and $C_2 := \mathrm{com}(\rho', r')$ and a challenge $\boldsymbol{c} = \mathsf{H}(\hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{e}}_1 + \boldsymbol{e}_2 + \sum_{j=1}^\kappa p_j \boldsymbol{R}_j, C_1, C_2)$. It partitions $\boldsymbol{c} = \sum_{j=1}^\kappa c_j \in \mathbb{S}^n_\kappa$ and individually blinds each partitioning term via $\boldsymbol{c}^*_j := p_j^{-1} \cdot c_j \in \mathbb{S}$. It sets $\boldsymbol{c}^* := (\boldsymbol{c}^*_1, \dots, \boldsymbol{c}^*_\kappa)$ and sends $\boldsymbol{c}^*$ to the signer.

3. **Signer**: The signer receives $\boldsymbol{c}^*$ and computes its responses with the help of its secret key sk = $(\hat{\boldsymbol{z}}_1, \boldsymbol{z}_2)$. In particular, it computes $\hat{\boldsymbol{s}}^*_{j,1} := \hat{\boldsymbol{r}}^*_{j,1} + \boldsymbol{c}^*_j \hat{\boldsymbol{z}}_1$, $\boldsymbol{s}^*_{j,2} := \boldsymbol{r}^*_{j,2} + \boldsymbol{c}^*_j \boldsymbol{z}_2, \forall j \in [\kappa]$, and sets $\hat{\boldsymbol{s}}^* := (\hat{\boldsymbol{s}}^*_{1,1}, \dots, \boldsymbol{s}^*_{\kappa,2})$, and it rejection-samples $\hat{\boldsymbol{s}}^*$ using Algorithm 1 to ensure that it is independent from sk. In case of rejection (this occurs with probability $(1 - exp(-12/\alpha^* - 1/(2\alpha^{*2}))))$, the entire protocol restarts. Otherwise, it returns $\hat{\boldsymbol{s}}^*$ to the user.

4. **User**: The user receives $\hat{\boldsymbol{s}}^* := (\hat{\boldsymbol{s}}^*_{1,1}, \dots, \boldsymbol{s}^*_{\kappa,2})$ and computes $\hat{\boldsymbol{v}}_1 := \sum_{j=1}^\kappa p_j \hat{\boldsymbol{s}}^*_{j,1}$, $\boldsymbol{v}_2 := \sum_{j=1}^\kappa p_j \boldsymbol{s}^*_{j,2}$. If $\|(\hat{\boldsymbol{v}}_1, \boldsymbol{v}_2)\| > \eta s^* \sqrt{(m+1)\kappa n}$, then the signer submitted an invalid response and the entire protocol must be restarted. Otherwise, it "unblinds" the response via $\hat{\boldsymbol{s}}_1 := \hat{\boldsymbol{v}}_1 + \hat{\boldsymbol{e}}_1$ and $\boldsymbol{s}_2 := \boldsymbol{v}_2 + \boldsymbol{e}_2$. It then invokes Rejection_Sample($(\hat{\boldsymbol{s}}_1, \boldsymbol{s}_2), (\hat{\boldsymbol{v}}_1, \boldsymbol{v}_2); \rho'$) to make $(\hat{\boldsymbol{s}}_1, \boldsymbol{s}_2)$ independent from $(\hat{\boldsymbol{v}}_1, \boldsymbol{v}_2)$. Notice that the user needs to fix the random coins of Algorithm 1 through ρ' to which it committed to earlier in the protocol. If rejection sampling fails (this occurs with probability $(1 - exp(-12/\alpha - 1/(2\alpha^2)))$), the

user sends $(C_1, \rho, \rho', r', p_1, \ldots, p_\kappa, \boldsymbol{c})$ to the signer, requesting a protocol restart. Otherwise, it compresses $(\hat{\boldsymbol{s}}_1, \boldsymbol{s}_2)$ via $(\hat{\boldsymbol{s}}_1, \boldsymbol{s}_2) :=$Compress$(\hat{\boldsymbol{s}}_1, \boldsymbol{s}_2)$ and it outputs $(C_2, r, \hat{\boldsymbol{s}}_1, \boldsymbol{s}_2, \boldsymbol{c})$ as its signature.

5. **Signer**: Upon receiving $(C_1, \rho, \rho', r', p_1, \ldots, p_\kappa, \boldsymbol{c})$, the signer uses ρ to retrieve[4] $\hat{\boldsymbol{e}}_1$, $\boldsymbol{e}_2$ via $(\hat{\boldsymbol{e}}_1, \boldsymbol{e}_2) \leftarrow_\rho D^{m+1}_{\mathbb{Z}^n, s}$. It then computes $C_2 := \mathrm{com}(\rho', r')$, $\hat{\boldsymbol{s}}_1 := \hat{\boldsymbol{e}}_1 + \sum_{j=1}^{\kappa} p_j \hat{\boldsymbol{s}}^*_{j,1}$, $\boldsymbol{s}_2 := \boldsymbol{e}_2 + \sum_{j=1}^{\kappa} p_j \boldsymbol{s}^*_{j,2}$. If $\sum_{j=1}^{\kappa} p_j \boldsymbol{c}^*_j = \boldsymbol{c}$, $\boldsymbol{c} = \mathsf{H}(\hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{e}}_1 + \boldsymbol{e}_2 + \sum_{j=1}^{\kappa} p_j \boldsymbol{R}_j \ (\mathrm{mod} q), C_1, C_2)$, $\boldsymbol{c} = \mathsf{H}(\hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{s}}_1 + \boldsymbol{s}_2 - \boldsymbol{bc} \ (\mathrm{mod} q), C_1, C_2)$, and Rejection Sample $((\hat{\boldsymbol{s}}_1, \boldsymbol{s}_2); \rho') = 0$, the signer is convinced and restarts the protocol. Otherwise, it ignores the request.

Verification. On input public key pk = (seed, $\boldsymbol{b}$), message $msg \in \{0,1\}^*$ and a purported signature $(C_2, r, \hat{\boldsymbol{s}}_1, \boldsymbol{s}_2, \boldsymbol{c})$, the verifier expands the seed to obtain $\hat{\boldsymbol{a}} :=$ Expand(seed), and it decompresses $(\hat{\boldsymbol{s}}_1, \boldsymbol{s}_2)$ using Decompress. If $\|(\hat{\boldsymbol{s}}_1, \boldsymbol{s}_2)\| < \eta s \sqrt{(m+1)n}$ and $\boldsymbol{c} = \mathsf{H}(\hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{s}}_1 + \boldsymbol{s}_2 - \boldsymbol{bc} \ (\mathrm{mod} q), \mathrm{com}(msg, r), C_2)$, it outputs 1 (accept). Otherwise, it outputs 0 (reject).

Table 3: Parameter definitions for the BLAZE blind signature scheme

Parameter	Definition and Constraints
λ	Main security parameter
n	Integer power of 2
m	Number of polynomials in the secret key, s.t. $m + 1 \geq 2$
q	Prime modulus, s.t. $q \equiv 1 \ (\mathrm{mod}\ 2n)$
σ	Standard deviation for the distribution from which the secret key is drawn, s.t. $\sigma > 0$, $(m+1)\log(t\sigma) > \log(q)$
κ	Hamming weight of H's output, s.t. $2^\kappa \binom{n}{\kappa} > 2^\lambda$
s^*	Standard deviation for the distribution from which the signer draws its blinding parameters, s.t. $s^* = a^* \sqrt{\kappa} \|\mathrm{sk}\|$ where $a^* > 0$
s	Standard deviation for the distribution from which the user draws its blinding parameters, s.t. $s = \eta a s^* \sqrt{(m+1)\kappa n} \|\mathrm{sk}\|$ where $a, \eta > 0$, and $\eta^{(m+1)n} e^{\frac{(m+1)n}{2}(1-\eta^2)} \leq 2^{-\lambda}$
M	Expected number of iterations, s.t. $M = e^{\frac{12}{a} + \frac{1}{2a^2} + \frac{12}{a^*} + \frac{1}{2a^{*2}}}$

3.2.2. Claimed Security Results

Thanks to the use of signed permutations, the correctness error that would be induced when unblinding the challenge part of a signature is completely eliminated:

Lemma 5. (Adapted from Theorem 1 of (Alkadri, 2020a)) If the parameters for BLAZE are set according to Table 3, then BLAZE has a correctness error of $(1 - exp(-12/\alpha^* - 1/(2\alpha^{*2}))(1 - exp(-12/\alpha - 1/(2\alpha^2))$.

Lemma 6. (Adapted from Theorem 2 of (Alkadri, 2020a)) If com is a statistically hiding commitment function, then BLAZE is statistically blind.

Similarly to (Rückert, 2010), unforgeability is also conditioned on the binding property of com:

Lemma 7. (Adapted from Theorem 3 of (Alkadri, 2020a)) If com is a statistically hiding and computationally binding commitment function, and R−SIS is hard for the parameters set according to Table 3, then BLAZE is strongly one-more-unforgeable.

3.2.3. Attacks and Countermeasures

BLAZE can be attacked by exploiting a subtle design flaw as hinted in (Hauck et al., 2020). Notice that because a malicious user has complete control over the randomness ρ, it can attack the protocol by rigging ρ so that u (line 5 of Algorithm 1) is always picked very close to 1 (e.g.: $1 - 2^{-128}$), thus causing the Rejection Sample algorithm to always output 0 when the user tries to unblind. This allows the user to keep asking for new signatures until it can produce its own forgery and win in the unforgeability game. One possible countermeasure to this kind of attack would be to switch the distribution from discrete Gaussian to uniform but this would increase key and signature sizes considerably.

3.3. BLAZE+

BLAZE+ (Alkadri et al., 2020) introduces a novel technique for reducing the correctness error by performing multiple rejection samplings in parallel. Instead of sampling a single pair of masking terms $(\hat{\boldsymbol{e}}_1, \boldsymbol{e}_2)$, the user samples multiple such pairs and stores (a function of) each such pair as a leaf of a Merkle tree. This offers the advantage that when the user tries to unblind to produce its signature, it will succeed for at least one of these pairs with very high probability. By tuning the number of sampled pairs to a sufficiently large amount, this probability can effectively be made negligible. The optimizations introduced are backwards compatible with BLAZE.

3.3.1. Three-move Variant of BLAZE+

We now describe the 3-move variant of the BLAZE+ blind signature scheme in detail. This variant makes use of the following cryptographic ingredients:

- a public (randomly chosen) deterministic function Expand: $\{0,1\}^{\lambda} \to R_q^m$ (instantiated for example with a PRF),
- a hash function H: $\{0,1\}^* \to \mathbb{S}_{\kappa}^n$ modelled as a random oracle,
- functions Compress and Decompress for compressing (resp. decompressing) integers distributed according to $D_{\mathbb{Z},\sigma}$.

Key Generation. On input the main security parameter λ, algorithm KeyGen(1^{λ}) samples a seed $\leftarrow_{\$} \{0,1\}^{\lambda}$ and $\hat{\boldsymbol{z}} := (\hat{\boldsymbol{z}}_1, \boldsymbol{z}_2) \leftarrow_{\$} D_{\mathbb{Z}^n,\sigma}^m \times D_{\mathbb{Z}^n,\sigma}$. If $\|(\hat{\boldsymbol{z}}_1, \boldsymbol{z}_2)\| > \gamma\sigma\sqrt{(m+1)n}$, the algorithm resamples $(\hat{\boldsymbol{z}}_1, \boldsymbol{z}_2)$. It expands the seed to a vector of polynomials by computing $\widehat{\boldsymbol{a}}' :=$ Expand(seed), and sets $\widehat{\boldsymbol{a}} := (1, \widehat{\boldsymbol{a}}')$ It also computes $\boldsymbol{b} := \widehat{\boldsymbol{a}} \cdot \hat{\boldsymbol{z}} \pmod{q}$. It sets sk = $\hat{\boldsymbol{z}}$, and pk = (seed, $\boldsymbol{b}$), and returns (sk, pk).

Table 4: Parameter definitions for the BLAZE+ blind signature scheme

Parameter	Definition and Constraints
λ	Main security parameter
n	Integer power of 2
m	Number of polynomials in the secret key, s.t. $m+1 \geq 2$
q	Prime modulus, s.t. $q \equiv 1 \pmod{2n}$
γ	Positive integer constant
σ	Standard deviation for the distribution from which the secret key sk is drawn, s.t. $\sigma > 0, (m+1)\log(t\sigma) > \log(q)$
κ	Hamming weight of H's output, s.t. $2^{\kappa}\binom{n}{\kappa} > 2^{\lambda}$
s^*	Standard deviation for the distribution from which the signer draws its blinding parameters, s.t. $s^* = a^*\gamma\sigma\sqrt{(m+1)\kappa n}$ where $a^* > 0$
s	Standard deviation for the distribution from which the user draws its blinding parameters, s.t. $s = \eta a s^*\sqrt{(m+1)\kappa n}$ where $a, \eta > 0$, and $\eta^{(m+1)n} e^{\frac{(m+1)n}{2}(1-\eta^2)} \leq 2^{-\lambda}$

Signing. The interactive signing protocol < S(sk), U(pk, msg)> works as follows:

1. **Signer**: On input secret key sk, as well as seed, the signer expands the seed $\widehat{\boldsymbol{a}}'$: =Expand(seed) and sets $\widehat{\boldsymbol{a}}$: = $(1, \widehat{\boldsymbol{a}}')$. It samples masking parameters $\hat{\boldsymbol{r}}_1^*, \dots, \hat{\boldsymbol{r}}_\kappa^* \leftarrow_\$ D_{\mathbb{Z}^n, s^*}^{m+1}$ and computes commitments $\boldsymbol{R}_j := \widehat{\boldsymbol{a}} \cdot \hat{\boldsymbol{r}}_j^* \pmod q$, $\forall j \in [\kappa]$. It sets $\widehat{\boldsymbol{R}} := (\boldsymbol{R}_1, \dots, \boldsymbol{R}_\kappa)$ and sends $\widehat{\boldsymbol{R}}$ to the user.

2. **User**: On input seed, and a message $msg \in \{0,1\}^*$, the user also expands the seed $\widehat{\boldsymbol{a}}' :=$ Expand(seed) and sets $\widehat{\boldsymbol{a}} := (1, \widehat{\boldsymbol{a}}')$. It samples signed permutations $p_1, \dots, p_\kappa \leftarrow_\$ \mathbb{S}$, randomness $\rho \leftarrow_\$ \{0,1\}^\lambda$, and masking terms $(\hat{\boldsymbol{e}}_0, \dots, \hat{\boldsymbol{e}}_{l-1}) \leftarrow_\rho D_{\mathbb{Z}^n, s}^{m+1}$ (notice that the random coins are fixed through ρ). It computes $\boldsymbol{y} := \sum_{j=1}^{\kappa} p_j \boldsymbol{R}_j \pmod q$ as well as $\boldsymbol{t}_j := \widehat{\boldsymbol{a}} \cdot \hat{\boldsymbol{e}}_j + \boldsymbol{y} \pmod q$, $\forall j = 0, \dots, l-1$. It uses the $\boldsymbol{t}_j$ elements as leaf nodes to construct a Merkle tree via (tree,root) := HashTree($(\boldsymbol{t}_0, \dots, \boldsymbol{t}_{l-1})$). It computes its challenge $\boldsymbol{c}$:= H(root, msg) and partitions it into polynomials c_j (this can trivially be done by writing $\boldsymbol{c}$ in the form $\boldsymbol{c} = \sum_{j=1}^{\kappa} c_j$, $c_j \in \mathbb{S}$). It blinds the partitioning polynomials with the help of signed permutations $p_1, \dots, p_\kappa$ via $c_j^* := c_j p_j^{-1}$, $\forall j$. It sets $\boldsymbol{c}^* := (c_1^*, \dots, c_\kappa^*)$ as the blinded challenge and transmits $\boldsymbol{c}^*$ to the signer.

3. **Signer**: On input a blinded challenge $\boldsymbol{c}^*$, the signer computes its responses $\hat{\boldsymbol{s}}_j^* := \hat{\boldsymbol{r}}_j^* + \mathsf{sk} \cdot c_j^*$, $\forall j \in [\kappa]$. It then invokes Rejection_Sample($(\hat{\boldsymbol{s}}_1^*, \dots, \hat{\boldsymbol{s}}_\kappa^*)$, $(\mathsf{sk} \cdot c_1^*, \dots, \mathsf{sk} \cdot c_\kappa^*)$) to make its response independent of sk. If rejection sampling fails, it restarts the entire protocol. Otherwise, it sets $\hat{\boldsymbol{s}}^* := (\hat{\boldsymbol{s}}_1^*, \dots, \hat{\boldsymbol{s}}_\kappa^*)$ and sends $\hat{\boldsymbol{s}}^*$ to the user.

4. **User**: The user receives $\hat{\boldsymbol{s}}^*$ and computes $\widehat{\boldsymbol{v}} := \sum_{j=1}^{\kappa} p_j \hat{\boldsymbol{s}}_j^*$. If $\|\widehat{\boldsymbol{v}}\| > \eta s^* \sqrt{(m+1)\kappa n}$, the protocol is aborted (this occurs with probability $2^{-\lambda}$). The user then locates the first $\hat{\boldsymbol{e}}_j$, $j \in \{0, \dots, l-1\}$ for which rejection sampling of $\hat{\boldsymbol{e}}_j + \widehat{\boldsymbol{v}}$ succeeds (if none succeed, the protocol is aborted)[5]. Let I be the index of the first successful rejection sampling. The user sets $\hat{\boldsymbol{s}}$: =Compress $(\hat{\boldsymbol{e}}_I + \widehat{\boldsymbol{v}})$ and also invokes BuildAuth(I, tree) to compute an authentication path proving that the I-th element under root was used to compute $\hat{\boldsymbol{s}}$. It outputs ($\hat{\boldsymbol{s}}$, $\boldsymbol{c}$, auth) as its blind signature.

Verification. On input public key pk, message $msg \in \{0,1\}^*$ and a purported signature ($\hat{\boldsymbol{s}}$, $\boldsymbol{c}$, auth), the verifier expands the seed to obtain $\widehat{\boldsymbol{a}}' :=$ Expand(seed), $\widehat{\boldsymbol{a}} := (1, \widehat{\boldsymbol{a}}')$ and decompresses the signature via $\hat{\boldsymbol{s}}$: =Decompress($\hat{\boldsymbol{s}}$). It computes $\boldsymbol{w} := \widehat{\boldsymbol{a}} \cdot \hat{\boldsymbol{s}} - \boldsymbol{bc} \pmod q$ and root := RootCalc($\boldsymbol{w}$, auth). If $\|\hat{\boldsymbol{s}}\| \le \eta s \sqrt{(m+1)n}$ and c = H(root, msg), it returns 1 (accept). Otherwise, it outputs 0 (reject).

Claimed Security Results:

Correctness is significantly improved over BLAZE thanks to the use of a Merkle tree:

Lemma 8. (Adapted from Theorem 1 of (Alkadri et al., 2020b)) If the parameters are set according to Table 4, then BLAZE+ has a correctness error of $2^{-2\lambda}$.

While this variant manages to decouple itself from relying a commitments scheme, it still satisfies blindness in a statistical sense:

Lemma 9. (Adapted from Theorem 2 of (Alkadri et al., 2020b)) BLAZE+ is statistically blind.

Finally, as long as the hash function G used for constructing the Merkle tree satisfies collision-resistance and R−SIS is hard, BLAZE+ is strongly one-more unforgeable:

Lemma 10. (Adapted from Theorem 3 of (Alkadri et al., 2020b)) If G : $\{0,1\}^* \to \{0,1\}^{2\lambda}$ is a collision-resistant hash function used for constructing the Merkle trees during the signing protocol, and R−SIS is hard for the parameters set according to Table 4, then BLAZE+ is strongly one-more unforgeable in the ROM.

3.3.2. Four-move Variant of BLAZE+

In (Alkadri et al., 2020b), the authors propose a second, 4-move, "hybrid" variant of BLAZE+ in which the user can prove that a session did not yield a valid signature similarly to BLAZE. This approach however circumvents the attack discussed in Section 3.2.3 because multiple rejection samplings are performed when the user unblinds. The number of such samplings can be set to a sufficiently high value, which guarantees that at least one of them will succeed, thus preventing the user from claiming otherwise. In addition to the cryptographic ingredients required in the 3-move variant of BLAZE+, this variant also makes use of a be a statistically hiding and computationally binding commitment function $\{0,1\}^* \times \{0,1\}^\lambda \to \{0,1\}^\lambda$.

Key Generation. Algorithm KeyGen(1^λ) is identical to the 3-move variant of BLAZE+.

Signing. The interactive signing protocol < S(sk), U(pk, msg)> works as follows:

1. **Signer**: On input secret key sk, as well as seed, the signer expands the seed $\widehat{\boldsymbol{a}}' :=$ Expand(seed) and sets $\widehat{\boldsymbol{a}} := (1, \widehat{\boldsymbol{a}}')$. It samples masking parameters $\hat{\boldsymbol{r}}_1^*, \ldots, \hat{\boldsymbol{r}}_\kappa^* \leftarrow_\$ D_{\mathbb{Z}^n,s}^{m+1}$ and computes commitments $\boldsymbol{R}_j := \widehat{\boldsymbol{a}} \cdot \hat{\boldsymbol{r}}_j^* \pmod q$, $\forall j \in [\kappa]$. It sets $\widehat{\boldsymbol{R}} := (\boldsymbol{R}_1, \ldots, \boldsymbol{R}_\kappa)$ and sends $\widehat{\boldsymbol{R}}$ to the user.

2. **User**: On input seed, and a message $msg \in \{0,1\}^*$, the user also expands the seed $\widehat{\boldsymbol{a}}' :=$ Expand(seed) and sets $\widehat{\boldsymbol{a}} := (1, \widehat{\boldsymbol{a}}')$. It samples signed permutations $p_1, \ldots, p_\kappa \leftarrow_\$ \mathbb{S}$, random coins r, r', ρ, $\rho' \leftarrow_\$ \{0,1\}^\lambda$, and masking terms $(\hat{\boldsymbol{e}}_0, \ldots, \hat{\boldsymbol{e}}_{l-1}) \leftarrow_\rho D_{\mathbb{Z}^n,s}^{m+1}$ (notice that the random coins are fixed through ρ). It

commits to the message-to-be-signed msg and the randomness ρ' by computing $C_1 \coloneqq \mathrm{com}(msg, r)$ and $C_2 \coloneqq \mathrm{com}(\rho', r')$, respectively. It computes $\boldsymbol{y} \coloneqq \sum_{j=1}^{\kappa} p_j \boldsymbol{R}_j \pmod q$ as well as $\boldsymbol{t}_j \coloneqq \hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{e}}_j + \boldsymbol{y} \pmod q$, $\forall j = 0, \dots, l-1$. It uses the $\boldsymbol{t}_j$ elements as leaf nodes to construct a Merkle tree via (tree, root) := HashTree($\boldsymbol{t}_0, \dots, \boldsymbol{t}_{l-1}$). It computes its challenge $\boldsymbol{c} \coloneqq$H(root, C_1, C_2) by passing C_1 and C_2 as inputs to H, and partitions the challenge into monomials c_j (this can trivially be done by writing $\boldsymbol{c}$ in the form $\boldsymbol{c} = \sum_{j=1}^{\kappa} c_j$, $c_j \in \mathbb{S}$). It blinds the partitioning polynomials with the help of signed permutations $p_1, \dots, p_\kappa$ via $c_j^* \coloneqq c_j p_j^{-1}$, $\forall j$. It sets $\boldsymbol{c}^* \coloneqq (c_1^*, \dots, c_\kappa^*)$ as the blinded challenge and transmits $\boldsymbol{c}^*$ to the signer.

3. **Signer**: On input a blinded challenge $\boldsymbol{c}^*$, the signer computes its responses $\hat{\boldsymbol{s}}_j^* \coloneqq \hat{\boldsymbol{r}}_j^* + \mathsf{sk} \cdot c_j^*$, $\forall j \in [\kappa]$. It then invokes Rejection_Sample($(\hat{\boldsymbol{s}}_1^*, \dots, \hat{\boldsymbol{s}}_\kappa^*)$, $(\mathsf{sk} \cdot c_1^*, \dots, \mathsf{sk} \cdot c_\kappa^*)$) to make its response independent of sk. If rejection sampling fails, it restarts the entire protocol. Otherwise, it sets $\hat{\boldsymbol{s}}^* \coloneqq (\hat{\boldsymbol{s}}_1^*, \dots, \hat{\boldsymbol{s}}_\kappa^*)$ and sends $\hat{\boldsymbol{s}}^*$ to the user.

4. **User**: The user receives $\hat{\boldsymbol{s}}^*$ and computes $\hat{\boldsymbol{v}} \coloneqq \sum_{j=1}^{\kappa} p_j \hat{\boldsymbol{s}}_j^*$. If $\|\hat{\boldsymbol{v}}\| > \eta s^* \sqrt{(m+1)\kappa n}$, the protocol is aborted (this occurs with probability $2^{-\lambda}$). The user expands ρ' into l random coins via $(\rho_0, \dots, \rho_{l-1})$:= Expand(ρ'). The user then locates the first pair of the form $(\hat{\boldsymbol{e}}_j, \rho_j)$, $j \in \{0, \dots, l-1\}$ for which rejection sampling of $\hat{\boldsymbol{e}}_j + \hat{\boldsymbol{v}}$ with fixed randomness ρ_j succeeds. Let I be the index of the first successful rejection sampling. The user sets $\hat{\boldsymbol{s}}$: =Compress($\hat{\boldsymbol{e}}_I + \hat{\boldsymbol{v}}$) and also invokes BuildAuth(I, tree) to compute an authentication path proving that the I-th element under root was used to compute $\hat{\boldsymbol{s}}$. It outputs (C_2, r, $\hat{\boldsymbol{s}}$, $\boldsymbol{c}$, auth) as its blind signature. On the contrary, if all rejection samplings fail, it sends (C_1, ρ, ρ', r', $p_1, \dots, p_\kappa$, $\boldsymbol{c}$) to the signer, requesting a restart.

5. **Signer**: Upon receiving (C_1, ρ, ρ', r', $p_1, \dots, p_\kappa$, $\boldsymbol{c}$), the signer computes $C_2 \coloneqq \mathrm{com}(\rho', r')$, $(\rho_0, \dots, \rho_{l-1}) \coloneqq$ Expand(ρ'), $(\hat{\boldsymbol{e}}_0, \dots, \hat{\boldsymbol{e}}_{l-1}) \leftarrow_\rho D_{\mathbb{Z}^{n},\mathrm{s}}^{m+1}$, $\boldsymbol{y} \coloneqq \sum_{j=1}^{\kappa} p_j \boldsymbol{R}_j \pmod q$, $\boldsymbol{t}_j \coloneqq \hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{e}}_j + \boldsymbol{y} \pmod q$, $\forall j = 0, \dots, l-1$, (tree, root) := HashTree($\boldsymbol{t}_0, \dots, \boldsymbol{t}_{l-1}$), $\hat{\boldsymbol{v}} \coloneqq \sum_{j=1}^{\kappa} p_j \hat{\boldsymbol{s}}_j^*$. For each $j \in \{0, \dots, l-1\}$, the signer computes $\boldsymbol{w} \coloneqq \hat{\boldsymbol{a}} \cdot (\hat{\boldsymbol{e}}_j + \hat{\boldsymbol{v}}) - \boldsymbol{bc} \pmod q$ and auth_j: =BuildAuth(j, tree). It then verifies that all rejection samplings on the user's side failed by checking whether $\boldsymbol{c} \neq$H(RootCalc($\boldsymbol{w}_j$, auth_j), C_1, C_2) or Rejection_Sample($\hat{\boldsymbol{e}}_j + \hat{\boldsymbol{v}}$, ρ_j) = 1, $\forall j = 0, \dots, l-1$, and if that is the case, it ignores the user's request. Finally, if $\boldsymbol{c}$ = H(root, C_1, C_2) = $\sum_{j=1}^{\kappa} p_j c_j^*$, the signer restarts the entire protocol. Otherwise, it ignores the user's request.

Verification. On input public key pk, message $msg \in \{0,1\}^*$ and a purported signature (C_2, r,$\hat{\boldsymbol{s}}$, $\boldsymbol{c}$, auth), the verifier expands the seed to obtain $\hat{\boldsymbol{a}}'$:= Expand(seed), $\hat{\boldsymbol{a}} \coloneqq (1, \hat{\boldsymbol{a}}')$ and decompresses the signature via $\hat{\boldsymbol{s}}$:= Decompress($\hat{\boldsymbol{s}}$). It computes $\boldsymbol{w} \coloneqq \hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{s}} - \boldsymbol{bc} \pmod q$ and root := RootCalc($\boldsymbol{w}$, auth).

If $\|\hat{\boldsymbol{s}}\| \leq \eta s\sqrt{(m+1)n}$ and $\boldsymbol{c}$ = H(root, com(msg, r), C_2), it returns 1 (accept). Otherwise, it outputs 0 (reject).

3.4. Ermann's Blind Signature Scheme

Ermann et al. (Ermann et al., 2020) propose a 3-move "Schnorr-like" blind signature scheme from lattice assumptions but with a twist in order to achieve perfect correctness. The key idea is to trapdoor the SIS function using a technique from (Micciancio and Peikert, 2012). This allows the signer to sample a preimage for its response until the latter satisfies a certain shortness condition. Since the signer can always come up with an appropriately distributed response, it is freed from having to restart the entire protocol. Moreover, the user is also freed from having to rejection sample when it unblinds to obtain its signature. The only cryptographic block required for their scheme is a hash function H: $\{0,1\}^* \to R_2$ modelled as a random oracle.

3.4.1. Construction

Key Generation. Let $\hat{\boldsymbol{g}} := (1, 2, 2^2, \ldots, 2^{k-1})^T \in R_q^k$, with $k = log(q)$ be the *gadget vector*. On input the security parameter n, algorithm KeyGen(1^n) samples $\hat{\boldsymbol{s}} \leftarrow_{\$} R_3^m$, a vector of polynomials $\hat{\boldsymbol{a}}' \leftarrow_{\$} R_q^{m-k}$, a polynomial $\boldsymbol{h} \leftarrow_{\$} R_q$ and a short trapdoor vector $\hat{\mathbf{T}}_{\hat{\boldsymbol{a}}} \in R_q^{(m-k)\times k}$ from a discrete Gaussian distribution with standard deviation τ. It computes a vector of polynomials $\hat{\boldsymbol{a}} := \left(\hat{\boldsymbol{a}}'^T, \boldsymbol{h}\hat{\boldsymbol{g}} - \hat{\boldsymbol{a}}'^T\hat{\mathbf{T}}_{\hat{\boldsymbol{a}}}\right)^T$. Let $\mathrm{F}_{\hat{\boldsymbol{a}}}: R_q^m \to R_q$ be the SIS function defined by $\hat{\boldsymbol{a}}$ (i.e., $\mathrm{F}_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{x}}) := \hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{x}}$). The algorithm computes $\mathbf{S} := \mathrm{F}_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{s}})$, it sets sk := $(\hat{\boldsymbol{s}}, \hat{\mathbf{T}}_{\hat{\boldsymbol{a}}})$, pk := $(\mathbf{S}, \hat{\boldsymbol{a}})$, and outputs (sk, pk).

Signing. The interactive signing protocol < S(sk), U(pk, msg)> works as follows:

1. **Signer**: The signer samples masking a vector $\hat{\boldsymbol{r}} \leftarrow_{\$} D_{R,\sigma}^m$ and computes a commitment $\mathbf{R} := \mathrm{F}_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{r}})$. It sends $\mathbf{R}$ to the user.

2. **User**: The user receives $\mathbf{R}$ and samples masking parameters $\boldsymbol{t}_1 \leftarrow_{\$} D_{R,\alpha}$, $\hat{\boldsymbol{t}}_2 \leftarrow_{\$} D_{R,\beta}^m$. If $\|\hat{\boldsymbol{t}}_2\| > t\beta\sqrt{mn}$, it resamples $\hat{\boldsymbol{t}}_2$. It computes its challenge via $\boldsymbol{c} := \mathrm{H}(\mathbf{R} - \boldsymbol{t}_1 \cdot \mathbf{S} - \mathrm{F}_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{t}}_2), msg)$ and blinds it by computing $\boldsymbol{c}^* := \boldsymbol{c} - \boldsymbol{t}_1$. With probability $min(1, D_{R,\alpha}/(G_1 \cdot D_{R,\alpha,\boldsymbol{c}}))$, the user sends $\boldsymbol{c}^*$ to the signer. Otherwise, it repeats the entire step from scratch.

3. **Signer**: The signer receives $\boldsymbol{c}^*$ and computes its response $\hat{\boldsymbol{z}}^* := \boldsymbol{c}^* \cdot \hat{\boldsymbol{s}} + \hat{\boldsymbol{r}}$. With probability $min(1, D_{R,\sigma}^m/(G_2 \cdot D_{R,\sigma,\boldsymbol{c}^*\hat{\boldsymbol{s}}}^m))$, $\hat{\boldsymbol{z}}^*$ will be used by the signer. With probability $1 - min(1, D_{R,\sigma}^m/(G_2 \cdot D_{R,\sigma,\boldsymbol{c}^*\hat{\boldsymbol{s}}}^m))$, the signer uses $\hat{\mathbf{T}}_{\hat{\boldsymbol{a}}}$ to sample a preimage of $\boldsymbol{c}^* \cdot \mathbf{S} + \mathbf{R}$ via $\hat{\boldsymbol{z}}^* \leftarrow$PreSample$(\hat{\mathbf{T}}_{\hat{\boldsymbol{a}}}, \boldsymbol{c}^* \cdot \mathbf{S} + \mathbf{R}, \sigma)$. If $\|\hat{\boldsymbol{z}}^*\| > t\sigma\sqrt{mn}$

Table 5: Parameter definitions for the Ermann et al. blind signature scheme

Parameter	Definition and Constraints
λ	Main security parameter
n	Integer power of 2
m	Number of polynomials in the secret key, s.t. $m \coloneqq \lfloor \log(q) \rfloor + 1$
α	$\omega\left(k\sqrt{\log(n)}\right)$
β	$2^{\omega(\log(n))}\sigma\sqrt{n}$
γ	$n\alpha$
τ	Standard deviation of the distribution from which the secret key is drawn
σ	$\omega\left(\left(n\sqrt{n}\alpha\right)\sqrt{\log(n)}\right)$
$\mathbb{D}$	$t\sqrt{nm}(\beta + \sigma)$
q	Prime modulus, s.t. $q \geq 4mn\sqrt{n}\log(n)$

, it samples a fresh preimage for $\boldsymbol{c}^* \cdot \mathbf{S} + \mathbf{R}$. Once this condition is satisfied, it sends $\hat{\boldsymbol{z}}^*$ to the user.

4. **User**: The user unblinds the signer's response by computing $\hat{\mathbf{z}} \coloneqq \hat{\mathbf{z}}^* - \hat{t}_2$. It outputs $(\hat{\boldsymbol{z}}, \boldsymbol{c})$ as its blind signature.

Verification. On input public key pk, a purported signature $(\hat{\boldsymbol{z}}, \boldsymbol{c})$ and message $msg \in \{0,1\}^*$, algorithm Ver(pk, $(\hat{\boldsymbol{z}}, \boldsymbol{c})$, msg) outputs 1 iff $\|\hat{\boldsymbol{z}}\| \leq t(\beta + \sigma)\sqrt{mn}$ and $\mathsf{H}(\mathrm{F}_{\hat{\boldsymbol{a}}}(\hat{\boldsymbol{z}}) - \mathbf{S} \cdot \boldsymbol{c}, msg) = \boldsymbol{c}$. Otherwise, it outputs 0.

4.1.2. Claimed Security Results

Thanks to the use of a trapdoor, the signer is always able to respond to the signer, without having to abort the interactive protocol. This also results in freeing the user from having to rejection sample when unblinding:

Lemma 11. (Theorem 2 in (Ermann et al., 2020)) The above scheme has perfect correctness.

Even though no commitment scheme is used, blindness is shown to hold in a statistical sense:

Lemma 12. (Theorem 3 in (Ermann et al., 2020)) The above scheme is statistically blind.

Finally, unforgeability is based on the hardness of the (Ring) k–SIS problem:

Lemma 13. (Theorem 4 in (Ermann et al., 2020)) If Ring $k - \mathrm{SIS}_{q,m,\mathbb{D}}$ is hard for the parameters set according to Table 5, then the above scheme is one-more unforgeable.

3.5. The Forking Lemma and Other Flawed Constructions

The recent work of (Hauck et al., 2020) states a very subtle flaw that is shared by all of the constructions presented so far and which stems from an incorrect application of the general Forking Lemma (Bellare and Neven, 2006). The key strategy followed in their unforgeability proofs is to rewind the adversary with a partially changed random oracle so as to obtain two distinct values χ and χ' s.t. $\mathrm{F}(\chi) = \mathrm{F}(\chi')$. The value $\chi - \chi'$ is then a non-trivial solution for the underlying hard lattice problem (i.e., SIS). In order to prove that $\chi - \chi'$ is non-trivial, they try to apply an argument similar to Lemma 8 from (Pointcheval and Stern, 2000), and state that non-triviality is a direct consequence of the scheme's witness indistinguishability. This is incorrect because Lemma 8 of (Pointcheval and Stern, 2000) only implies that there exist two distinct secret keys sk, sk', leading to identical protocol transcripts. This argument does not suffice for claiming non-triviality and applying the general Forking Lemma. (Hauck et al., 2020) leaves mending these proofs as an interesting open question.

Zhu et al. (Zhu et al., 2017) follow a completely different approach based on the hardness of the closest vector problem (CVP) in order to design round-optimal (i.e., with only 2-moves) blind signature schemes. Their construction however has been shown to be flawed in (Cheon et al., 2019) (also see (Alkadri et al., 2020a) for an attack). Another line of papers (Liang, 2011; Zhang, 2014; Zhang, 2016; Gao, 2017) attempt to construct "RSA-style" blind signature schemes (and variants thereof). All of them however are vulnerable to an attack described in (Alkadri et al., 2020a) (also see (Rückert, 2010) for a discussion).

Remark 1. (from (Rückert, 2010)) It is impossible to construct secure RSA-style (Chaum, 1983; Chaum, 1984; Chaum, 1988) blind signatures from lattice assumptions (i.e., following the pattern: hash → blind → invert →

unblind) because then the scheme becomes vulnerable to an attack described in (Rückert, 2010).

Finally, (Papachristoudis et al., 2019) tries to construct partially-blind signature schemes (i.e., schemes in which both the signer and the user share a common public value) from lattice assumptions. This work also has a flawed security proof due to incorrect application of the Forking Lemma. We are currently unaware of any provably secure partially-blind signature scheme from lattice assumptions. It is an interesting open question whether one can extend the modular framework of (Hauck et al., 2020) to render partially-blind signature schemes from lattices.

4. Provably Secure Lattice-Based Blind Signature Schemes

In this section, we cover provably secure proposals of blind signature schemes from lattice assumptions. There currently exist two approaches for rendering blind signatures from lattices. The first by (Hauck et al., 2020) adapts the paradigm of the Okamoto-Schnorr blind signature (Okamoto, 1992) from the discrete logarithm setting to the lattice setting. The second one followed by (Agrawal et al., 2021) is based on the observation that homomorphic encryption can be used to achieve round-optimality for blind signatures in the lattice setting (Garg et al., 2011).

4.1. Hauck et al.'s Blind Signature Scheme

The recent work of (Hauck et al., 2020) proposes for the first time a correct and modular framework for rendering blind signature schemes from *any* linear hash function family displaying some form of correctness error. Their construction is provably secure in the ROM even against forgers that are allowed to perform concurrent protocol executions. The key idea in their scheme is to have the signer commit to multiple masking terms during its first move, then have the user also pick multiple masking parameters and to store (a function of) each such combination as a leaf of a Merkle tree. This approach guarantees that for sufficiently many sampled blinding parameters, the probability of aborting during rejection-sampling (on either side) in the signing protocol will be negligible. The user can use an authentication path in order to prove that a particular trial under the Merkle tree's root was indeed used for producing its signature. While the construction in (Hauck et al., 2020) is generic, below we focus on its instantiation from the SIS linear hash function family.

4.1.1. Construction

Let $2\text{Int}_{\eta,\nu,\mu}: [\eta] \times [\nu] \times [\mu] \to [\eta\nu\mu]$ be the mapping $(i, j, k) \mapsto i + \eta \cdot (j-1) + \eta\nu \cdot (k-1)$, s.t. $2\text{Int}_{\eta,\nu,\mu}(1,1,1) = 1$ and $2\text{Int}_{\eta,\nu,\mu}(\eta, \nu, \mu) = \eta\nu\mu$. The main building blocks are:

- a hash function $\mathsf{H}\ \{0,1\}^* \to S_{c\prime} \coloneqq \{\boldsymbol{c} \in R_q : \|\boldsymbol{c}\|_\infty \leq d_{c\prime}\}$, modeled as a random oracle,
- a collision-free and chain-free hash function $\mathrm{G}: \{0,1\}^* \to \{0,1\}^{2\lambda}$.

Table 6: Parameter definitions for the Hauck et al. blind signature scheme

Parameter	Definition and Constraints
λ	Main security parameter
n	Integer power of 2
m	Number of polynomials in the secret key s.t. $m > \log(q)\ /\log\ (2d)$
q	Prime modulus s.t. $q \geq 4dmn\sqrt{n}\log\ (n)$
ι	Number of irreducible factors of $x^n + 1$ modulo q s.t. $q \equiv 2\iota + 1\ (\text{mod}\ 4\iota)$
δ	Bound for the infinity norm of torsion-free elements from the kernel of F, s.t. $(\delta + 1)^{mn} > q^n$
d_{sk}	Bound for the infinity norm of secret keys
$\mathbb{D}_{sk}$	$\{\boldsymbol{v} \in R_q : \|\boldsymbol{v}\|_\infty \leq d_{sk}\}$
$d_{c\prime}$	Bound for the infinity norm of the outputs of H
$S_{c\prime}$	The challenge space $\{\boldsymbol{v} \in R_q : \|\boldsymbol{v}\|_\infty \leq d_{c\prime}\}$
u, v, w	Positive integer constants for controlling the accept-reject ratio of rejection sampling
μ	Number of blinding parameters $\boldsymbol{b}_j$ picked by the user
η	Number of commitments $\boldsymbol{R}_i$ sent by the signer
ν	Number of blinding parameters $\widehat{\boldsymbol{a}}_k$ picked by the user
d_b	Bound for the infinity norm of blinding parameters $\boldsymbol{b}_j$ s.t. $d_b \coloneqq ud_{c\prime}n$

Parameter	Definition and Constraints
S_b	$\{\boldsymbol{v} \in R_q : \|\boldsymbol{v}\|_\infty \leq d_b\}$
d_c	Bound for the infinity norm of blinded challenges $\boldsymbol{c}$, s.t. $d_c < \frac{1}{2\sqrt{\iota}} q^{1/\iota}$
S_c	$\{\boldsymbol{v} \in R_q : \|\boldsymbol{v}\|_\infty \leq d_c\}$
d_r	Bound for the infinity norm of blinding parameters $\hat{\boldsymbol{r}}_i$, s.t. $d_r \geq vmn^2 d_{sk} d_c$
$\mathbb{D}_r$	$\{\boldsymbol{v} \in R_q : \|\boldsymbol{v}\|_\infty \leq d_r\}$
d_s	Bound for the infinity norm of signer responses $\hat{\boldsymbol{s}}$, s.t. $d_s := d_r n d_{sk} d_c$
$\mathbb{D}_s$	$\{\boldsymbol{v} \in R_q : \|\boldsymbol{v}\|_\infty \leq d_s\}$
d_a	Bound for the infinity norm of blinding parameters $\hat{\boldsymbol{a}}_k$, s.t. $d_a := w d_s n m$
$\mathbb{D}_a$	$\{\boldsymbol{v} \in R_q : \|\boldsymbol{v}\|_\infty \leq d_a\}$
$d_{s\prime}$	Bound for the infinity norm of unblended responses $\hat{\boldsymbol{s}}'$, s.t. $d_{s\prime} := d_a - d_s$
$\mathbb{D}_{s\prime}$	$\{\boldsymbol{v} \in R_q : \|\boldsymbol{v}\|_\infty \leq d_{s\prime}\}$
d	Bound for the infinity norm of the collision set, s.t. $d := 2d_{s\prime}, d < \frac{1}{2}\min\left\{q, 2^{2\sqrt{n\log(q)\log(\delta)}}\left(\frac{n\log(q)}{\log(\delta)}\right)^{-1/4}\right\}$
$\mathbb{D}$	$\{\boldsymbol{v} \in R_q : \|\boldsymbol{v}\|_\infty \leq d\}$

Key Generation. On input the security parameter λ, algorithm KeyGen(1^λ) samples a secret key $\hat{\boldsymbol{z}} \leftarrow \mathbb{D}_{sk}^m$. It sets sk := $\hat{\boldsymbol{z}}$ and computes the public key via pk := F(sk) and outputs (sk, pk).

Signing. The interactive signing protocol < S(sk), U(pk, msg)> works as follows:

1. **Signer**: The signer picks masking parameters $\hat{\boldsymbol{r}}_i \leftarrow_\$ \mathbb{D}_r^m$, $\forall i \in [\eta]$ and computes $\boldsymbol{R}_i := \mathsf{F}(\hat{\boldsymbol{r}}_i), \forall i \in [\eta]$. It sends commitment $\widehat{\boldsymbol{R}} := (\boldsymbol{R}_1, \ldots, \boldsymbol{R}_\eta)$to the user.

2. **User**: The user receives $\widehat{\boldsymbol{R}} := (\boldsymbol{R}_1, \ldots, \boldsymbol{R}_\eta)$ and picks its own masking parameters $\hat{\boldsymbol{a}}_1, \ldots, \hat{\boldsymbol{a}}_\nu \leftarrow_\$ \mathbb{D}_a^m$, $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_\mu \leftarrow_\$ S_b$, and $\gamma \leftarrow_\$ \mathbb{Z}_\eta$. It computes all possible combinations of masked commitments $\boldsymbol{R}'_{i\oplus\gamma,j,k} := \boldsymbol{R}_i + \mathsf{F}(\hat{\boldsymbol{a}}_k) + \boldsymbol{b}_j \cdot \mathsf{pk}$ for all $(i, j, k) \in [\eta] \times [\mu] \times [\nu]$ ($\oplus$ denotes the bitwise XOR operator). It constructs

a Merkle tree with the masked commitments as leaves via (tree, root) := HashTree($\boldsymbol{R}'_{1,1,1}, \ldots, \boldsymbol{R}'_{\eta,\mu,\nu}$). It then computes its challenge as $\boldsymbol{c}' :=$H(root, msg) and proceeds to locate the first masking polynomial $\boldsymbol{b}$ for which rejection-sampling succeeds. If there exists an index $j \in [\mu]$ s.t $\boldsymbol{c}' + \boldsymbol{b}_j \in S_c$, it sets $\boldsymbol{c} := \boldsymbol{c}_j + \boldsymbol{b}_j$ and sends $\boldsymbol{c}$ to the user. Otherwise, (i.e., if no such index is found), it sends $\perp$ to the signer, indicating failure.

3. **Signer**: The signer receives $\boldsymbol{c} \in S_c$ and computes its response with the help of the secret key. In particular, it locates the first $i \in [\eta]$ s.t. $\hat{\boldsymbol{s}} := \hat{\boldsymbol{r}}_i + \boldsymbol{c} \cdot$sk falls within the set $\mathbb{D}_s^m$. The signer sends $\hat{\boldsymbol{s}}$ to the user. Otherwise, if no masking term $\hat{\boldsymbol{r}}_i$ satisfies this criterion, it sends $\perp$ to the user.

4. **User**: The user receives $\hat{\boldsymbol{s}} \in \mathbb{D}_s^m$ and locates the first index $i \in [\eta]$ s.t. $\mathsf{F}(\hat{\boldsymbol{s}}) = \boldsymbol{c} \cdot \mathsf{pk} + \boldsymbol{R}_i$ (if no such index is found, it outputs $\perp$). It then finds the first index $k \in [\nu]$ for which the corresponding blinding term $\hat{\boldsymbol{a}}_k$ causes $\hat{\boldsymbol{s}}' := \hat{\boldsymbol{s}} + \hat{\boldsymbol{a}}$ to fall within $\mathbb{D}_{s'}^m$ (if no such index is found, it outputs $\perp$). The user recalls the index $j \in [\mu]$ that it used during Step 2 and computes an authentication path auth := BuildAuth((2Int($i \oplus \gamma, j, k$), tree) for the specific combination under root that was used. It outputs ($\hat{\boldsymbol{s}}'$, $\boldsymbol{c}'$, auth) as its blind signature.

Verification. On input the public key pk, a message $msg \in \{0,1\}^*$and a purported signature of the form ($\hat{\boldsymbol{s}}'$, $\boldsymbol{c}'$, auth), the verifier computes $\boldsymbol{R}' :=\mathsf{F}(\hat{\boldsymbol{s}}')-\boldsymbol{c}' \cdot$ pk and root := RootCalc($\boldsymbol{R}'$, auth). If $\boldsymbol{c}'$ =H(root, msg) and $\hat{\boldsymbol{s}}' \in \mathbb{D}_{s'}^m$, it outputs 1. Otherwise, it outputs 0.

4.1.2. Proved Security Results

The main advantage of using a Merkle tree is that both parties can sample multiple masking parameters but only use the combination which causes all rejection samplings on their respective side of the protocol to succeed. This leads to the following result about correctness:

Lemma 14. (Adapted from Lemma 3 of (Hauck et al., 2020)) The construction by (Hauck et al., 2020) has a correctness error of $(1 - e^{-1/u} + o(1))(1 - e^{-1/v} + o(1))(1 - e^{-1/w} + o(1))$.

By avoiding the use of a commitment scheme, the construction of (Hauck et al., 2020) achieves statistical blindness. If the underlying hash function family F has sufficient min-entropy, the construction also seems to attain perfect blindness.

Lemma 15. (Adapted from Theorem 2 of (Hauck et al., 2020)) Let LHF = (PGen, F) denote the R-SIS hash function family. For parameters set according to Table 6, the construction by (Hauck et al., 2020) is perfectly blind relative to all par ∈PGen(1^κ).

Finally, unforgeability is proven in two steps: (i) by reducing

collision-resistance of the underlying LHF to one-more-man-in-the-middle security (OMMIM) (Hauck et al., 2019) for an intermediate identification scheme (cf. Section 5.2 of (Hauck et al., 2020)), and (ii) reducing OMMIM security of the identification scheme to one-more unforgeability of the blind signature scheme. This leads to the following result:

Lemma 16. (Adapted from Theorem 1 of (Hauck et al., 2020)) Let LHF = (PGen, F) denote the R-SIS hash function family. If LHF is collision-resistant relative to par ∈PGen(1^{κ}), then the construction by (Hauck et al., 2020) is one-more unforgeable relative to par in the ROM.

Remark:We observe that although unforgeability is proved relative to fixed par ∈PGen(1^{κ}), it is possible to extend the proof for par $\leftarrow_{\$}$ PGen(1^{κ}) using techniques from (Hauck et al., 2019).

4.1.3. Discussion on Hauck et al.'s Blind Signature Scheme

The scheme by Hauck et al is an adaptation of the Okamoto-Schnorr blind signature (Okamoto, 1992) from the discrete logarithm regime to the lattice regime. This incurs a significant loss in advantage larger than $2Q_S/|S_{c'}|$ for the reduction, where Q_S denotes the maximum number of signatures that the signer can issue before needing to replace its key. This loss is due to the forger's ability to perform concurrent protocol executions with the signer which significantly limits Q_S in practice. For example, for a security level of 128 bits, the number of signatures that can be issued before needing to change the public key is $\log(128) = 7$.

An important remark about the unforgeability proof of (Hauck et al., 2020) is that due to the multiple trials involved in each rejection sampling, the protocol will, with overwhelming probability not abort. This allows the construction of (Hauck et al., 2020) to remain consistent with the standard notion of unforgeability which is only meaningful for blind signature schemes with (at most) negligible correctness error. If the scheme can abort with noticeable probability, then even honest adversaries may not be able to produce even l valid signatures after l signing sessions. However, it still has to come up with $l + 1$ signatures in order to win in the unforgeability game. This leads to a significant weakening of the definition and could potentially point towards a more general notion of unforgeability in which signing sessions can be revoked like in (Rückert, 2010; Alkadri et al., 2020a; Alkadri et al., 2020b).

4.2. Agrawal et al.'s Blind Signature Scheme

The state-of-the-art lattice-based proposal by (Agrawal et al., 2021) follows

a completely different design approach for rendering blind signature schemes in the ROM. This is accomplished by simplifying the standard model, 2-move construction by (Garg et al., 2011) which results in a round optimal, very efficient and at the same time simple scheme. Furthermore, unlike (Hauck et al., 2020), their constructions do not limit the signer to issuing a polylogarithmic amount of signatures.

4.2.1. Construction

A crucial component of (Agrawal et al., 2021) is a rejection-free variant of Lyubashevsky's digital signature scheme (Lyubashevsky, 2012). Removing the rejection-sampling step is important in order to be able to express the signing algorithm as a relatively simple circuit. The main building block sare:

- a hash function $\mathsf{H}:\{0,1\}^* \to \{\boldsymbol{v} \in \{0,\pm 1\}^k : \|\boldsymbol{v}\|_1 \leq a\}$, modeled as a random oracle,
- a pseudorandom function family (PRF) $F: \{0,1\}^r \times \{0,1\}^* \to \{0,1\}^r$ (used for derandomizing the signing algorithm).

Key Generation. On input the security parameter 1^λ, algorithm Sig.KeyGen(1^λ) samples the key of PRF F as $k_{\text{prf}} \leftarrow_{\$} \{0,1\}^r$ as well as matrices $\mathbf{A} \leftarrow_{\$} \mathbb{Z}_q^{n\times m}$ and $\mathbf{S} \leftarrow \{-d, \ldots, d\}^{m\times k}$. It computes $\mathbf{R} \coloneqq \mathbf{AS}$, and sets vk := ($\mathbf{A}$, $\mathbf{T}$) as the (public) verification key and sk := (k_{prf}, $\mathbf{S}$) as the (private) signing key. It outputs vk, sk.

Signing. On input the signing key sk and a message $msg \in \{0,1\}^*$, algorithm Sig.Sign(sk, msg) generates message-specific randomness $rnd = F(k_{\text{prf}}, msg)$. It samples $\boldsymbol{y} \leftarrow_{rnd} D_\sigma^m$ using fixed randomness rnd. It sets $\boldsymbol{c}$: =$\mathsf{H}(\mathbf{A}\boldsymbol{y}, msg)$ and $\boldsymbol{z} := \boldsymbol{y} + \mathbf{S}\boldsymbol{c}$ and it outputs $(\boldsymbol{z}, \boldsymbol{c})$ as the signature on message msg.

Verification. On input the verification key vk, message msg, and a purported signature (z, c), algorithm Sig.Verify(vk, msg, $(\boldsymbol{z}, \boldsymbol{c})$) checks if $\|\boldsymbol{z}\| \leq (\sigma + \alpha d)\sqrt{m}$ and $\mathsf{H}(\mathbf{A}\boldsymbol{z} - \mathbf{T}\boldsymbol{c}, msg) = \boldsymbol{c}$. If both conditions are true, it outputs 1 (accept). Otherwise, it outputs 0 (reject).

We now describe the construction of (Agrawal et al., 2021). In the following, let $\mathbf{G}$ denote the gadget matrix, i.e., $\mathbf{G} \coloneqq \left(1,\ 2,\ 2^2, \ldots, 2^{\log(q)-1}\right)^T \otimes \mathbf{I}_n$ for given parameters q, n, where $\mathbf{I}_n$ denotes the $n \times n$ identity matrix and $\otimes$ denotes their tensor product. The blind signature scheme requires the following cryptographic blocks:

- a hash function $\mathsf{H}: \{0,1\}^* \to \mathbb{C}$ be a hash function modelled as a random oracle,
- a signature scheme Sig = (Sig.KeyGen, Sig.Sign, Sig.Verify) that can be used within an HE scheme (instantiated with the rejection-free variant presented above).

- zero-knowledge proofs of knowledge (ZKPoK) for exact linear relations with small coefficients, i.e., for the existence of a vector $\boldsymbol{v}$ such that $\boldsymbol{v}$ has low Euclidean norm and $\mathbf{A}\boldsymbol{v} = \boldsymbol{b} \pmod{q}$ for some public $(\mathbf{A}, \boldsymbol{b}, q)$.

Key Generation. On input the security parameter λ, algorithm KeyGen(1^λ) generates the keys by invoking the digital signature's key generation algorithm (Sig.sk, Sig.vk) ← Sig.KeyGen(1^λ). It outputs (sk, pk) := (Sig.sk, Sig.vk).

Signing. The interactive signing protocol <S(sk), U(pk, msg)>, where $msg \in \{0,1\}$, works as follows:

1. **User**:
   - The user samples $\boldsymbol{s}^* \leftarrow_\$ \mathbb{Z}_q^{n-1}$, $\boldsymbol{e} \leftarrow_\$ D_{\mathbb{Z}^m,a}$ and computes $\mathbf{A}$ =H(pk, id) using a user identifier id, $\boldsymbol{s} := (-\boldsymbol{s}^*, 1) \in \mathbb{Z}_q^n$ and $\mathbf{A}^* := \left(\mathbf{A}, \boldsymbol{s}^{*T}\mathbf{A} + \boldsymbol{e}^T\right)^T$. It sets HE.SK := $\boldsymbol{s}$ and HE.PK := $\mathbf{A}^*$.
   - The user encrypts $msg \in \{0,1\}$ using PK. This is done by sampling a matrix $\mathbf{R} \leftarrow_\$ \{0, \pm 1\}^{m \times m}$, and then computing $\mathbf{C} := \mathbf{A}^*\mathbf{R} + b\mathbf{G} \in \mathbb{Z}_q^{m \times n}$. It sets $CT_{msg} := \mathbf{C}$ as the ciphertext. Notice that the last column of $\boldsymbol{s}^T\mathbf{C} = \boldsymbol{e}^T\mathbf{R} + b\boldsymbol{s}^T\mathbf{G}$ is close to $bq/2$.
   - The user generates ZKPoKπ_{SK} and π_{CT} proving that its public key and ciphertext are well-formed. In particular, π_{SK} proves knowledge of a short vector $(\boldsymbol{x}, \boldsymbol{y})$ s.t. the last row of $\mathbf{A}^*$ has the form $\boldsymbol{x}^T\mathbf{A} + \boldsymbol{y}$, while π_{CT} proves that $CT_{msg} = \mathbf{A}^*\mathbf{R} + b\mathbf{G}$, for a low-norm matrix $\mathbf{R}$ and $b \in \{0,1\}$.
   - It sends (PK, π_{SK}, CT_{msg}, π_{CT}) to the signer.
2. **Signer**:
   - The signer receives (PK, π_{SK}, CT_{msg}, π_{CT}) and it verifies the validity of both π_{SK} and π_{CT}. If either proof is invalid, it outputs $\perp$.
   - It homomorphically evaluates the digital signature's signing algorithm (viewed as a circuit) on the encrypted message by computing $CT_\sigma :=$ HE.Eval(Sig.Sign$_{sk}$, CT_{msg}).
   - It sends CT_σ back to the user.
3. **User**: The user decrypts ciphertext CT_σ using its secret key SK. This is done by computing the inner product of $\boldsymbol{s}^T$ and the last column of CT_σ. If the norm of the result is smaller than $q/4$, it outputs 0. Otherwise, itoutputs 1.

Verification. Verification is performed identically to Sig.Verify.

4.2.2. Proved Security Results

Under the assumption that the ZKPoK systems underlying the scheme's instantiation are correct, the scheme of (Agrawal et al., 2021) is also correct:

Lemma 17. (from (Agrawal et al., 2021)) If the ZKPoK proof systems π_{SK}

and π_{CT} are correct, HE.Eval and HE.Dec are correct, and Sig.Verify are correct, then the construction of (Agrawal et al., 2021) is also correct.

Furthermore, the zero-knowledge property implies blindness for the scheme:

Lemma 18. (Theorem 6.3 in (Agrawal et al., 2021)) If the underlying proof systems are ZKPoK, then the construction of (Agrawal et al., 2021) is blind against honest-signers.

Finally, unforgeability is derived from the UF-CMA security of the rejection-free variant of Lyubashevsky's signature.

Lemma 19. (Theorem 6.4 in (Agrawal et al., 2021)) If the underlying digital signature scheme is unforgeable against chosen-message attacks (UF-CMA secure), then the construction of (Agrawal et al., 2021) is one-more unforgeable.

4.2.3. Discussion on Agrawal et al.'s Blind Signature Scheme

What is notable about the construction of (Agrawal et al., 2021) is its reliance on heavy machinery such as Non-Interactive Zero-Knowledge (NIZK) proofs and homomorphic encryption schemes that are capable of evaluating a random oracle homomorphically. In particular, while this construction shows great promise for practical use, there are several serious roadblocks barring implementation. First, by design, the signing algorithm $\text{Sig.Sign}_{\text{Sig.sk}}$ acts as a circuit on which the ciphertext must be homomorphically evaluated by the signer. However, $\text{Sig.Sign}_{\text{Sig.sk}}$ internally uses a hash function modeled as a random oracle and as such, this hash function must also be evaluated homomorphically. Unfortunately, choosing such a hash function is a highly non-trivial matter which to the best of our knowledge is still a major open problem. Second, the homomorphic encryption scheme itself needs to be chosen carefully and in a way capable of handling the diverse formats involved during the homomorphic signing. Ensuring compatibility between the homomorphic encryption format and the format needed for evaluating the hash function seems particularly tricky to ensure when instantiating Sig.Sign with their proposed abort-free variant of Dilithium-G's signing algorithm[6]. Finally, Dilithium-G compresses the signature elements with Huffman codes. However, in (Agrawal et al., 2021) this will need to be done under the homomorphic encryption layer, which could be expensive to implement. Addressing all of these issues simultaneously is particularly tricky and could lead to insecure implementations.

5. Impossibility Results

An important consideration to take into account when designing blind signature schemes are impossibility results. These typically state that under certain conditions, reductions to underlying cryptographic problems do not provide a meaningful security statement. In other words, if such a reduction exists, then the underlying problem is already easy. In this section, we review these results and how they impact the lattice-based constructions covered in this survey.

The first result that we examine is proven by (Katz et al., 2011). The authors prove that blind signature schemes are impossible to construct from one-way permutations, even in the ROM.

Theorem 1. (Theorem 1 from (Katz et al., 2011)) There is no black-box construction of blind signature schemes from one-way functions.

While it is currently unknown whether one-way permutations can even be constructed from the LWE problem, all of the constructions considered in this paper circumvent this result by relying on the (stronger) collision-resistance property of R − SIS (or Ring *k*-SIS in the case of (Ermann et al., 2020)).

The second result by (Baldimtsi and Lysyanskaya, 2013) states that Schnorr-type blind signatures are impossible to construct when unforgeability is based on a one-witness hard problem. In the context of lattice-based schemes, this rules out any hopes of designing a blind signature scheme based solely on the LWE problem. No constructions exist whose unforgeability relies solely on LWE. All of the constructions considered in this survey avoid this kind of impossibility result by relying on a multi-witness problem (namely, SIS or Ring k-SIS). Interestingly, an earlier version of BLAZE (Alkadri, 2019) managed to avoid this kind of impossibility result by taking a "hybrid" approach akin to (Ducas et al., 2018). In particular, it bases key-secrecy on the hardness of LWE (i.e., a one-witness problem), and unforgeability on SIS (i.e., a multi-witness problem). Unfortunately, (Alkadri, 2019) then attempts to simulate the signer without the secret key which exposes it to universal forgeability (Pointcheval and Stern, 2000).

The final result by (Fischlin and Schröder, 2010) provides a resetting metareduction (i.e., a reduction against another reduction) which rules out the possibility of constructing secure schemes with at most three moves, statistical blindness, and which have statistical signature-derivation checks (i.e., one can verify from the protocol transcript between a signer and an honest user if the user was able to obtain a valid signature from the interaction). While this immediately rules out any blind signature schemes in the standard model with

Table 7: Summary of all lattice-based blind signature schemes in the literature and their adherence to impossibility results

Proposal	(Baldimtsi and Lysyanskaya, 2013)	(Katz et al., 2011)	(Fischlin and Schröder, 2010)	Incorrect use of the Forking Lemma
(Ruckert, 2010)	–	–	–	✓
BLAZE (Alkadri et al., 2020a)	–	–	–	✓
3-move BLAZE+ (Alkadri et al., 2020b)	–	–	–	✓
4-move BLAZE+ (Alkadri et al., 2020b)	–	–	–	✓
(Ermann et al., 2020)	–	–	–	✓
(Hauck et al., 2020)	–	–	–	–
(Agrawal et al., 2021)	–	–	–	–

at most 3 moves, it does not capture direct constructions of lattice-based blind signatures proven secure in the ROM. In general, the impossibility results of (Fischlin and Schröder, 2010) are typically circumvented by using complexity leveraging (Döttling et al., 2017; Schröder and Unruh, 2011) or by using a common reference string (Fischlin, 2006).

Theorem 2. (Theorem 2 from (Fischlin and Schröder, 2010)) Let BS be a three-move blind signature scheme, which is statistically blind and has statistical signature-derivation checks. Then there is no resetting (with restricted cross-resets) black-box reduction from unforgeability of the blind signature scheme BS to a hard non-interactive problem.

All of the constructions considered in this paper circumvent this result by using a programmable random oracle. Table 7 summarizes the above observations.

6. Comparison with Other Post-Quantum Proposals

In this section, we review the concrete sizes of keys, produced signatures and total communication for each of the schemes discussed in Sections 3 and 4. In addition, we compare them to other post-quantum proposals in the literature

Table 8: Summary of post-quantum blind signature schemes in the literature. We denote unspecified sizes with a dash

Proposal	Hardness assumption(s)	Bit security	sk size	pk size	Signature size	Total communication
Flawed Lattice-Based Blind Signature Schemes						
(Ruckert et al., 2010)	R-SIS	102	23.6 KB	23.6 KB	89.4 KB	119.1 KB
BLAZE (Alkadri et al., 2019, 2020a)	R-SIS	≈ 128	0.8 KB	3.9 KB	6.6 KB	351.6 KB
3-move BLAZE+ (Alkadri et al., 2020b)	R-SIS	≈ 128	0.75 KB	3.9 KB	6.7 KB	177.8 KB
4-move BLAZE+ (Alkadri et al., 2020b)	R-SIS	≈ 128	0.75 KB	3.9 KB	6.7 KB	≈ 265 KB
Ermann et al. (Ermann et al., 2020)	Ring k – SIS	100	5.86 MB	852 KB	868 KB	–
Provably secure Lattice-Based Blind Signature Schemes						
(Hauck et al., 2020)	R-SIS	128	4.15 MB	0.4 MB	7.73 MB	33.3 MB
(Agrawal et al., 2021)	R – LWE & R – SIS	128	–	< 2 KB	< 3 KB	–
Other Post-Quantum Blind Signature Schemes						
(Petzoldt et al., 2017)	Rainbow	128	70.2 KB	106.8 KB	28.5 KB	–
(Blazy et al., 2017)	CFS & Syndrome Decoding	100	–	15 KB	200 KB	–

[1] For more formal definitions, we refer the reader to (Fischlin and Schröder, 2009).
[2] The recent work of (Hauck et al., 2019) formalizes this pattern but only for hash functions with negligible enclosedness errors.
[3] These parameters are globally known and implicit inputs to all other algorithms.
[4] Here, the signer essentially samples with fixed random coins.
[5] This occurs with probability $2^{-\lambda}$.
[6] A Fisher-Yates shuffle no longer works for mapping to Dilithium-G's challenge space because this task must be done homomorphically.

(namely, code-based, and multivariate cryptography). Table 8 summarizes the aforementioned sizes per scheme, also listing the underlying (post-quantum) hardness assumption per schemes, as well as the estimated bit security level.

References

Abe, M., Okamoto, T. (2000). 'Provably Secure Partially Blind Signatures'. Advances in Cryptology – CRYPTO 2000, pp. 271–286.

Agrawal, S., Stehle, D., and Yadav, A. (2021). 'Towards practical and round-optimal lattice-based threshold and blind signatures'. CryptologyePrintArchive, Report 2021/381, 2021. Availableat: https://ia.cr/2021/381.

Ajtai, M. (1996). 'Generating hard instances of lattice problems (extended abstract)'. Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC '96, pp. 99–108.

Alkadri, N. A., El Bansarkhani, R., and Buchmann, J. (2019). 'Blaze: Practical lattice-based blind signatures for privacy-preserving applications'. CryptologyePrintArchive, Report 2019/1167, 2019. Availableat: https://ia.cr/2019/1167.

Alkadri, N. A., El Bansarkhani, R., and Buchmann, J. (2020). 'Blaze: Practical lattice-based blind signatures for privacy-preserving applications'. FinancialCryptography and DataSecurity, pp. 484–502.

Alkadri, N. A., El Bansarkhani, R., and Buchmann, J. (2020). 'On lattice-based interactive protocols: An approach with less or no aborts'. Information Security and Privacy, pp. 41–61.

Baldimtsi, F., and Lysyanskaya, A. (2013). 'Anonymous credentials light'. CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pp. 1087–1098.

Baldimtsi, F., and Lysyanskaya, A. (2013). 'On the security of one-witness blind signature schemes'. Advances in Cryptology - ASIACRYPT 2013, pp. 82–99.

Bellare, M., and Neven, G. (2006). 'Multi-signatures in the plain publickey model and a general forking lemma'. Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS '06, pp. 390–399.

Blazy, O., Gaborit, P., Schrek, J., and Sendrier, N. (2017). 'A code-based blind signature'. 2017 IEEE International Symposium on Information Theory (ISIT), pp. 2718–2722.

Boneh, D., and Freeman, D. M. (2011). 'Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures'. Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography, PKC '11, pp. 1–16.

Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry,

M. (2011). 'Random Oracles in a Quantum World'. Advances in Cryptology – ASIACRYPT 2011, pp. 41–69.

Bouaziz-Ermann, S., Canard, S., Eberhart, G., Kaim, G., Roux-Langlois, A., and Traoré, J. (2020). 'Lattice-based (partially) blind signature without restart'. Cryptology ePrint Archive, Report 2020/260, 2020. Availableat: https://eprint.iacr.org/2020/260.

Camenisch, J. L., Piveteau, J. M., and Stadler, M. A. (1994). 'Blind signatures based on the discrete logarithm problem'. Advances in Cryptology – EUROCRYPT '94, pp. 428–432.

Carlsson, B. (2004). 'The digital economy: what is new and what is not?'. StructuralChange and Economic Dynamics, 15 (3), pp. 245–264.

Chaum, D. (1983). 'Blind signatures for untraceable payments'. In Advances in Cryptology, pp. 199–203.

Chaum, D. (1984). 'Blind Signature System'. Advances in Cryptology, pp. 153–153.

Chaum, D. (1988). 'Blinding for unanticipated signatures'. Advances in Cryptology – EUROCRYPT ' 87, pp. 227–233.

Cheon, J. H., Jeong, J. H., and Shin, J. S. (2019). 'Cryptoanalysis on ´a round-optimal lattice-based blind signature scheme for cloud services´'. FutureGeneration Computer Systems, 95, pp. 100–103.

Cormen, T. H., Leiserson, C. E, Rivest, R. L., and Stein, C. (2009). Introduction to Algorithms. (3rd ed). United States: The MIT Press.

Döttling, N., Fleischhacker, N., Krupp, J.,, and Schröder, D. (2017). 'Two-message, oblivious evaluation of cryptographic functionalities'. Cryptology ePrint Archive. Availableat: https://ia.cr/2017/958.

Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and Stehle, D (2017). 'Crystals – dilithium: Digital signatures from module lattices'. IACR Cryptology ePrint Archive. Availableat: https://ia.cr/2017/633.

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and Stehle, D (2018). 'Crystals-dilithium: A lattice-based digital signature scheme'. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018 (1), pp. 238–268.

EC (n.d.). Digital Single Market, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32006L0123 [Accessed: 2021-12-02]

Fan, C., and Lei, C. (1998). 'User efficient blind signatures'. Electronics Letters, 34 (6), pp. 544–546.

Fischlin, M. (2006). 'Round-optimal composable blind signatures in the common reference string model'. Proceedings of the 26th Annual International Conference on Advances in Cryptology, CRYPTO '06, 4117, pp. 60–77.

Fischlin, M., and Schröder, D. (2009). 'Security of blind signatures under aborts'. PublicKeyCryptography – PKC 2009, 5443, pp. 297–316.

Fischlin, M., and Schröder, D. (2010). 'On the impossibility of three-move blind signature schemes'. Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques, EUROCRYPT '10, pp. 197–215.

Gao, W., Hu, Y., Wang, B., Xie, J., and Liu, M. (2017). 'Identity-based blind signature from lattices'. WuhanUniversity Journal of NaturalSciences, 22 (4), pp. 355–360.

Garg, S., Rao, V., Sahai, A., Schröder, D., and Unruh, D. (2011). 'Roundoptimalblindsignatures'. Advances in Cryptology – CRYPTO 2011, pp. 630–648.

Hauck, E., Kiltz, E., and Loss, J. (2019). 'A modular treatment of blind signatures from identification schemes'. Advances in Cryptology – EUROCRYPT 2019, pp. 345–375.

Hauck, E., Kiltz, E., Loss, J., and Nguyen, N. K. (2020). 'Lattice-based blind signatures, revisited'. Advances in Cryptology – CRYPTO 2020, pp. 500–529.

Heilman, E., Baldimtsi, F., and Goldberg, S. (2016). 'Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions'. CryptologyePrintArchive, Report 2016/056, 2016. Availableat: https://ia.cr/2016/056.

Juels, A., Luby, M., and Ostrovsky, R. (1997). 'Security of blind digital signatures'. Advances in Cryptology – CRYPTO '97, pp. 150–164.

Katz, J., Loss, J., and Rosenberg, M. (2021). 'Boosting the security of blind signature schemes'. Advances in Cryptology – ASIACRYPT 2021, pp. 468–492.

Katz, J., Schröder, D., and Yerukhimovich, A. (2011). 'Impossibility of blind signatures from one-way permutations'. Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, pp. 615–629.

Kumar, M., Katti, C. P., and Saxena, P. C. (2017). 'A secure anonymous e-voting system using identity-based blind signature scheme'. Information Systems Security, pp. 29–49.

Langlois, A., and Stehle, D. (2015). 'Worst-case to average-case reductions for module lattices'. Designs, Codes and Cryptography, 75 (3).

Liang, C., Yongquan, C., Xueming, T., Dongping, H., and Xin, W. (2011). 'Hierarchical id-based blind signature from lattices'. In 2011 Seventh International Conference on Computational Intelligence and Security, pp. 803–807.

Lyubashevsky, V. (2009). 'Fiat-shamir with aborts: Applications to lattice and factoring-based signatures'. Advances in Cryptology – ASIACRYPT 2009, pp. 598-616.

Lyubashevsky, V. (2012). 'Lattice signatures without trapdoors'. Advances in Cryptology – EUROCRYPT 2012, pp. 738-755.

Lyubashevsky, V., and Micciancio, D. (2006). 'Generalized compact knapsacks are collision resistant'. Automata, Languages and Programming, pp. 144-155.

Micciancio, D., and Peikert, C. (2012). 'Trapdoors for lattices: Simpler, tighter, faster, smaller'. Advances in Cryptology – EUROCRYPT 2012, pp. 700–718.

Micciancio, D., and Regev, O. (2007). 'Worst-case to average-case reductions based on gaussian measures'. SIAM Journal on Computing, pp. 372-381.

NIST. (n.d.). Post-Quantum Cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions [Accessed: 2021-12-02]

Nyberg, K., and Rueppel, R. A. (1993). 'A new signature scheme based on the dsa giving message recovery'. Proceedings of the 1st ACM Conference on Computer and Communications Security, CCS '93, pp. 58–61.

Okamoto, T. (1992). 'Provably secure and practical identification schemes and corresponding signature schemes'. Advances in Cryptology — CRYPTO' 92, pp. 31–53.

Papachristoudis, D., Hristu-Varsakelis, D., Baldimtsi, F., and Stephanides, G. (2019). 'Leakage-resilient lattice-based partially blind signatures'. IET Information Security, 13 (6), pp. 670–684.

Paquin, C., and Zaverucha, G. (2013). 'U-prove cryptographic specification v1.1 (revision 3)'. Technical report, Microsoft Corporation.

Peikert, C. (2009). 'Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract'. Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, STOC '09, pp. 333–342.

Peikert, C., and Rosen, A. (2006). 'Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices'. TCC'06: Proceedings of the Third conference on Theory of Cryptography, pp. 145–166.

Petzoldt, A., Szepieniec, A., and Mohamed, M. S. E. (2017). 'A practical multivariate blind signature scheme'. FinancialCryptography and DataSecurity, pp. 437–454.

Pointcheval, D. (1998). 'Strengthened security for blind signatures'. Advances in Cryptology – EUROCRYPT '98, pp. 391– 405.

Pointcheval, D., and Stern, J. (1996). 'Provably secure blind signature schemes'. Advances in Cryptology – ASIACRYPT '96, pp. 252–265.

Pointcheval, D., and Stern, J. (1997). 'New blind signatures equivalent to

factorization (extended abstract)'. Proceedings of the 4th ACM Conference on Computer and Communications Security, CCS '97, pp. 92–99.
Pointcheval, D., and Stern, J. (2000). 'Security arguments for digital signatures and blind signatures'. Journal of Cryptology, 13 (3), pp. 361–396.
Regev, O. (2005). 'On lattices, learning with errors, random linear codes, and cryptography'. Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing, STOC '05, pp. 84–93.
Rückert, M. (2010). 'Lattice-based blind signatures'. Advances in Cryptology - ASIACRYPT 2010, pp. 413–430.
Schnorr, C. P. (1989). 'Efficient identification and signatures for smart cards'. Advances in Cryptology – CRYPTO' 89 Proceedings, pp. 239–252.
Schnorr, C. P. (2001). 'Security of blind discrete log signatures against interactive attacks'. Proceedings of the Third International Conference on Information and Communications Security, ICICS '01, pp. 1–12.
Schröder, D., and Unruh, D. (2011). 'Round optimal blind signatures'. IACR Cryptology ePrint Archive. Availableat: https://ia.cr/2011/264.
Shor, P. W. (1997). 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer'. SIAM Journal on Computing, 26 (5), pp. 1484–1509.
Stadler, M., Piveteau, J. M., Camenisch, J. (1995). 'Fair Blind Signatures'. Advances in Cryptology – EUROCRYPT '95, pp. 209–219.
Statista. (n.d.). Number of cryptocurrencies worldwide from 2013 to November 2021. https://www.statista.com/statistics/863917/number-crypto-coins-tokens [Accessed: 2021-12-02]
Zhang, L., and Ma, Y. (2014). 'A lattice-based identity-based proxy blind signature scheme in the standard model'. MathematicalProblems in Engineering, 2014 (1).
Zhang, R., Zhang, Y., and Ren, K. (2012). 'Distributed privacy-preserving access control in sensor networks'. IEEE Transactions on Parallel and Distributed Systems, 23 (8), pp. 1427–1438.
Zhang, Y (2016). 'Forward-secure identity-based shorter blind signature from lattices'. American Journal of Networks and Communications, 5 (1), pp. 1–17
Zhu, H., Tan, Y., Zhang, X., Zhu, L., Zhang, C., and Zheng, J. (2017). 'A round-optimal lattice-based blind signature scheme for cloud services'. FutureGeneration Computer Systems, 73 (C), pp. 106–114.

THE CENTRAL ROLE OF TRUST IN INTERNATIONAL BUSINESS RESEARCH OVER THE 2017-2021 PERIOD

N. SKLAVOUNOS*

Abstract

The growing number of theoretical and empirical research papers on trust in international business literature shows that trust is considered as one of the most significant concepts that affect the success of various forms of business collaborations such as international strategic alliances (ISAs) and international joint ventures (IJVs). This paper includes a detailed review of the literature over the 2017-2021 period in regards to the key role of trust in ISAs and IJVs with reference to the related theoretical models, empirical findings and managerial implications. The paper ends with the conclusions and suggestions for future research.

JEL Classification: M16 International Business Administration

Keywords: Trust, International business (IB), International strategic alliances (ISAs), International joint ventures (IJVs)

1. Introduction

The recognition of the significant role of trust by scholars and practitioners in international business (IB) collaborations has grown substantially in recent years (Bijlsma-Frankema et al., 2008). Trust is a highly abstract and multidimensional concept that has been adopted from numerous scientific disciplines. Lascaux (2020) argue that trust is the most crucial lever to build collaborative relationships. Sklavounos et al. (2018, p. 205) define trust as "*a firm's willingness to depend on its international strategic alliance partner based on the positive expectations of the partner's reliability, fairness and goodwill*". The purpose of this paper is to present some contemporary research articles over the 2017 – 2021 period that involve trust in international inter-firm collaborations in order to highlight its ongoing significance in the field of IB.

2. Latest Research Findings on Trust IB literature

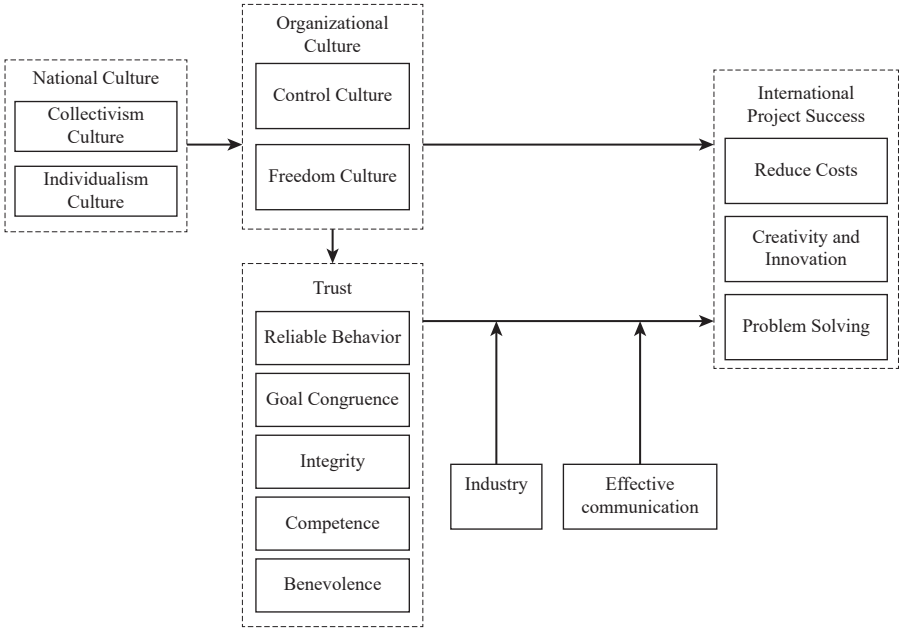
In this review, details from research papers only of the last five years are

* Adjunct Lecturer, Department of Accounting and Information Systems, International Hellenic University, Thessaloniki, Greece, e-mail: sklavounosnikos@yahoo.gr, sklavou@uom.edu.gr

presented in order to highlight the most contemporary findings of IB literature about the concept of trust. First, Ajmal et al. (2017) aim to draw attention toward how the process of trust development is affected in global business environments where an increasing number of International Joint Ventures (IJVs) and International Strategic Alliances (ISAs) are established. The researchers attempt to answer how national and organizational cultures impact the trust-building process in global business environments by proposing a conceptual framework. More specifically, based on prior research findings, Ajmal et al. (2017) develop a cultural effect model to show how culture impacts the development of trust in global projects and what actions should be taken to create trust among culturally diverse stakeholders (See Figure 1). The researchers believe that all these factors contribute to trust-building between the project and stakeholders in an environment with cultural similarities and create an optimistic atmosphere in which more efficient project execution is established.

The theoretical study of Ajmal et al. (2017) shows that cultural differences

Figure 1: Ajmal et al. (2017) Research Model



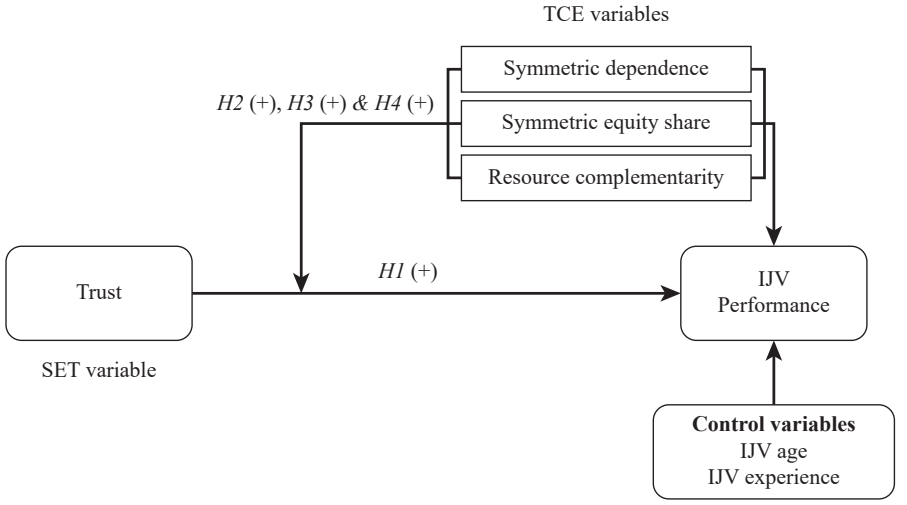
Source: Ajmal et al. (2017, p. 1109)

among project teams can lead to conflict, misunderstanding, and can negatively affect project performance. Their findings reveal that culture is a key factor in trust-building among international project stakeholders since trust is vital to develop an effective long-term business relationship.

Moreover, Ali and Khalid (2017) adopt a transaction cost approach and investigate the relationship between trust and performance in IJVs with the moderating effects of three structural mechanisms of IJVs (symmetric dependence, symmetric equity share and resource complementarity) on the trust-performance relationship. Their model examines the direct relationship between trust and performance through the moderating influence of the above-mentioned structural mechanisms. Their study contributes on previous research by empirically testing the moderating nature of three structural mechanisms on the trust-performance relationship in IJVs. Their theoretical model is depicted in Figure 2.

The majority of prior IB literature concludes that trust always enhances IJV performance. However, some scholars identify that the relationship between trust and IJV performance is dependent on other factors (Krishnan et al., 2006; Robson et al., 2008; Silva et al., 2012). In their study, Ali and Khalid (2017) suppose that the positive relationship between trust and performance should

Figure 2: Ali and Khalid (2017) Research Model



Source: Ali and Khalid (2017, p. 965).

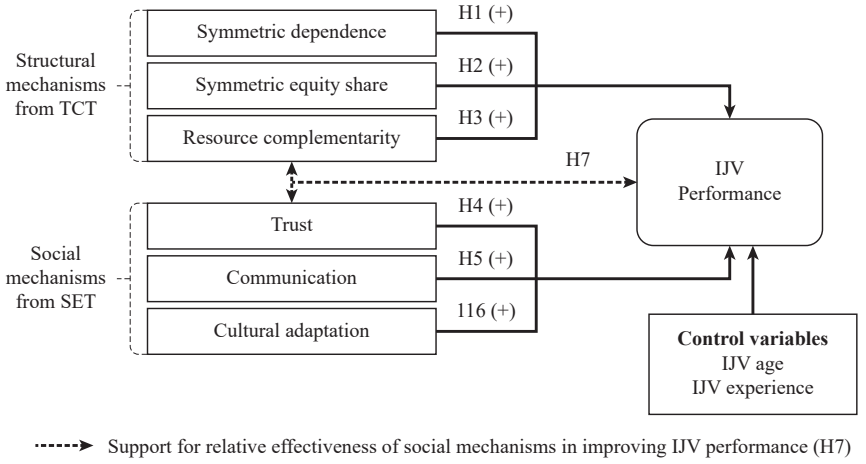
be contingent on the structural mechanisms of the IJV that limits the extent to which the trusted party can be opportunistic. Their sample consists of 89 Nordic IJVs in Asia, Europe and America and their results show that symmetric dependence between IJV partners increases the positive impact of trust on IJV performance, thus providing empirical support to previous theoretical studies (Hennart & Zeng, 2005). Moreover, their results do not support the moderating role of symmetric equity share on the positive effect of trust on IJV performance, but reveal that trust can improve IJV performance regardless of the equity structure. Finally, Ali and Khalid's (2017) findings confirm that resource complementarity improves the positive impact of trust on IJV performance. This result is in line with prior research (Madhok, 1995; Ali & Larimo, 2016) which supports the positive effect of resource complementarity on the performance of the IJV.

The same researchers with the use of the same sample of 89 Nordic IJVs joined forces with two other scholars from the University of Vaasa and published another interesting study in 2021. More specifically, Ali et al. (2021) aim to gain a broader understanding of IJV management mechanisms that improve performance by integrating elements from the Transaction Cost Theory (TCT) and the Social Exchange Theory (SET) and they investigate which theoretical view is more effective in improving IJV performance.

Ali et al.'s (2021) study contributes to IB literature by developing and empirically examining an integrated framework of enhancing IJV performance, which includes both structural and social mechanisms of IJV management. Their proposed research model includes three structural mechanisms from the TCT and three social mechanisms from the SET. The TCT based structural mechanisms are symmetric dependence, symmetric equity share and resource complementarity, while the SET based social mechanisms are trust, communication and cultural adaptation. The model suggests a positive relationship of TCT and SET mechanisms with IJV performance and is illustrated in Figure 3.

According to Ali et al. (2021), social mechanisms, such as trust, aid IJV partners to effectively share information and knowledge, endure environmental uncertainties, mutually address any problems that may arise and eventually enhance IJV performance. Companies allocate more resources in developing structural mechanisms to protect their interests in an IJV, with the hope that these mechanisms will also improve IJV performance. However, some cultures are more relationship oriented than structural oriented and do business based on relationships, which eventually improve performance (Cavusgil et al., 2013). Ali et al.'s (2021) sample consists mainly from Asian firms that

Figure 3: Ali et al. (2021) Research Model



Source: Ali et al. (2021, p. 5)

had formed IJVs with Nordic European partners. Managers from these cultures give more attention to social mechanisms, as both cultures recognize the importance of tradition, values and relationship building among partners (Ghauri & Usunier, 2003).

Another interesting study is the one of Balboni et al. (2018) who use a sample of 138 ISAs involving Italian firms and foreign partners in order to investigate the existing debate in IB literature in regards to the substitutive or complementary nature of the relationship between inter-organizational trust and formal control as governance mechanisms and how they affect ISA performance. More specifically, according to the substitute view (Gulati, 1995; Dyer & Singh, 1998), control and trust are antagonistic governance mechanisms: the use of one reduces or avoids the use of the other and vice versa, while their coexistence does not guarantee ISA success (Li et al., 2010). On the contrary, according to the complementary view (Poppo & Zenger, 2002; Liu et al., 2009), trust and control are regarded as mutually reinforcing mechanisms: trust makes partners to reduce their reluctance toward control mechanisms (Das and Teng, 2001), while formal control, can support the formation of trust-based governance by reducing the risks of opportunistic behavior (Poppo & Zenger, 2002). Balboni et al. (2018) attempt to reconcile these divergent

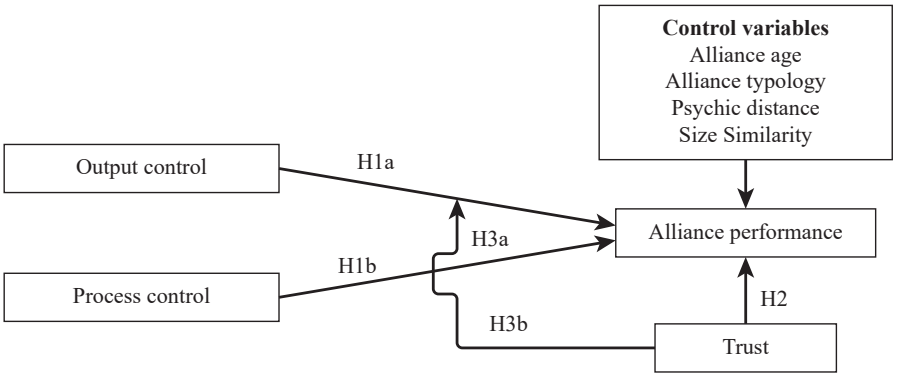
'complements–substitutes' views. In particular, their study contributes to the existing debate over the substitutive or complementary nature of the trust–formal control relationship by suggesting that trust is a moderator of the direct relationship between the two types of control mechanisms and alliance performance, a relationship that has been proposed at a theoretical level (Das & Teng, 1998), but has been poorly tested empirically (Mellewigt et al., 2007). The theoretical model of Balboni et al. (2018) is illustrated in Figure 4.

Based on a multidimensional view of formal control (Chen et al., 2009), Balboni et al.'s (2018) results show that the multidimensional nature of formal control needs to be further explored in ISA research (Li et al., 2010). Their results offer empirical evidence that the linkages between ISA performance and control governance mechanisms are affected by the nature of the formal control mechanisms, output and process control. By controlling for the possible different impacts of the two mechanisms, their results highlight the significance of distinguishing the different roles played by output and process control in predicting cross-border alliance performance. Actually, alliance performance is positively affected only by output control, while process control has no impact. As far as the joint impact is concerned, Balboni et al.'s (2018) results confirm the predicting role of inter-organizational trust in leveraging ISA performance (Silva et al., 2012) and suggest that trust may overrule formal control mechanisms in improving ISA performance (Liu et al., 2009).

Balboni et al. (2018) conclude that the two views (substitute – complementary) should be regarded not as competitive, but as coexisting (Huber et al., 2013) and empirically show that the moderating effect of trust varies according to the specific nature of the control mechanisms in use (Malhotra & Lumineau, 2011). In fact, they have found a negative interaction between output control and trust on ISA performance and a positive interaction between process control and trust on ISA performance. Overall, their results suggest that the moderating effect of trust should be interpreted by bearing in mind the specific stage of the alliance life-cycle (Cao & Lumineau, 2015).

Furthermore, Jha et al. (2019) constructed 315 country pairs from a set of 26 countries, over the period from 1996 to 2004 and gathered a total number of 16,196 ISAs in order to investigate whether four macro variables (i.e. trust and cultural, institutional, and geographical distances) that impact ISA success also impact the propensity to form one. The four variables that they examine are trust and cultural, institutional, and geographical distances. Their findings show that when trust is high, the number of ISAs is larger. They also found that cultural distance decreases the propensity to form an alliance and that geographical distance remains a key factor. However, they did not find that the

Figure 4: Balboni et al. (2018) Research Model



Source: Balboni et al. (2018, p. 547)

institutional distance has a significant impact. In addition, they show that trust mitigates the adverse impact of geographical distance, but cultural familiarity does not. This finding is in line with the idea that while trust can reduce the fear of a partner's opportunism, the cultural familiarity cannot.

Jha et al.'s (2019) study contribute to IB literature by extending prior research that suggests cultural familiarity and trust facilitate ISA formation (Ahern et al., 2015; Bryan et al., 2015; Shi & Tang, 2015) and that greater geographical distance deters it (Disdier & Head, 2008; Mian, 2006). They also show that macro level trust can mitigate some of the adverse impact of geographical distance, but cultural familiarity cannot. This second finding raises the possibility that trust might have such an impact on foreign direct investment (FDI) and international trade as well. Moreover, Jha et al. (2019) found that in country pairs where both countries have poor quality institutions, institutional distance does not have an impact on the propensity to form an ISA. This finding indicates that the impression that the poor institution countries might prefer other poor institution countries because they find it easier to navigate the system might be over stated. This latter finding also constitutes a useful implication for scholars who investigate the effect of institutional distance on FDI and trade.

The final study of this review is the one of Guo et al. (2020) who conduct a survey of 302 Chinese firms in order to examine the effects of two fundamental control mechanisms (trust and formal contracts) on the ambidexterity

dimension in strategic alliances. The researchers note that there is a lack of research focusing on both knowledge sharing and knowledge protection (Yang et al., 2014) that limits our understanding of how the simultaneous adoption of knowledge sharing and protection affects firm and innovation performance. Additionally, prior research has proposed two types of control mechanisms for organizing inter-firm knowledge flow: trust and formal contracts (Cao & Lumineau, 2015). Since most companies use both these control mechanisms at the same time, debate has arisen regarding their joint impacts on strategic alliances (Li et al., 2010). On one side of the debate, the interplay between the two control mechanisms is considered as valuable for firms (Li et al., 2010). On the other side, the same interplay is regarded as detrimental for firms (Wang et al., 2011; Jiang et al., 2013). Despite this lack of agreement, the IB literature has sustained a focus on the direct relationship between performance and joint use of the two control mechanisms (Cao & Lumineau, 2015). Hence, questions of how trust and formal contracts interact with each other, and how they impact the simultaneous application of knowledge sharing and knowledge protection remain unanswered.

To address these research gaps, Guo et al. (2020) introduce the concept of ambidexterity, a state in which the focal firm has achieved high levels of knowledge sharing and knowledge protection at the same time (Yang et al., 2014). They investigate how a firm in the Chinese market can apply knowledge sharing and knowledge protection at the same time to new product development while also using trust and formal contracts to create ambidexterity. Their findings show that ambidexterity in knowledge sharing and protection facilitates the focal firm's new product development and that trust has an inverted U-shaped relationship with the ambidexterity dimension. In addition, Guo et al.'s (2020) results indicate that formal contracts negatively affect the ambidexterity dimension and that the interaction of the two control mechanisms is damaging to ambidexterity. These results challenge prior studies that have considered trust and formal contracts as always beneficial in strategic alliances, especially in the Chinese context (Wang et al., 2011). Guo et al.'s (2020) findings indicate that the interaction of trust and formal contracts can expose a firm to risk by inhibiting it from applying knowledge sharing and knowledge protection mechanisms at the same time. Finally, the results of Guo et al. (2020) highlight the positive role of trust compared to formal contracts in managing knowledge sharing and knowledge protection simultaneously. Thus, firms need to maintain a moderate level of trust to take full advantage of its impacts on the ambidexterity dimension.

3. Conclusions and objectives for further research

This paper contains an in-depth review of the most recent IB literature about the central role of trust in ISAs and IJVs. The main body of the paper includes details from the contemporary studies of Ajmal et al. (2017), Ali and Khalid (2017), Balboni et al. (2018), Jha et al. (2019), Guo et al. (2020) and Ali et al. (2021). The common characteristic of these studies is that they focus greatly on the concept of interorganizational trust. These publications over the 2017-2021 period indicate that trust continues to represent an important factor in IB literature with many theoretical and practical implications both for scholars and practitioners.

As far as future research is concerned, more longitudinal and geographically dispersed studies should be conducted in order to test the causal assumptions of the above-mentioned papers. Additionally, I encourage scholars to further explore research areas such as the development of trust among ISA partners over time, inter-partner trust repair and rebuilding, the potential existence of a bidirectional causal relationship between trust and ISA performance. as well as the investigation of the most important antecedents of inter-partner trust development in ISAs.

References

Ahern, K. R., Daminelli, D., & Fracassi, C. (2015). Lost in translation? The effect of cultural values on mergers around the world. *Journal of Financial Economics*, 117(1), pp. 165-189.

Ajmal, M., Helo, P., & Kassem, R. (2017). Conceptualizing trust with cultural perspective in international business operations. *Benchmarking: An International Journal*, 24(4), pp. 1099-1118.

Ali, T., Khalid, S., Shahzad, K., & Larimo, J. (2021). Managing international joint ventures to improve performance: The role of structural and social mechanisms. *International Business Review,* 30(3), 101791.

Ali, T., & Larimo, J. (2016). Managing opportunism in international joint ventures: the role of structural and social mechanisms. *Scandinavian Journal of Management*, 32(2), pp. 86-96.

Balboni, B., Marchi, G., & Vignola, M. (2018). The moderating effect of trust on formal control mechanisms in international alliances. *European Management Review*, 15(4), pp. 541-558.

Bijlsma-Frankema, K. M., de Jong, B. A., & van de Bunt, G. G. (2008). Heed, a missing link between trust, monitoring and performance in knowledge

intensive teams. *International Journal of Human Resource Management*, 19(1), pp. 19-40.

Bryan, S., Nash, R., & Patel, A. (2015). The effect of cultural distance on contracting decisions: The case of executive compensation. *Journal of Corporate Finance*, 33, pp. 180-195.

Cao, Z., & Lumineau, F. (2015). Revisiting the interplay between contractual and relational governance: A qualitative and meta-analytic investigation. *Journal of Operations Management*, 33-34, pp. 15-42.

Cavusgil, S. T., Ghauri, P. N., & Akcal, A. A. (2013). *Doing business in emerging markets*. London: Sage Publications Ltd.

Chen, D., Park, S. H., & Newburry, W. (2009). Parent contribution and organizational control in international joint ventures. *Strategic Management Journal*, 30(11), pp. 1133-1156.

Das, T. K., & Teng, B.-S. (1998). Between trust and control: Developing confidence in partner cooperation in alliances. *Academy of Management Review*, 23(3), pp. 491-512.

Disdier, A.-C., & Head, K. (2008). The puzzling persistence of the distance effect on bilateral trade. *The Review of Economics and Statistics*, 90(1), pp. 37-48.

Dyer, J., & Singh, H. (1998). The relational view: Cooperative strategy and sources of interorganizational competitive strategy. *Academy of Management Review*, 23(4), pp. 660-679.

Ghauri, P. N., & Usunier, J.-C. (2003). *International business negotiations*. London: Pergamon Press.

Gulati, R. (1995). Does familiarity breed trust? The implications of repeated ties for contractual choice in alliances. *Academy of Management Journal*, 38(1), pp. 85-112.

Guo, W., Yang, J., Li, D., & Lyu, C. (2020). Knowledge sharing and knowledge protection in strategic alliances: the effects of trust and formal contracts. *Technology Analysis & Strategic Management*, 32(11), pp. 1366-1378.

Huber, T. L., Fischer, T. A., Dibbern, J., & Hirschheim, R. (2013). A process model of complementarity and substitution of contractual and relational governance in IS outsourcing. *Journal of Management Information Systems*, 30(3), pp. 81-114.

Jha, A., Kim, Y., & Gutierrez-Wirsching, S. (2019). Formation of cross-border corporate strategic alliances: The roles of trust and cultural, institutional, and geographical distances. *Journal of Behavioral and Experimental Finance*, 21, pp. 22-38.

Jiang, X., Li, M., Gao, S., Bao, Y., & Jiang, F. (2013). Managing Knowledge

Leakage in Strategic Alliances: The Effects of Trust and Formal Contracts. *Industrial Marketing Management*, 42(6), pp. 983-991.

Krishnan, R., Martin, X., & Noorderhaven, N. G. (2006). When does trust matter to alliance performance? *Academy of Management Journal*, 49(5), pp. 894-917.

Lascaux, A. (2020). Coopetition and trust: What we know, where to go next. *Industrial Marketing Management*, 84, pp. 2-18.

Li, J. J., Poppo, L., & Zhou, K. Z. (2010). Relational Mechanisms, Formal Contracts, and Local Knowledge Acquisition by International Subsidiaries. *Strategic Management Journal*, 31(4), pp. 349-370.

Li, Y., Xie, E., Teo, H.–. H., & Peng, M. W. (2010). Formal control and social control in domestic and international buyer–supplier relationships. *Journal of Operations Management*, 28(4), pp. 333-344.

Liu, Y., Luo, Y., & Liu, T. (2009). Governing buyer–supplier relationships through transactional and relational mechanisms: Evidence from China. *Journal of Operations Management*, 27(4), pp. 294-309.

Madhok, A. (1995). Revisiting multinational firms' tolerance for joint ventures: a trust-based approach. *Journal of International Business Studies*, 26(1), pp. 117-137.

Malhotra, D., & Lumineau, F. (2011). Trust and collaboration in the aftermath of conflict: The effects of contract structure. *Academy of Management Journal*, 54(5), pp. 981-998.

Mellewigt, T., Madhok, A., & Weibeld, A. (2007). Trust and formal contracts in interorganizational relationships – Substitutes and complements. *Managerial and Decision Economics*, 28(8), pp. 833-847.

Mian, A. (2006). Distance constraints: The limits of foreign lending in poor economies. *The Journal of Finance*, 61(3), pp. 1465-1505.

Poppo, L., & Zenger, T. (2002). Do formal contracts and relational governance function as substitutes or complements? *Strategic Management Journal*, 23(8), pp. 707-725.

Robson, M. J., Katsikeas, C. S., & Bello, D. C. (2008). Drivers and performance outcomes of trust in international strategic alliances: the role of organizational complexity. *Organization Science*, 19(4), pp. 647-665.

Shi, W., & Tang, Y. (2015). Cultural similarity as in-group favoritism: The impact of religious and ethnic similarities on alliance formation and announcement returns. *Journal of Corporate Finance*, 34, pp. 32-46.

Silva, S. C., Bradley, F., & Sousa, C. M. P. (2012). Empirical test of the trust-performance link in an international alliances context. *International Business Review*, 21(2), pp. 293-306.

Sklavounos, N., Rotsios, K., & Hajidimitriou, Y. (2018). Key Antecedents of Foreign Partner's Trust in International Strategic Alliances and the Impact of Trust on ISA Performance. In: Das, T. K. (ed.), *Managing Trust in Strategic Alliances*, Charlotte, NC: Information Age Publishing, pp. 199-226.

Wang, L., Yeung, J. H. Y., & Zhang, M. (2011). The Impact of Trust and Contract on Innovation Performance: The Moderating Role of Environmental Uncertainty. *International Journal of Production Economics*, 134(1), pp. 114-122.

Yang, S. M., Fang, S. C., Fang, S. R., & Chou, C. H. (2014). Knowledge Exchange and Knowledge Protection in Interorganizational Learning: The Ambidexterity Perspective. *Industrial Marketing Management*, 43(2), pp. 346-358.

AIMS AND SCOPE

With our semi-annual edition we aim to present the exploratory work of experienced economists as well as economists of the younger generation who take an active interest in economic life and economic thought as well as their development.

Above all the *Archives of Economic History* will endeavor to shed some light on the course of economic policy and economic thought based on historical material.

In order to render its mission more complete, the *Archives of Economic History* will include the publication of selected double blind peer reviewed papers of general scientific interest cited in the Journal of Economic Literature (JEL) classification system.

The *Archives of Economic History* is indexed/abstracted in the electronic bibliographies of the American Economic Association since 1995 and in the Greek Reference Index for the Social Sciences and Humanities (GRISSH) since 2015.

AUTHORS GUIDELINES

The submitted papers must be original work without prior publication or currently being considered for publication, and will be approved by two specialists. The following conditions and procedures for the articles submission should be taken into consideration:

1. **Articles must be written in English and submitted in MS-Word (doc or docx).**

   Their length should not exceed a maximum of 30 pages. A complete article should contain two files: the abstract file (maximum length: 120 words) and a main body text file.

2. **On the first page of the abstract file** the following information should be printed:
   - **a.** Title of the article
   - **b.** Author's/Authors' name and surname (in capital letters)
   - **c.** Name of Institution and Department where the author is employed
   - **d.** Author's contact details: mailing address, telephone number and e-mail address. The code of classification of the submitted article should appear after the abstract according to the JEL classification system, and should be no more than 6 keywords.
3. **Only the title of the article** should appear at the top of the first page of the main body text file. All papers should be submitted to: akiohos@otenet.gr
4. **Acknowledgements of references** of the original source of the articles should appear after the endnotes and before the bibliographical references.
5. **Tables or Graphs** should be written clearly and their size should not exceed a regular A4 page. They should also be entitled and numbered accordingly (e.g. "Table 1:", "Graph 1:" etc.)
6. **Paragraphs** must be numbered in Arabic numbers, starting from introduction (e.g. 1, 1.1, 1.2,2, 2.1, 2.2 etc.).
7. **The article** should be accompanied by the bibliography directly relevant to its subject. Footnotes should be consecutively numbered and appear at the end of the article, before the bibliographical references.
8. **The formulae** should follow a consecutive numbering on the right hand side of the page.
9. **Quotations cited in the main text or in the footnotes** include the surname of the author, the year of publication and specific page numbers, for example: (Elton, 1967) or (Montesano and Brown, 2008) citing both names of two, or (Viaggi et al., 1991), when there are three or more authors.

   Bibliographical references on the last page of the article should be written in alphabetical order, as follows:

   - **i) For books:** e.g. Strunk, W., and White, E. B. (1979). The elements of style. (3rd ed.). New York: Macmillan.
   - **ii) For articles:** e.g. Van der Geer, J., Hanraads, J. A., and Lupton, R. A. (2000). 'The art of writing a scientific article'. Journal of Scientific Communications, 163 (1), pp. 51–59.
10. **Among the articles submitted**, those that fulfill the above criteria are forwarded to referees for assessment.
11. **Failure to apply the above terms** will result in the rejection of the article or its return to the author for review and editing.
12. **The author is informed** whether or not the article submitted has been accepted or will be accepted upon improvements made based on the comments of the referee or the editorial board. When the author has completed the proofs reading of the articles no further additions or changes to the text are allowed.
13. **Failure to a timely submission** of the proofread article directly means that the article will not be included in the current issue.
14. **Articles under review** should be submitted to the following address: Professor Petros A. Kiochos, Editor in Chief of the Archives of Economic History, 84 Galatsiou avenue, Athens 111 46, Greece, **Tel. No.** (+30) 210-2910866 or, (+30) 693-7244739. Alternatively papers may be submitted to: akiohos@otenet.gr