A New Monetary System with New Monetary Policy

Kees van Hee
Jacob Wijngaard

WHITE PAPER

Vaart-Dommel-Rotte Collective, January 2017

A new monetary system with new monetary policy

Kees van Hee

Jacob Wijngaard

Content

Preface

Next to a common background as PhD students at the Eindhoven University of Technology, in the seventies, we share an interest in Monetary Economics. This interest developed (for one of us) through consultancy for financial organizations and (for the other) through research interest in supply chain finance and involvement in the development of complementary currencies. This interest would not have produced more than pipe dreaming without the financial crisis. Such a crisis is challenging for all civilians. And for us sufficiently challenging to overcome the hesitation we had as scientists to start to write seriously about a field of research and expertise that is not our own.

It has led to this white paper. We like to stress once more that we are not economists. That is also clear from the limited embedding in the economic literature. Hopefully sufficient to have the main relationships, but certainly far from complete. Economists are generally directed to explaining and predicting economic phenomena. We follow a more design oriented approach. We are not complete technocrats, however. We don't believe that the world is makeable. But we are convinced that a good monetary system can be designed and that such a design is helpful in directing the further development of the real monetary systems.

We think we formulated our proposal rather precise. But it is clear that further research is required to explore the consequences more completely, and investigate the challenges of communication and implementation. Not to speak about the political decision making. It is just a start. But we don't see another way to start. The remedies proposed presently by banks and politics are only papering the cracks. The problems are too big for that.

Kees van Hee and Jacob Wijngaard

The third member of the "collective" is sorely missed. That is why we dedicate this paper to our friend and former colleague Jo van Nunen. He would certainly have contributed to this paper.

A new monetary system with new monetary policy

Kees van Hee en Jacob Wijngaard

1 Introduction

Since the financial crisis, a fierce debate has started about the role of banks in financial and monetary systems. Is it not too easy for banks to create money? Is this boom and bust phenomenon in economics not mainly caused by banks? Are the too high debts in the private sector not mainly due to the banks? Is it not better to leave the creation of money to the government? The Stichting Ons Geld (Foundation Our Money), supported by a sufficiently large part of the Dutch population, has put these questions to parliament and government. The Minister of Finance is asked to give more structural attention to this point. That is why he asked the WRR (scientific council for government policy) for advice. This paper is meant to contribute to this debate.

In the present system we have two forms of money, *cash* (coins and bank notes) and *demand deposits* (balances on current accounts). Cash is part of the so called *base money*[1]. The rest of the base money is digital and invisible for normal economic actors. It consists of the *reserves* of (commercial) banks and government at the Central Bank (CB). A demand deposit is (only) a *claim* on base money. Such claims are generally accepted however, and form the main part of the available money. Because it is more and more common to use demand deposits as medium of exchange, there is less and less tendency to effectuate (cash) the claims. That gives the banks more and more freedom to create new claims, new money. It is also helpful here that, in order to support the system, the CB provides base money whenever that turns out to be necessary.

The most fundamental element of the debate about the role of the banks is the question whether we are going to keep using demand deposits as medium of exchange. Instead of that, it is also possible to give all economic actors access to the base money and use only that. The proposals of Positive Money (PM) in the UK and of the Stichting Ons Geld in The Netherlands choose this second possibility. In this paper, we do the same. However, in our view, the PM proposals are not sufficiently strict yet. We add three elements: (1) abolish cash and introduce

[1] See Ryan-Collins, Greenham, Werner and Jackson, “Where does Money come from”, NEF, 2011

base money as the only legal tender, (2) introduce a public system to administer the base money accounts of all economic actors and (3) renew the monetary policy and link the base money amounts to the GDP.

The first element prevents the occurrence of black money and makes tax evasion a lot more complicated. The second element is about the position of the banks. In the actual system, demand deposits are the main medium of exchange. And, of course, the commercial banks administer the demand deposits. If we switch to base money as medium of exchange, this role can be played by a public organization. This is worked out in Section 3. The third element is the monetary policy. Having base money as legal tender makes it possible to link base money amounts on individual accounts to the GDP. This leads to a completely different monetary policy. This is worked out in Section 4. In Section 5 we discuss the transition from the actual system to the proposed system.

Before we start to develop these elements, we discuss in Section 2 the problems with respect to the actual system and the measures that are proposed. Why there are really serious problems, our view on these problems and our position with respect to possible solutions. In Section 6 we draw conclusions.

2 Why the current system needs an overhaul

After the second world war, the Bretton Woods agreement has been applied for a number of years. That agreement implied (about) fixed exchange rates. And (only) the dollar could be exchanged for gold. So there was still an (indirect) connection with something real. That worked all right as long as there was confidence that the dollar could be exchanged indeed for gold. When the US government created more and more dollars, also to finance the Vietnam war, that confidence disappeared. Central banks outside of the US started to claim gold for dollars, and the system deteriorated and was abolished. Since then (1971) the "highest" form of money in a country is the money issued by the CB, cash and bank and government reserves. The total of cash and reserves is the *monetary base* (consisting of *base money*).

We pay each other generally not with base money, but with a demand deposit on a current account at some commercial bank. Such a demand deposit is a *claim* on base money. The alternative of using a current account is using cash. But the use of cash decreases, at least relatively. It is mainly used for small expenses[2]. And a significant, but rather stable part of it is hoarded. The need of cash is so small that banks can easily create claims, without having available sufficient base money. It is not necessary to fear that the claims are cashed.

In case of a payment to another demand deposit at the same bank, there is no effect on the (base money) reserves of that bank. In case of a payment to a demand deposit at another bank, the reserves of the paying bank are reduced and the reserves of the receiving bank are increased. Banks have mutual accounts. At certain moments, the banks liquidate their debts: *clearing* (determine what has to be transferred) and *settlement* (the actual transfer of the reserves). That can be problematic for a bank, but there are various ways to complement the reserves: mutual credits or a credit from the CB. The CB is, just as the banks, oriented to a smooth payment traffic, also if the shortages are due to credits provided by a bank. If a bank sees a good possibility to give a credit, she will do that. Possible problems due to payments to other banks will be resolved. The decision to provide credit and to create money in that way is taken by the banks, together with the customers. Banks can give money, claims on base money, without having the corresponding amount of base money. There are general rules with respect to reserves and liquidity (Basel I, II and III). But the position of a bank is judged afterwards and the judgement of the different categories of assets and the validity of the rules are not always clear[3]. This implies that the banks have in fact a large freedom with respect to the creation of money: the claims are rarely cashed.

[2] See e.g. "Cash Report 2016, Europe", G4S, 2016
[3] See e.g. Admati and Hellwig, "The Bankers New Clothes", Princeton University Press, 2013

So, bank credits are a strange form of money. Nevertheless, from 1971, after the abolition of the Bretton Woods agreement, it has functioned well for a while. By adapting the interest rate for reserves, the availability of credit was controlled, and through this the whole economy. And especially during the period 1985 – 2005, the system appeared to be really "under control". That is why that period is called "the great moderation". In between, however, there are serious doubts. It is clear that the banks have played an important role in the emergence of the financial crisis. The American mortgage market was the biggest culprit. But the lack of transparency and the sale of too complex financial products contributed as well[4]. The structural freedom of banks due to the current monetary system is often seen as the root cause. There are different proposals for improvement. Sharper restrictions with respect to liquidity and solvability[5], better monitoring and control, narrow banking (banks concentrate on payment and saving and give credit only insofar as that can be guaranteed absolutely)[6].

The Positive Money movement (PM) gives the most fundamental and clear recommendation[7]. Their advice implies that base money is made available for all economic actors. The claims on base money that are presently issued by the banks, cannot be used freely anymore. Governments and government related organizations do not accept such claims any longer. Base money is going to be the single legal tender and banks cannot create such money. Banks can only give credit if they have base money and are willing to provide that. They can borrow base money from the CB (under certain conditions) but the CB is the only money creating organization. The proposal is inspired by the much older Chicago plan[8]. That plan proposed *full reserve banking.* In case of full reserve banking the banks still provide the money, but they need to have 100% coverage with base money[9]. PM justly draws the conclusion that it is more logical and also clearer to give everybody access to base money. They still assume that the banks facilitate the accounts, but that is not by definition so anymore. In The Netherlands the initiative is taken over by the "Burgerinitiatief Ons Geld" (Citizen's initiative Our Money). That has led eventually to a request of the Minister of Finance to the WRR (scientific council for government policy) to give an advice on this issue.

The PM proposals are an important reference point for us in this paper. Therefore, it is important to know the pros and cons of the PM proposal compared with the present system.

[4] See e.g. Roubini and Mihm, "Crisis Economics", Penguin Books, 2010
[5] See e.g. Admati andHellwig, "The Bankers New Clothes", Princeton University Press, 2013
[6] See e.g. Narrow Banking; The Reform of Banking Regulation, Centre for the Study of Financial Innovation, 2009
[7] See Jackson and Dyson, "Modernising Money", Positive Money, 2012
[8] Fisher, I. "100% Money and the Public debt" Economic Forum, Spring Number, April-June 1936, 406-420.
[9] That plan was refreshed already recently by Benes and Kumhof, "The Chicago Plan Revisited" IMF, 2012

The recent special issue of the Cambridge Journal of Economics[10] is very helpful here. It is completely devoted to alternative monetary systems, with substantial attention for PM.

Instability in the present system is the main argument of PM. That is confirmed again in the PM contribution to this special issue[11]. The most important product of banks are loans. They love to sell loans. However, too easily provided credits lead to overvaluation of the assets involved and stimulates new credits. Until the vicious circle breaks. Competition and fancy financial products worsen the instability: it is not necessary anymore that a bank has confidence in a certain product, it is sufficient that a potential buyer has confidence. The deposit insurance systems pushes in the same direction, if things go wrong there is sufficient back-up. This tendency to instability is not really disputed by the critics of the PM proposals. It is rather whitewashed. The defense is that there are all kind of improvement possibilities. And they explain that, also if the PM proposals are implemented, there is going to be instability. Instability is argued to be inevitable. We see these points, but we see not why that implies that the PM proposals should not be implemented. As long as PM leads to a more stable and more transparent system there need to be other objections to drop it.

The two most important arguments against PM are:

- Combining monetary policy with fiscal policy
- Not sufficiently flexible with respect to credits

The first objection is right. The PM proposals suggest rather easily that the creation of money can also be used to finance government expenses. And it is politically not pure to do that. The government has many functions. One of these is to facilitate a good monetary system. That function is important whatever your opinion is about the further functions of the government. So, it is important to organize this monetary function as good as possible, independent of further decisions with respect to the role of the government and government expenses. The creation of money that is necessary for a proper functioning of the monetary system should not be used to facilitate government expenses that would have been impossible otherwise. The PM proposals are too sloppy with respect to this. But the positive money concept as such does not imply this[12]. It is quite possible to combine the positive money concept with a strict separation of monetary policy and fiscal policy. For instance by determining that the effect of new money

[10] Cambridge Journal of Economics, 2016, **40**

[11] Dyson, Hodgson and Van Lerven, "A response to Critiques of 'Full Reserve Banking'", Cambridge Journal of Economics, 2016, **40**, 1351 - 1361

[12] In this respect PM differs fundamentally from MMT (Modern Monetary Theory). In MMT, functional finance is essential. That means that the CB creates money on behalf of the government, for the purpose of (especially) full employment. So, not the monetary system is leading here, but full employment. See e.g. Juniper and Mitchell, "There is no financial crisis so deep that cannot be dealt with by public spending", University of Newcastle, Australia, 2008.

creation on the government budget is compensated. For instance by a reduction of the value added tax or by requiring that the government deficit is reduced or the government surplus is increased. So, this objection is in fact not an objection against positive money, but only against a certain form of it.

The second objection may be right. It goes back to a publication of Schumpeter, who connects the credit supply of banks with innovation[13]. The financial flexibility that is required is, according to Schumpeter, only available through the possibility of banks to create new money. Dyson et al state in their reaction that also in the PM proposal, banks can borrow base money from the CB and in this way can put more money in the economy. The monetary authority responsible for these loans has to put restrictions on these loans, however, that these loans are only for productive purposes[14]. We are concerned that if it is easy to get around these restrictions, banks have again the same freedom as in the present system and it is questionable whether the transition is worth the effort. And if the restrictions are hard, it could be that the transition to a PM monetary system goes at the expense of important financing flexibility.

Our conclusion is that positive money is an attractive monetary concept. But that it has to be elaborated such that it is fiscally neutral. And that it is important to give attention to this matter of sufficient credit flexibility. Detailed monetary rules for credits from the CB to the banks should be prevented here. The more robust the rules the better. Such an elaboration is described in the next two sections.

We assume a monetary zone, a country or the Eurozone, with a coherent monetary policy. The structure of storage and transfer of money is considered in the next section. The PM proposals assume that payments are still facilitated by the banks. We drop that. We assume that the basics of storage and transfer of money are provided by a monetary system that is organized by a public organization. The system is organized such that it is possible to provide the information that is necessary for executing the monetary policy. All kinds of services, by private service suppliers, may be added to that public system..

In Section 4 we describe the monetary policy. By coupling the base money amounts on the accounts with the (nominal) GDP, in combination with an anti-hoarding tax, there is absolute control of inflation. The PM proposal presupposes a rather finicky monetary authority, very close to the precise functioning of the economy who also tries to control the inflation in this way. In our proposal this is more relaxed and at distant.

[13] Schumpeter, “The Theory of Economic Development”, Harvard University Press, 1912 [1934]
[14] See Dyson, Hodgson and Van Lerven, “A response to Critiques of ‘Full Reserve Banking’”, Cambridge Journal of Economics, 2016, **40**, 1351 - 1361.

In both sections we do not take into account the possibility of cash. In the PM proposal cash is still part of the base money. We propose to drop that and to support also no alternative forms of cash, but to work *cashless*[15]. The advantages of working cashless (security, tax evasion, criminality, etc.) are anyway big already, also in the present system. In Section 5 we discuss the transition to the system we propose. We also give some attention to the complications of starting to work cashless.

[15] A form of cash that would fit in the system is cash in the form of vouchers, claims on certain products/services or claims on base money.

3 Monetary system

In this section we consider the storage and transfer of base money. These basic functions form the infrastructure for the whole monetary system. Contrary to the existing monetary system, the storage and transfer of base money are not controlled by the banks anymore. There will exists accounts for base money, independent of the banks. The approach of Kay[16] is appealing to us. These functions are such a vital utility for the community that the government should oversee the availability, security and quality. Therefore it is more efficient if the government or an authority controlled by the government, provides these essential functions. Then it is also easier to realize an increase in performance and safety[17]. Banks still play an important role, but they do not stand in between the accounts of private persons and corporates on the one hand and the CB on the other hand. If the infrastructure is functioning well, there is plenty of room for banks and other companies (e.g. fintech companies) to offer all kind of additional financial services on top of the storage and transfer layer.

The most important actors in the monetary system are:

- Central bank
- Owners of *A-accounts* (payment accounts)
- Banks

Besides these actors there is the 'central administrative actor' who we call the Monetary System (MS for short). Only the CB creates the base money. Created money always arrives on the accounts of the economic actors in the monetary zone of the CB. The amount of base money on an account is always positive (or zero). You can't pay more than there is available on the account. The government also has its own A-accounts and they also can't spend more than they have on the account.

Also banks have for their own business such A-accounts. Economic actors who have a surplus of money for some time can lend it to a bank. Contracts for such a loan will have a duration and an interest rate. The administration of such contracts will be done by the banks. PM uses the term *investment account*. The basic money of a lender is deposited on a so called *B-account* of the bank. The B-account corresponds to the *investment pool* of PM. From the B-account base money can be lend to all (A-)accounts. It might be necessary to create more credit facilities (the "Schumpeter-argument", see former section). To that end banks will have the opportunity to loan base money from the CB. Therefore we introduce the so-called *C-account* at the CB. The

[16] See Kay,: "Narrow Banking; The Reform of Banking Regulation", Centre for the Study of Financial Innovation, 2009

[17] It is interesting to notice that the first digital money system in the Netherlands was a state-owned company, called Postcheque en Girodienst.

lent base money is transferred from the C-account to the B-account of the bank. The amount of a base money on a C-account is always *negative.* So the total amount of base money on all accounts (A, B and C) together always remains *constant* in case of a transfer from one account to another, independent of the kind of account.

The fact that the storage and transportation of base money becomes a task for the government does not imply that the government has to become a 'trusted third party' that keeps record of all transactions. There are several possibilities (via encryption techniques) to reduce the information the administrator of the MS will have. These possibilities are considered below.

3.1 Payment

Each actor has one or more accounts in the MS, always with a non-negative amount. Each account has its own unique internet address (url, uniform resource locator). There is an *asymmetric encryption* system installed (see Appendix 1). So each account has its own pair of a *secret key* and a *public key.* All data of an account are encrypted with the secret key of the owner and so it can't be manipulated by administrators or hackers. Without further security measures it is in principle possible for administrators and also for hackers to see the accounts data with the public key of the owner.
The MS manages two kind of *records*: (1) *balance records* en (2) *transaction records*:

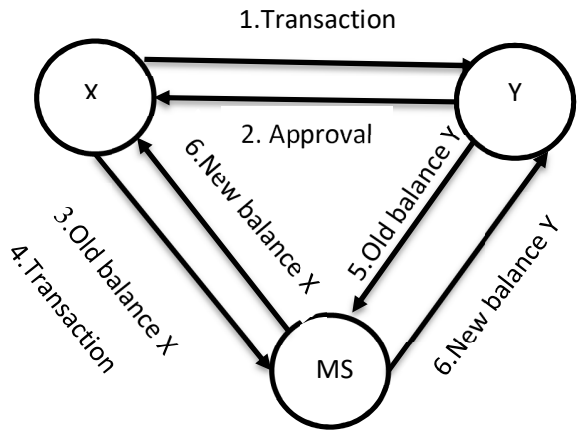
- Balance record: [acnr: X, balance: A, seqnr: M, $S_{MS}(X,A,M)$]
- Transaction record: [from: X, amount: B, to :Y, trnr:N, $S_X(X,B,Y,N)$, $S_Y(X,B,Y,N)$]]

A record is in between brackets […] and a record contains fields separated by comma's. Most fields have an attribute (name) and a value, separated by a semicolon ':'. The last fields have only a value, which is the encrypted information of the preceding fields. The attribute 'acnr' is the account number of an actor, seqnr is the sequence number of the updates of the balance in the MS and trnr is the transaction number of the paying account. Here X and Y are the accounts involved in the transaction. The fields denoted by $S_{MS}(X,A,M)$ and $S_X(X,B,Y,N)$ are the values presented before, encrypted with the secret key of MS and of actor X respectively. They are readable with the public keys, but immutable without the secret key of MS. The objective is to protect the rest of the record against manipulation: a malicious person may change in a balance record the values X, A or M, but only the MS can change $S_{MS}(X,A,M)$ so if an actor is cheating it is to see in the record. For technical reasons variations of this record structure are possible but they will in essence be the same.
The balance records show the succession of balances of the account. The transaction records the transfer of basic money from one to another account.

An actor can transfer maximally the whole balance of his account to another account, possibly another own account. Accounts never become negative. The actors offer their transactions with their *current* balance record to the MS and the MS checks the information and, if correct, executes the money transfer on the balance records and sends them back to the actors. The only thing the MS really has to remember are current sequence numbers of all accounts.
The reason is that this prevents the possibility for an actor to offer a balance record twice in order to do two payments with the same money. In the bitcoin alternative (see Appendix 3) the big issue is to avoid that a bitcoin can be spend twice. For that reason the public *block chain* is invented. Our solution is much more simple and does not require the huge computer resources needed for the block chain approach. The bitcoin has the advantage that a centralized organization is not necessary, like our MS. But in our proposal the MS is not a Big Brother and guarantees the same anonymity. The other information does not have to be stored in the MS but with the actors themselves. In the minimal variant of the MS only the sequence numbers of the updates of the balances are known and not the transactions and balances themselves.

3.2 Protocol for a standard payment

We describe here the protocol for the transfer of an amount B from actor (account) X to actor Y. This is also a reference for other types of payment in the monetary system.
First X and Y have to agree on the payment. In the diagram below we see the protocol for the minimal variant, where actors X and Y, after the agreement, send their current balance records to MS. The paying actor, X, sends also the approved transaction record to MS. (This is an arbitrary choice: the receiving actor could do this as well). The MS executes the updates, i.e. MS decreases the balance of X with the amount of the transaction record and increases the balance of Y with the same amount. The MS also increases the sequence numbers of the balances and then sends them back and remembers only the sequence numbers of the accounts. The numbers in the diagram denote the order of steps. (If two actions have the same number the may be executed simultaneously. Actions 3, 4 en 5 may be performed in an arbitrary order). In Appendix 2 the protocol is described in more detail.



We distinguish (decreasing) *levels of privacy*, in which the MS will remember more and more of the transactions, but at the same time the MS offers more *services* to the actors. The MS communicates to the actors via an application program interface (API) and internet. So actors may apply mobile devices as well as computer systems. The variants are:

1. MS remembers only the sequence numbers of the last update of the balance record of each account. So it is prevented that an actor offer an old balance record, with an amount bigger than the current one, twice. Further the MS keeps record of a list with account numbers, public keys and url's of the actors. Actors have their own systems for storage of balance and transaction records and they make only use of the API for steps 4, 5 and 6 of the protocol. Companies like banks, payment facilitators or accounting firms could set up and manage this kind of systems for the actors and offer it as a service.
   In this variant MS is only involved in steps 3 t/m 6 of the protocol.
2. MS remembers also a *hash* (see Appendix 1) of the old *balance records* of the actors. So it can be verified easily if actors have changed their balance records later for fraudulent reasons. So actors can ask the MS for such checks, while the MS does not know the records.
3. MS remembers the balance records in a distributed database, for instance in a *blockchain* (see Appendix 3). So steps 3 and 5 of the protocol can be skipped. Actors don't have to keep and update their own balance records since they can query the MS via an API.
4. MS remembers besides the balance records also the transaction records for instance in a block chain. So the whole history of each account can be reconstructed. Actors don't have to keep records anymore and can query the MS for all the data they need for accounting reporting via an API.
   In this variant MS supports all steps of the protocol. This is a Big Brother solution, which

does not have to be dangerous if it is guaranteed that the MS does no give third parties insight in these data and so it must be impossible to hack the MS.

We recommend level 3 because it protects actors against loss of data and the MS can easily be used for monetary policy making (see Section 4).

3.3 Functionality and performance of the MS

In practice there are all kinds of special transactions, such as a *deferred payment* and the *direct debit.* The first occurs when the exact amount of the transaction is not yet known at the moment the transaction starts, e.g.in case of parking or refuel of gasoline. The protocol only differs in the first two steps of the protocol: the message from X to Y has not yet an amount but it appears in the answer from Y to X. In all variants this happens outside of the MS. Only if the transaction record is ready it is sent to the MS. The direct debit occurs when there is a contract between actors X and Y such that Y may collect automatically, which is usual for utility companies. In this case the protocol starts with an authorization message from X without an amount and Y adds the amount in the answer message later. But here Y can send this kind of transaction messages unlimited until X sends a message to retract the authorization. This process only concerns the first two steps of the protocol and so it stays out of the scope of the MS. In the practice of payment services there are more payment variants. But we are convinced that they can be implemented on top of the proposed MS.

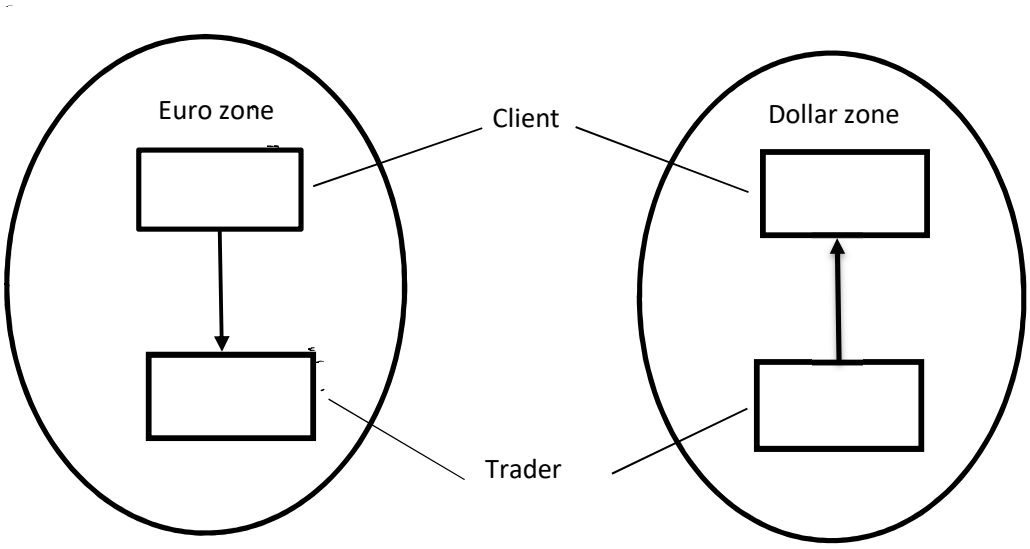
Besides the transaction related functions the MS also has *management functions*, such as creation, combining, splitting and removing accounts. To increase the security of the system it is necessary to refresh periodically the key pairs, i.e. the private and public keys of the accounts. This also requires functionality, but therefore proven technology is available already.

About 300 million people are living in the Euro zone, and if we add the companies and other organizations we estimate a need for one to two billion accounts. For other payment zones, like the dollar, the yen and the yuan similar calculations can be made. With a total storage of ca 1 MB per account the MS needs a storage capacity of ca 1 petabytes. The computing time per transaction is small (a fraction of a second): the data of the accounts has to be retrieved (the public key, the balance sequence number or the balance record in the last two variants). The computations consist of decryption and encryption of the messages and in between the trivial updates of the balance records. It is possible and preferable to implement these services of the MS on a distributed server network (cloud). Think about 100 to 1000 servers geographically spread over the euro zone. One of the possible architectures distributes the accounts over the servers and the transaction is executed at the server of the paying account. The server of the paying account demands the server of the receiving account for the balance record and sends the updated version back. With a *load balancing* algorithm the accounts can be distributed in

such a way that each server in the MS has about the same workload. In this way the system is *scalable* and the performance is controllable. For safety and security reasons it is wise to back up copies of each account on several other servers (10 to 100) while only one server is managing (hosting) the account. So the probability of the loss of an account can be made as small as the probability that a meteorite destroys the earth.

3.4 The trade with other monetary zones

Of course there is trade with other payment zones. This can be facilitated by actors in the role of valuta trader. Such a trader has an A-account in each zone, e.g. one in the euro zone and one in the dollar zone. The trader receives from an euro actor an amount of euro's on its A-account and sends this actor, who also has a dollar account, a corresponding amount of dollars on its dollar account in the other zone. He should have enough buffer in euro's and dollars to play this game successfully. Often banks will play the role of valuta trader.



3.5 'Free' market in the financial services layer

On top of the MS infrastructure providers arrive to offer new services in the so-called financial services layer. An example is bookkeeping services that add information to transactions, such that they can be recorded directly in the general ledger. Existing services as factoring and credit loan are other examples. A new service could be automatic VAT computation and payment.

This service could be built in in the MS. That requires an extra attribute for the classification code for VAT. And it is probably 'cleaner' to put this kind of services in a separated layer. This layer is the playing field of new *fintech* companies, but also old services of existing financial institutions will migrate to his layer.
There are also existing services that will disappear, since the debit card transactions will be streamlined. Today they involve specialized payment service providers (PSP) and debit card companies. In the end the payments are effectuated via the banks but this may take hours and sometimes even days. These PSP's obtain their reason of existence from the impotence of the banks to execute payments in real time, in particular if two banks are involved. This also means that functions that are fulfilled by SWIFT, will disappear. Today banks make a list of what they have to pay and a list of what they will receive of other banks (called *clearing*) and periodically the balance of these lists are 'transferred' which means that the banks update their own accounts. These functions will disappear.
Of course there should be oversight on the services in the financial services layer. But the advantage of the MS infrastructure is that it becomes much easier for providers of new services to enter this layer. Comparable with the app stores for smart phones and tablets.

4 Monetary policy

Monetary policy is about realizing stability and economic development. Stability of buying power and stability of exchange rates. Without that stability money is less suitable as medium of exchange. The most important instrument of monetary policy is the interest banks pay for borrowing base money from the CB (refinancing rate). In the Eurozone, the emphasis is on stability of buying power. The ECB has as explicit goal to keep the inflation just below 2%. The assumption is that this is good for the economic development. Since the interest rate is already about 0% presently, accompanying measures are necessary to stimulate credit supply and economic development. This has led to the quantitative easing (QE) programme of the ECB: purchasing bonds, to increase the reserves of the banks. And even this appears to be insufficient to reach the inflation goal. Apparently it is not so easy to stimulate the economy in this way, at least not such that the inflation goal is realized. We aim to reach this inflation goal in a completely different way.

Monetary policy is separated from fiscal policy, in our proposal just as in present practice. Fiscal policy is also partly directed to economic development. So there is some overlap in goals of the two policy fields. But the instruments are completely different. And the goals of monetary policy regarding economic development are very general: stimulating economic eagerness and innovation and facilitating a sufficiently broad credit supply. We assume that the monetary policy is taken care of by the CB, just as in the present situation.

For the PM movement the control of the amount of base money is the main instrument of monetary policy. Monetary policy and fiscal policy are not strictly separated. The goals of money creation include tax reduction and paying for government expenses as well as stimulating credit supply[18]. Moreover, the PM proposals imply a rather finicky monetary authority. The limits on loans of base money to the banks depend on the way the banks use this base money, for what type of credits. If it is used for new production, the limits are higher than if it is used for existing assets and financial products. The hope is that by controlling this, the economy can be stimulated and inflation can be controlled. We don't have much confidence in this detailed interference with banking matters. The role of the government is surely important. But generally, the government is not very good in detailed stimulation of economic activity. And it is also questionable whether it is possible in this way to control inflation. It may look as if it is possible to keep banks tight in certain areas, but banks are supposed to be creative in the transfer of money from one destination to another.

[18] See Dyson, Hodgson and Van Lerven, "A response to Critiques of 'Full Reserve Banking'", Cambridge Journal of Economics, 2016, **40**, 1351 - 1361.

In the current system it seems to be impossible to control the inflation. In the PM proposal the monetary authority gets too finicky. Our solution is completely different. Once it is accepted that base money is completely digital, the solution is straight forward. Inflation control has to be interpreted just a little broader. It is not necessary to control the buying power of a single unit of money. Inflation control can also be performed by linking the base money *amounts* with the (nominal) GDP.

4.1 GDP-linking (and taxed linking) of base money amounts

Suppose that each day, we have a new estimate of the (nominal) GDP. The estimation procedure is discussed in the next sub-section. Let $B(t)$ be the GDP and $\hat{B}(t)$ the GDP-estimate at the start of day t. At that moment the base money amount on each account (A-, B and C-accounts) is multiplied with $\hat{B}(t)/\hat{B}(t-1)$. That means that the buying power stays in line with the GDP (estimate). The total amount of base money on all accounts is equal to $M(t) = \boldsymbol{f} \cdot \hat{B}(t)$. The constant $\boldsymbol{f}$ here is a monetary parameter to be determined. If there are only price increases and no real growth, the buying power of the account stays the same. If there is also real growth, the buying power of the account grows at the same rate.
Although the corrections of the base money amounts are very small per day, the holders of the accounts may be tempted not to spend temporarily or speculators could consider the possibility to include base money in their options. That is why GDP-linking has to be combined with a small anti-hoarding tax ($\boldsymbol{\tau}$ per year). The parameter $\boldsymbol{\tau}$ could be used to realize the inflation goal. If the real growth is 0.01 per year and $\boldsymbol{\tau} = 0.03$ per year, the buying power of an unused base money account shrinks per year with 2%. It is a form of taxation as proposed by Gesell, with some appreciation mentioned by Keynes[19]. The tax comes on top of possible other taxes on assets.
This anti-hoarding tax, in combination with the just mentioned linking implies that each base money amount is multiplied daily with a factor $\left(\hat{B}(t)/\hat{B}\,(t-1)\right) - \tau/365$[20]. The daily adjustments are so small that it is hardly noticed by a normal user. For instance, if the real growth is 0.01 per year and there is also 0.01 inflation, and $\boldsymbol{\tau} = 0.03$ per year, the multiplication factor is equal to 0.0000274.
The total amount of base money over all accounts as fraction of the GDP can be kept constant by transferring the tax to an A-account of the government. See Appendix 4 for a more detailed explanation of the linking procedures.
By transferring less than the tax to the government account, or more than the tax, it is possible to reduce or increase the amount of base money as fraction of the GDP.

[19] J.M. Keynes, "The General Theory of Employment, Money and Interest", Book VI, Chapter 23
[20] Dividing by 365 is not completely correct of course. But in case of a small fraction of tax, the error is very small.

4.2 The GDP estimation procedure

There are more possibilities to realize a daily estimate of the GDP. A straight forward one is elaborated here. Periodically an official estimate of the GDP is made available. In between the transaction sum for transactions regarding the production, distribution and sales of real products and services (the "real" transactions) during the past year (365 days) can be used to update the GDP estimate. This transaction sum can be tracked by the MS by adding a *label* to the "real" transactions (Section 3).

Let $P_r(t)$ bet he sum of all "real" transactions during the past year, at the start of day t. The main difference between $B(t)$ and $P_r(t)$ is that in the latter all transactions *in* the supply chains are also counted. So, the fragmentation of the supply influences the ratio of $B(t)$ and $P_r(t)$. But if this fragmentation does not change too fast, it holds that $B(t) = \beta(t)P_r(t)$, with $\beta(t)$ a constant that changes only slowly with t. This implies that at the start of the day, the GDP estimate of the previous day can be multiplied with $(P_r(t)/P_r(t-1))$to get a new estimate:

$$\hat{B}(t) = \hat{B}(t-1) \cdot (P_r(t)/P_r(t-1))$$

This is the main rule. But as soon as a new official estimate of the GDP is becoming available, this estimate has to be corrected. It may be necessary to smooth this correction. See Appendix 4 for details.

4.3 Alternatives for base money

The monetary policy is based on the base money amounts. Base money is the legal tender. The link with the GDP Is attractive, but tax is unattractive for the user. So, one will certainly look for alternatives. Obvious solutions are dollars, gold and bitcoins. But for all these solutions the risk of exchange rate fluctuations forms an important threshold. So, in comparing base money with these possibilities, the link with the GDP may be expected to compensate easily for the disadvantage of the anti-hoarding tax.

A more promising possibility is to work with claims on base money issued by a bank or by a combination of banks. That is in fact the present form of money put forward as alternative for base money. Every actor can issue claims on himself and this claim can be used by all "believers" as medium of exchange. In case the claims are issued by a bank or by a combination of banks there will probably many believers. Banks could even go one step further and issue claims that are also linked with the GDP, although it may be difficult for a bank to guarantee such claims. And issuing such claims is anyway complicated since the government and government related organizations are not going to accept payment with such claims. Legal tender may not be so important in economic exchange, but it means at least that government

and government related organization accept only this legal tender. That implies that the base money reserves to guarantee these claims need to be high; the holders of the claims will frequently want to convert the claims for base money. If necessary it is also possible to prohibit banks to issue such claims. Non-banks could issue such claims then, but for such companies it is even more difficult to organize sufficient reserves, because they are not allowed to borrow base money. Non-banks can organize *money market funds* (MMF) as a kind of substitute for money, just as they do now. MMF play a role at present in storing large amounts of cash, also because the deposit insurance is limited. Base money, however, is absolutely guaranteed, so, the role of MMF may become less important.

So, it may not be expected that alternatives are going to drive out base money. It is nevertheless wise to restrict the tax on base money so that the advantage of the link with the GDP compensates the disadvantage of the tax and does not make it too attractive to look for alternatives. No tax leads to sticky fingers, people are tempted not to spend. But a too high tax makes people afraid to accept it.

4.4 Monetary policy parameters

The most important monetary parameters are the total amount of base money as fraction $\boldsymbol{f}$ of the GDP and the tax on base money, $\boldsymbol{\tau}$. Next to that there are the limits on base money credit from the CB (banks' C-accounts) and the interest on these credits. These are discussed later in this section.

The CB can adjust $\boldsymbol{f}$. This can be done by transferring the tax not completely to the indicated government account ($\boldsymbol{f}$ decreases) or by transferring more than the tax ($\boldsymbol{f}$ increases). It is important to be modest here. The more stability the better. It is also important to make $\boldsymbol{f}$ not unnecessary large. Too much money in the economy may also lead to instability. In a greedy economy, not much money is needed; actors find easily other ways to settle their transactions, if necessary by bartering. It is in fact rather strange that the ECB expects the economy to become greedier by extending the amount of money. That is comparable with expecting that inactive boxers become fiercer by extending the ring.

To estimate how much (base) money is required, we consider the various reasons to use money. Money is needed as working capital and housekeeping money. Money may be needed to make it easier at the capital market to switch from one asset to another in a portfolio. And money is needed to finance (real) investments. In Appendix 4 we sketch how to estimate the amount of money that is necessary for each of these three functions. In that way it is possible to derive a first estimate of what is necessary in total. It is expected that this is less than what is

available now at all current accounts. And with the transition to this system, that is the base money we start with (see Section 5). Then a trial-and-error process follows with an ongoing reduction of $\boldsymbol{f}$. Until it can be seen from the behavior of the banks that the edge is reached, if the money that is borrowed from the CB is also going to be used to complement the working capital. The ex-ante estimate is a useful point of reference for this trial-and-error process.

Next the choice of $\boldsymbol{\tau}$.This parameter has to be made as large as possible, but not so large that the quest for alternatives is getting too fierce (see previous section). The bigger $\boldsymbol{\tau}$, the less actors are tempted to keep base money or invest in base money, the smaller $\boldsymbol{f}$ can be made and the more stable the system is. The advantage of this monetary system is the link of base money amounts with the GDP. Suppose the predicted nominal increase of the GDP is 2%. Let half of it be due to price increase and the other half to real growth. If $\boldsymbol{\tau}$ is made equal to 1%, the buying power of the base money amounts, (the account balances, not the buying power per unit of base money) remains constant. It is possible to increase $\boldsymbol{\tau}$, because it is not easy to find liquid alternatives with also constant buying power. So, inflation helps also to make base money attractive, at least if compared with nominal claims on base money. And some inflation may be expected. In the battle for the cake (the GDP) nobody is inclined to be modest, to devaluate the own contribution. So there is a tendency of price increases and some inflation is normal. Next to some real growth, this gives sufficient slack to choose $\boldsymbol{\tau} > 0$.

The objection against the PM proposals, that there is also bank credit required to realize sufficient flexibility to finance investments and innovation, will also hold for our proposal. That criticism could be right. That is why PM adds already the possibility for banks to borrow base money from the CB. We follow PM in that. The CB allows banks to have a negative amount of base money on their C-account and have the corresponding amount added to their B-account. Our proposal is to relate the limit on the C-account to the average of the total amount of base money that is provided by other actors to the bank for the investment pool (B-account). The limit on the C-account is a fixed fraction $\boldsymbol{g}$ of that average. It is a form of fractional reserve banking. Important is that there is no bargaining about $\boldsymbol{g}$.Trial-and error is also needed here to determine $\boldsymbol{g}$. The goal is to choose $\boldsymbol{g}$ such that the total availability of base money through the B-accounts is sufficient to give banks the opportunity to pre-finance the investments that are necessary to make the economy flourish. The goal of the bank has to be to transfer such credits as soon as possible to other actors. See Appendix 4 for details.

The fourth monetary parameter is the interest $\boldsymbol{r}$ due for the base money borrowed from the CB. That is the only monetary parameter that may be adapted more actively. For instance, if it turns out that the slack on the C-accounts is used to finance transactions on the capital market,

it is appropriate to increase **r**. With respect to the other three parameters, it is a matter of careful calibration and leaving the system alone thereafter

4.5 Stability of exchange rates

Monetary policy is also about exchange rate stability, to facilitate international trade, of goods and services and of financial products. That is not different from the present system. And we do not claim that the system proposed here makes everything completely clear and stable in international trade.

But some extra stability may be expected. The development of the buying power of a GDP linked amount of base money is well predictable, since the development of the GDP is well predictable. And it is unnecessary to insure inflation risks. That advantage is even bigger if GDP linking is applied in more monetary zones. It has to be noticed however that GDP linking brings about the possibility that the base money of some monetary zone is getting attractive at the international capital market. That is certainly so if there are zones with a high predicted real growth in combination with a low tax. Then it may occur that a large part of the available base money is bought by international investors and is not available as medium of exchange anymore. It is important to consider this in determining the tax.

GDP-linking implies also an interesting possibility for the Eurozone. Most straight forward is to treat the Eurozone as one monetary zone. That means that the base money amounts are linked with the GDP of the Eurozone. Instead of that it is also possible to work with more monetary zones, all with the Euro as currency, but linked with their own GDP. That gives some freedom within the Eurozone, without dropping the Euro completely. In that case it is also important that the predicted growth of the real GDP minus the tax is about equal for the different zones. If not, all liquidity is stored in the most attractive zone, the zone with the highest difference of growth and tax.

5 Implementation and migration

It is very important that the migration of the existing monetary system to the new one proceeds smoothly. An incremental change strategy, in which a big change is realized in small steps, is preferable to a big-bang strategy where the new system has to be used at once. The introduction of the euro was a comparable operation with also more or less incremental migration process.

We have to make a clear distinction between the monetary system (MS) and the monetary policy. The implementation of MS mainly concerns the organization of the A-accounts and the software to realize the transactions. We start with the minimal variant of the MS in which the MS only remembers the last sequence number of the balance record of each account, so the number of the last update of each account. This has to be done anyway and the other functions can be added later. There is also another good reason to start with the minimal variant: the banks can keep a big part of their existing functions so that they have the time to prepare for competition with other providers of payment services in the financial service layer such as payment service providers, ict-companies, providers of cloud services, telecom operators and accounting firms. Although the real operation requires an comprehensive planning, we sketch here only the most important steps:

1. For all actors we have to create A-accounts. Almost all actors will have already accounts at a bank and these accounts have a unique number. So it is obvious to use these numbers also for the accounts in the MS. The MS should be able to provide the elementary functions: receive one transaction record and two balance records, perform the necessary verifications, update the balance records and send them back.
2. In the beginning digital payments will be performed by the banks: they will store the balance records for their clients and if an actor gives a payment order the bank will produce the transaction record and retrieve the two balance records, send this all to the MS and receives the updated balance records for the client. If it is money transfer between two clients of the same bank, then it is easy, if the transfer is between accounts at different banks then the bank of the payer will request the balance record of the receiver at his bank. By the encryption there is no risk of fraud, but the banks have to protect the privacy of the clients, both the payer and the receiver.
   This step requires a software effort of the banks, but the clients do not notice the difference with the existing system. Once this step is realized, other actors may provide these functions as well. In principle everybody can do it himself and most likely big companies will do that.

3. If the minimal variant is implemented the MS can be extended with functions for the registration of balance records and some actors will bypass the banks for save storage and transfer of money.
4. For consumer transactions, mainly in shops and hospitality and catering services, we must make a distinction between cash and card transactions. The cash transactions will die out in time. So an actor can pay with cash in shops for some time, but the change is added to his account. Also at banks actors can convert cash to digital, i.e. the amount of cash is added to the balance record of the actor. But nobody can obtain cash anymore. Note that in this phase the amount of basic money is increasing because the cash was not yet in the MS.
5. For credit card payments the existing systems have to be adapted. Today one uses in the eurozone mostly the C-TAP protocol, where the transactions are processed via the debit card organizations (e.g. Master Card, with Maestro, Visa with V-pay). In shops payment with a card and a payment terminal is also possible. In the minimal variant where the actor keeps his own balance record the card has to be adapted to be able to keep the balance record and some supporting data. (This looks like the obsolete 'chip knip' debit card of the Netherlands). The payment terminal produces the transaction record from its cash desk and sends the balance records of the consumer and the shop together with the transaction record to the MS and puts at the end of the transaction the balance record of the consumer back on its card. Consumers may have a special account for shopping.
   If variant 3 is implemented the balance records do not have to be kept on the cards and the payment terminal only has to send the transaction record. (Note that we normally assume that the payer is sending the records to MS but here it is the receiver, a minor difference that is not relevant further) Today it is possible to pay with a smartphone in shops by holding them close to a payment terminal (near field communication). But then the smartphone is used as a card and only passes the identity of the consumer and its master data.
   Debit card organizations will vanish.
6. For transactions between consumers and between consumers and shops there will be new smartphone apps allowing two consumers to transfer money directly from one account to another. In shops this means by-passing the payment terminal. In variant 3 it is not necessary to keep the balance records on the smartphones but in the first two variants it is. That is a function we are already familiar with: the e-wallet. Although debit card organizations become superfluous, credit cards may continue to exist. With a credit card the consumer pays with the money from the credit card organization and so the consumer builds up a debt to the credit card organization, just like today.

This is the main course of action. It is basically not more complicated than sketched here. But of course, in practice there are going to be many other issues.

An important question is what happens if there is a major power outage. Of course all balance records will be stored in several places in the cloud. (In variant 3 this is already foreseen.) Then one can continue business when the power is up again. Maybe a few transactions are lost and

have to be renewed. During the outage there is still some payment possible between mobile devices and systems with power back up. Of course the MS should have the best possible power back up. This is not is different from the existing systems.
Finally people want to know what the cost of this MS will be. It is obvious to charge actors per transfer and for the storage of money, but a fixed subscription fee may also be attractive. Today these charges are dependent of the amounts of money stored or transferred. But there is no good reason for, since the cost are independent of the amounts.

Concerning the monetary policy the implementation starts with linking the base money amounts on the A-accounts with the GDP. Therefore we need an estimation procedure (see Appendix 4). It is not necessary to have the link available right at the start of the MS (see step 1 above), but it has to be available as soon as the MS starts to store balance records and the role of the banks may be reduced (see step 3 above). Simultaneous with the link, one has to make a first choice with respect to the tax rate ($\boldsymbol{\tau}$)[21]. From the moment of linking, the credits on all current accounts become base money. We foretell that there is first too much base money ($\boldsymbol{f}$ too large). Also from that moment on all actors have the opportunity to lend base money to the banks. The savings deposits are included here. This base money is transferred to the B-account of the bank. So, this B-account has to be available then as well, and has to be linked to the GDP.

At the moment of linking, the credits on the existing current accounts become base money. These credits are partly based on bank loans. These loans are made available now in base money. Banks do not have so much base money and need a loan from the CB, through their C-account. So, these C-accounts have to be operational as well from the moment of linking. It is important to start with a sufficient large limit ($\boldsymbol{\tau}$) and a low interest rate ($\boldsymbol{r}$) on CB loans. Thereafter the monetary parameters can be tuned (see Section 4.4 and Appendix 4).

[21] Storing the balance records by the MS is essential for the way of linking that is proposed (each night, all amounts on all accounts). If the minimal variant is chosen, linking is also possible, but it necessitates a somewhat more complicated way of linking, e.g. combined with the transactions.

6. Conclusion

This paper is meant to contribute to the debate on the role of banks in the financial and monetary system. The Stichting Ons Geld in the Netherlands, inspired by the Positive Money (PM) movement in the UK, has focused the debate to the question whether the creation of money should not be an exclusive task for the government. The minister of Finance has asked for a recommendation of the Dutch Scientific Council for Government Policy (WRR). We hope our paper can be of help.

The most natural way to remove the creation of money from the banks, is to make the base money available for all economic actors. Base money consists of coins and bank notes and of the reserves of banks and government at the CB. In the form of coins and bank notes it is already available for all actors. But that is not a form that is very handy. PM proposes that base money in the form of reserves at the CB is also going to be accessible for everybody, and that base money is going to be the only legal tender. The advantages of such a revision of the monetary system (more stability and a better guaranteed utility function of storage and payment) are broadly acknowledged. But that has not led yet to acceptance of the proposal in the world banks and politics.

We followed the PM principle but have elaborated it in three directions.

- Abolish cash (coins and bank notes). The information technology that is available makes this possible and attractive.
- Create a new monetary system (MS) to store and transfer base money. Banks are not any longer between the CB and the economic actors but next to the economic actors. They provide extra services, on top of the public utility. And they are essential in making savings and credit from the CB available for the pre-financing of capital investments.
- Develop monetary policy with base money amounts on individual accounts linked to the GDP. In this way the buying power of the amounts can be guaranteed without continuous and extreme actions of the CB.

We have taken into account the objections to such a system: too little flexibility in credit provision and mixing fiscal and monetary policy.

We do not advocate a e-currency system like the bitcoin (see Appendix 3). These systems do not want a centralized system at all and no governmental control. The price they pay is exorbitant computer power and energy consumption. We believe that the government is the right party to provide the monetary system and to determine the monetary policy, of course with separated authorities. Another difference between the bitcoin and our system is that the bitcoins system has individual ‘coins’ and we only have ‘amounts of money’. The available information technology makes ‘coins’ a bit old fashioned.

The most important sections are Sections 3 and 4. In Section 3 we have sketched a new monetary system where all actors have one or more A-accounts with basic money. There is a payment protocol with high privacy and security for all actors (see Appendix 2). The essential cryptography is introduced in Appendices 1 and 3. Banks have besides A-accounts also B-accounts with base money that is partly borrowed from actors that have a temporary surplus and partly form the Central Bank. This account corresponds to the investment pool in the proposals of PM. In Section 4 we developed the GDP-link for the (amounts of) base money on all individual accounts. The monetary policy is represented by four parameters, (1) the proportionality of the total amount of base money to the GDP, (2) the tax on base money, (3) the limit on the credit space of the CB and (4) the interest due for that credit. In Appendix 4 the possibility to choose these parameters adequately is elaborated. This should lead to a stable monetary policy. The process of implementation and migration is dealt with in Paragraph 5. A stepwise implementation is advised with a gradual fine tuning of the monetary parameters.

The conclusion is that it is possible in this way to design and implement a robust monetary system. Recently the SFL (Sustainable Finance Lab) organized a survey with questions about who (according to the interviewee) creates he money and who is supposed to create it. It is not surprising that by far the majority of the people thinks that the government is doing this and that it should be the government indeed. It seems that the current system is unnatural: money based on claims which are rarely effectuated. This seems only understandable by experts. The real problem is that draconic measures are necessary to keep the system running. Despite these measures the system is spinning out from time to time. For each engineer this smells like a bad design. The objection to this observation will be that the monetary system is not designed but grown by some organic process. Our answer is then: “Is it not time to govern the further growth by a good design?”

We have sketched such a design in this paper. Starting point is that money should be *objective, ‘positive’* and *hard*. This is possible. In our proposal the ownership of money is independent of the role of the banks. It is hard because it is linked with the GDP.

About the authors

Kees van Hee and Jacob Wijngaard both have a PhD in mathematics and are emeriti professors in respectively computer science (TU/e) and business administration (TU/e Eindhoven and University of Groningen). The first author has also been management consultant during 16 years among others a partner at Deloitte.
E-mail adresses: k.m.v.hee@tue.nl and j.wijngaard@rug.nl
Website: www.robuustgeld.nl

Appendix 1: Cryptography in a nutshell

An *asymmetric encryption system* has two *keys*, a *secret* key S, that should be known only to the owner and a *public* key P that is publicly known (e.g. in a public register). A key is a big number (with a magnitude of 100 digits) and the encryption system contains an algorithm that makes a key to behave as a *function* which transforms an arbitrary (big) number (or more general a character string) into another number (or character string). We will consider these keys S and P therefore as functions. So if we apply S to a number A then we obtain a number B and we denote this by S(A)=B. The keys S and P are each others *inverse,* which means that if we apply S to a number A with result B and if we apply afterwards P on B then we obtain A again. So for each number A we have: P(S(A))=A and also S(P(A))=A! If you only have one of the keys it is practically impossible to find the inverse. With 'practically impossible' we mean that it takes ca. 100 years of computing on a large computer network to find A if you only have B and that you know that S(A)=B. The most famous asymmetric encryption system was published in 1977 and is called RSA, after its developers Rivest, Shamir en Adleman.[22]

With such a pair of keys one is able to create a *digital signature*: an actor X sends a message to an actor Y and wants that Y knows that it is coming from him. Then X sends: [from:X, Sx(X), content, to:Y]. Because only X knows S_X the value Sx(X) can only be computed by X. The receiver Y can find the public key of X (note that X is mentioned in the message) and so he can verify $P_X(S_X(X))=X$. However this message can be intercepted and so everybody may read it. If X wants this message only readable for Y then X should encrypt the total message with the public key of Y:
P_Y([from:X, Sx(X), content, to:Y])
and then Y can read it by applying its secret key:
$S_Y(P_Y([from:X, Sx(X), content, to:Y]))=[from:X, Sx(X), content, to:Y]$

Another instrument of cryptography is a *hash function*. Such a function is also realized by an algorithm. An hash function H makes from a big number (or a character string) a shorter number (or string). So H applied to a string A gives as shorter string B: H(A)=B. The goal is to have a shorter representation of the first string, so to *identify* the original string from the shorter string. But this is in theory impossible because there exist several long strings that are mapped by H to the same short string. In practice this seldom happens, because the number of big strings that we use is 'neglectable' small compared to the total number of strings on which

[22] Rivest, R.L. ,A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM (1978); Elgamal,T, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory v31, (1985)
Handbook of Applied Cryptography CRC Press (2001)

we could apply the hash function. Hash functions are not injective and also not invertable such as the key pairs of an asymmetrical encryption system. But it cost very much computing time to find a string A if you know B and if you know that H(A)=B. A frequently used hash function is called SHA-256 (Secret Hash Algorithm 256)[23] which is developed by NSA.

That is why hash functions are also used to protect the *authenticity* of data. For instance if one wants to send a message A and one wants to guarantee that the message will not be altered during sending, then one sends A and separately H(A). If the receiver reads B instead of A he can see that the message is manipulated because when he computes H(B) he sees that it differs from H(A). The same system can be applied to files. At the moment a file A is stored the value H(A) is computed and stored separately. As soon as the file A is retrieved one also retrieves H(A) to check if file A has been altered. The probability that such a manipulation will not be detected is neglectable. A classic example of a very elementary hash function is the *check sum.* To protect a large number against manipulation one adds the sum of the digits separately. And one can verify the transmission by computing the sum of the digits of the received number and compare this with the check sum sent. No guarantee can be given of course since it is possible to make two errors that compensate each other in the sum.

[23] H.Gilbert, H. Handschuh, "Security analysis of SHA-256 and sisters", Selected areas in cryptography 2003, pp175-193

Appendix 2: Payment protocol

Here we describe in more detail the protocol for a standard payment, mentioned in Section 3.2. There are of course variations possible, here we present the essential steps:

1. X sends a message to Y, encrypted with the public key of Y and provided with its own 'signature', i.e. the message has an additional field with the content of the message encrypted with the secret key (S_X). There is a unique transaction number N of X :
   P_Y([from: X, amount: B, to Y: trnr: N, S_X (X,B,Y, N)])
   a. Y decrypt this message with its secret key S_Y with result:
      [from: X, amount: B, to: Y, trnr: N, S_X (X,B,Y,N)]
   b. With the public key of X, P_X , Y can verify the signature of X:
      $P_X(S_X(X,B,Y,N))=(X,B,Y,N)$
2. Now Y should decide to accept or reject the payment. If so, then Y sends a confirmation in the form of P_X([from: Y, S_Y(X,B,Y,N)]) and otherwise a reject message is sent and the protocol stops.
3. X sends now this confirmation from Y with two signatures to the MS:
   P_{MS}([from: X, amount: B, to: Y, trnr: N, S_X(X,B,Y,N],),S_Y(X,B,Y,N),]),
   MS is able to read this with S_{MS} , P_Y en P_X. So the MS can verify that X and Y have authorized the transaction.
4. X sends now his current balance record that is produced and encrypted by the MS with the secret key of the MS:
   P_{MS}([acnr:X, balance: A_X, seqnr: M_X, S_{MS} (X,A_X,M_X))).
   M_X is the unique sequence number given by the MS at the last update event of X.
5. Idem for Y: P_{MS}(acnr:Y, balance: B_Y, seqnr: M_Y, S_{MS} (Y,A_Y,M_Y))).
6. MS reads these records with its secret key and decrypt it with its own private key. MS verifies if the balances are the current ones i.e. if the sequence numbers are the last ones. Then the MS increases the balance of Y with B and decreases the balance of X with B and sends these records to X respectively Y:
   P_X([acnr:X, balance: A_X-B, seqnr:M_X+1, S_{MS}(X, A_X-B,M_X+1]) and
   P_Y([acnr: Y, balance: A_Y+B, seqnr: M_Y+1, S_{MS}(Y,A_Y+B,M_Y+1])

The sequence numbers of the balance records are increased by one and remembered by the MS. Note that X and Y can read their own records with P_{MS} but they can't change it; the same for the sequence numbers.

In the variant we propose (variant 3) the MS also remembers the balance records of the accounts. Steps 4 and 5 are then superfluous and in fact the sequence numbers don't have to be remembered, but it is an extra security.

Appendix 3: Bitcoin and blockchain

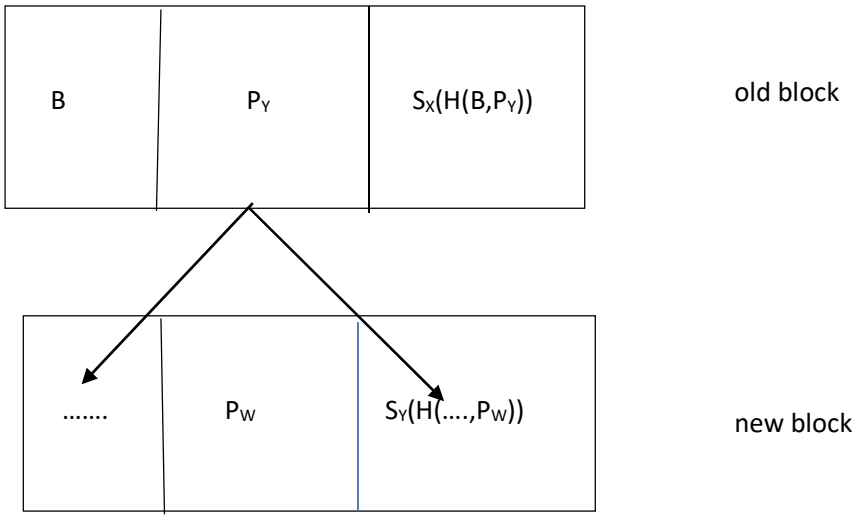
The bitcoin[24] is an alternative digital coin. In the past coins were made out of scarce materials such as silver or gold and the value of the coin corresponded to the value of the amount of material the coin was made of. Later coins and bank notes were made in a way that it was very difficult and costly to reproduce them, so that it did not pay of to forge them. The bitcoin is based on a comparable value: it takes years of computing on a tremendous large computer network to compute a new bitcoin. Only the energy consumption of this network cost more than the value of the bitcoin. (The first bitcoins were relative easy to compute but it becomes more difficult all the time.)

The bitcoin system has individual coins each represented by a very big number. The numbers that represent proper bitcoins have to be mapped by the hash function SHA-256, H for short,(see Appendix 2) onto a number that starts with a prescribed number of zero's. (Note that normal numbers never start with a zero, but we may think of these numbers as decimal fractions). It costs a huge amount of computing time to find such a number. The process of computing such a number is called *mining* and the required amount of computing time make the bitcoins scarce. To verify if a number A is a bitcoin takes relatively little time, one has to compute H(A). But mining a number with a prescribed number of leading zero's requires trial and error, which takes a lot of computing time. This is called a *proof-of-work.* The fresh bitcoins receive besides the unique number also the public key of the miner (the discoverer). So a bitcoin is a pair: [bitcoin-number, P_{miner}(miner)]. To keep this bitcoin safe the miner can encrypt the bitcoin with his public key and later transform it back with his secret key.

To *transfer* a bitcoin B from actor X to actor Y proceeds as follows: a new version of the bitcoin is created in which its *history* is stored. For a fresh bitcoin it is B=[bitcoin-number, P_{miner}]. A bitcoin with representation B gets after transfer from X to Y a representation B' with record [B, P_Y, S_X ((H(B), P_Y)]. So we see here the old bitcoin B, the public key of the new owner Y and the signature of the former owner X, namely the encryption of the former data with the secret key of the former owner. If Y transfers the bitcoin to W the new bitcoin is B":

[24] Satoshi Nakamoto, "Bitcoin: a peer to peer electronic cash system", www.bitcoin.org

$B'' = [B', P_W, S_Y(B', P_W)] = [[B, P_Y, S_X(H(B), P_Y)], P_W, S_Y([B, P_Y, S_X(H(B), P_Y)], P_W)]$.



With the bitcoin we can reconstruct and verify its *history*: with the public key of the former owner (P_X , readable in B) we can verify the public key of the new owner Y (not his name!), by calculating $P_X(S_X(H(B),P_Y))=(H(B),P_Y)$. So it is impossible to forge the bitcoin, since the former owner confirms with its secret key who the next owners is. To increase the privacy it is possible for an actor to use in each transaction a fresh pair of keys (P and S) . He only has to remember per bitcoin its secret key, because if he wants to transfer the coin he has to sign it with the proper secret key that belongs to the private key in the bitcoin, e.g. in the chain above S_Y in the new block belongs to P_Y of the old block. A bitcoin owner must have a wallet with a list of its bitcoins and proper private keys and may be the appropriate public key P. This wallet can be stolen!

The big problem of the bitcoin system is to exclude that the same bitcoin is spend twice, because all digital data can be copied. Our monetary system as described above, provides a simple solution: the central infrastructure gives a bitcoin in a new transfer a new sequence number encrypted with the secret key of the monetary system. So the MS can verify if a bitcoin has the current sequence number. If there are more copies of a bitcoin only one can get a new sequence number by the MS and so the other copies are immediately obsolete.

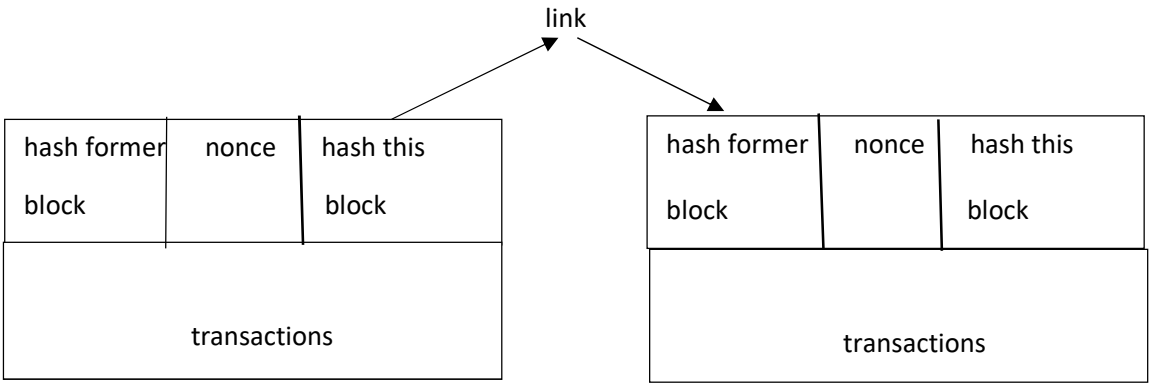
But the real bitcoin system does not want a central infrastructure, even if it only keeps track of sequence numbers. Therefore another mechanism is developed that also makes use of the proof-of-work principle: the *blockchain*. A blockchain is a public distributed database in which all confirmed transfers of bitcoins are stored. (Note that a bitcoin contains all information of its

transfers.) There are about different 4000 bitcoins per block, but that number is irrelevant. The blocks are linked together by a reference to the former block. Therefore we speak of a chain. Everybody may read the blocks of the chain but nobody can change the chain without corrupting it because the blocks are protected with a difficult to hack hash of the content of the block. Here the proof-of-work appears as we shall see later.

At each transaction a bitcoin obtains a new representation and it is broadcasted by the new owner to all computers in the bitcoin network. These computers are called nodes and it is required that there is a large number of them to keep the system safe. Each node collects new bitcoin representations and verifies them in two ways: (1) the node checks in the bitcoin if always the former owner has approved the transfer with its secret key and (2) the node checks if the bitcoin already occurs in the current blockchain (which means that the bitcoin is almost spend twice). As soon as one of the two checks is negative, the transaction, i.e. this version of the bitcoin, is deleted and this information can be broadcasted to the other nodes. Otherwise the bitcoin version is added to the waiting list of the node. So there is a publicly known blockchain with all verified current bitcoin representations.

The nodes are continuously busy trying to add a new block on the chain. To do so they have to deliver a proof-of-work. Therefore they collect a number of verified new bitcoin transactions and put them into a block. Then they have to add some data: (1) a hash of the former block in the chain and (2) a nonce which is an arbitrary character string. The content of the new block together with nonce have to be hashed. Only if the hash has a prescribed number of leading zero's the block is correct. By varying the nonce this goal can be achieved, but it requires a serious amount of computing effort. (There are techniques, e.g. the Merkle tree, to do this relatively efficient.) If a correct nonce is obtained the block is ready to be added to the blockchain. This is almost the same process as mining new bitcoins and therefore it is also called 'mining'. The requirement of leading zero's is less strong her and therefore it does not take so much computing effort as mining of a new bitcoin. If you want to change a block in the chain, then you have to change all successor blocks as well and this while other nodes are busy to add new blocks. This practically impossible. In practice every 10 minutes a new block is

added.



The area of the fields in the diagram above do not reflect the amount of data: the transactions area should be much bigger than the rest. The transactions form the *body* of the block and the hash of the former block, the nonce and the hash of the current block form the *header* of the block. The hash of the block is computed by applying H to the string consisting of all transactions, in a row, together with the hash of the former block and the nonce.

The blocks are linked, because each block contains a hash of its predecessor. If one has one block it is possible to search the whole distributed database till one has the predecessor. It is of course possible to organize this more efficiently by maintaining a table with the block hashes and their address (url).

Nodes always try to work on the last block in the chain. As soon as a new block is added the nodes stop their activities, remove bitcoin transactions from their waiting list that already appear in the new block and start building a new block. It may happen (and it has occurred already in practice) that two new blocks are published simultaneously. Then the nodes continue with these two blocks as potential last ones. As soon as a new block arrives that fits with one then that one is chosen and all nodes continue with the longest chain. So a receiver of a bitcoin has to wait to be sure that the transaction is correctly added to the blockchain and it is even better to wait till more blocks are added. This is time consuming and therefore it is not feasible for shop payments. Somebody who tries to spend a bitcoin twice should do this very fast, since the first transaction is already processed in a new block. Only with a very small probability a second transaction may appear in another new block that appears at the same time. Then there is a problem which implies that one of the receivers is passed and the other one obtains the bitcoin. But the current bitcoin will never appear twice in the block chain.

With many payments one needs more than one bitcoin, or only a fraction of it, like paying with cash. So the change is needed. Although this is extra work, it is straightforward to process.

The question arises: Why are nodes interested in performing all this work to verify blocks and to create new ones? The incentive is a reward for adding an new block. At the moment there is a transaction fee of ca 2% for the miners of a new block.

There are several drawbacks of the bitcoin system: (1) payment with coins created the need for change which makes the transactions more complicated, (2) the slowness of the process of confirmation of transactions makes it infeasible for real-time payments like the ones in shops, (3) the huge computer facilities to run the system on a world scale. The energy consumption for this facility is estimated to be equal to the total energy consumption of Ireland.[25].
Advantages of the bitcoin system are: (1) no need for a central system, (2) bitcoins are 'positive' money, not claims, and its scarceness creates its value, (3) all transactions are saved so the whole history can be reconstructed, but this is time consuming.

The blockchain mechanism is also applicable for other forms of 'positive money' systems, for instance with shares or bonds who also can be identified by a unique number.

[25] K. O'Dwyer, D. Malone, "Bitcoin mining and its energy footprint", Irish signals and systems conference (2014)

Appendix 4: GDP-linking and amount of base money

The amounts of base money on the individual accounts (A, B and C) are going to be linked with the (nominal) GDP. That means that the base money amounts are going to be made proportional to the GDP. If the real GDP does not change, the base money amounts rise and fall with the prices and the buying power of the account balance remains constant. If there is also an increase in real production, the buying power increases with this production increase. To prevent shocks and speculation around these shocks, it is necessary to adapt the amounts frequently. Preferably daily. So, we need a daily estimate of the GDP. To this end we use the sum of the transactions for the production, distribution and sales of real goods and services during the last year (the "real" transactions). That sum can be monitored by the MS if the transactions are labeled properly (see Section 3).

More precise now:
Let $B(t)$ bet he GDP of the past year, at the beginning of day t, and let $\hat{B}(t)$be its estimate.
Let $P_r(t)$ bet he sum of all "real" transactions (goods and services) during the past year, at the beginning of day t.
The big difference between $B(t)$ and $P_r(t)$ is that in the latter quantity, the transactions in the supply chains are also counted. So, the fragmentation of the production has an important impact. But if this fragmentation does not change to quickly, and that is what may be expected, it holds that $B(t) = \beta(t)P_r(t)$, with $\beta(t)$ a (proportionality) constant that changes only slowly with t. Each time a new formal estimate of the GDP becomes available, a new estimate of $\beta(\cdot)$ can be determined. Let the GDP-linking be active from day t_0 on. Assume that the most recent, official estimate of the GDP, B^-, regards the year period finishing with day $t^- - 1$ and that there is an estimate β^- of the proportionality constant. Then the GDP-estimate at the beginning of day t_0 is equal to $\hat{B}(t_0) = B^- \cdot (P_r(t_0)/P_r(t^-))$. Thereafter we update the estimate with $\hat{B}(t) = \hat{B}(t-1) \cdot (P_r(t)/P_r(t-1))$, until a new, official GDP estimate, B^*, becomes available. Assume this happens at day t_N and regards the year period finishing with day $t^* - 1$. Then, on day t_N the estimate is corrected with a factor $B^*/B(t^*)$. To reduce the jumps, the correction can be smoothed over a couple of days (the product of the correction factors has to be equal to the total correction factor)

This labeling real/non-real is not completely trivial. It is necessary to exclude transactions from the so called FIRE sector (Finance, Insurance, Real estate and Equity) and transactions due to government subsidies and income transfers. It is important that the labeling goes automatically. This can be realized by using the categories of actors that are distinguished already by CB's, e.g. the ECB. Each account belongs to one or more of such categories. Transactions between

households are excluded. The same for transactions with financial corporations. For government transactions it is necessary to make further distinctions. But this may not be a problem. Real estate and other trade in finished goods between corporations looks most complicated. Maybe for real estate, the role of the notary helps. It may not be expected to find a 100% precise way to label. the transactions. It is worthwhile to explore the different options of labeling real transactions The more stable $P_r(t)/B(t)$ is, the better it is. The (official) GDP estimation procedure and the VAT procedure are useful points of reference.

The GDP-linking of the base money amounts on the individual accounts implies also that the total amount of base money is proportional to the GDP(-estimate): $M(t) = \boldsymbol{f} \cdot \hat{B}(t)$. This proportionality is not disturbed by the tax on base money, as long as the tax is added to an A-account of the government. The proportionality of amount of money with GDP is generally considered to be normal[26]. It can be disturbed by disproportionally many financial transactions. It is useful to refer also to the quantity equation of Fisher here. ($MV = PT$). In our terminology and restricted to the real transactions that equation leads to : $M(t) \cdot V_r = P_r(t)$, with V_r the (average) velocity of the base money for real transactions. And, since $B(t) = \beta \cdot P_r(t)$, we have $M(t) = (B(t)/V_r \cdot \beta)$ en $\boldsymbol{f} = 1/(V_r \cdot \beta)$.

The constant $\boldsymbol{f}$ is the first monetary parameter. The choice of $\boldsymbol{f}$ is related to the fragmentation of the production and the velocity of the money for real transactions. This fragmentation is changing a little all the time, and by the application of supply chain finance and comparable forms of network financing, the actual fragmentation can be reduced[27]. But the factor β is anyway stable and can be determined. So, $\boldsymbol{f}$ depends mainly on the velocity of the base money. Suppose, an owner keeps base money in average for 0.2 year before he uses it. Then $V_r = (1/0{,}2) = 5$ and if base money were only necessary for working capital and housekeeping money, $\boldsymbol{f} = 1/(\beta \cdot 5)$ would be sufficient.

There is also base money needed for financial transactions. Although these transactions are often settled in another way, base money may be useful to switch from one asset to another in a portfolio. Suppose each asset is replaced every two years and it takes a two weeks interim period: the old asset is sold first and the new one is bought two weeks later or a loan is acquired to buy the new asset two weeks before the old asset is sold. That contributes an average of 2% of the total value of all portfolio's to the amount of base money that is required. Given that the total private wealth is about equal to 6 times the GDP (compare Piketty[28]) that is

[26] See e.g. Bezemer, "Finance and Growth; when Credit Helps and when in Hinders", INET, 2012
[27] See e.g. Van der Vliet, "Concepts and Trade-Offs in Supply Chain Finance", PhD thesis TU/e, 2015
[28] Thomas Piketty, "Capital in the Twenty-First Century", Harvard University Press

12% of the GDP. Added to the requirement for working capital and housekeeping money, this would lead to a requirement of $\boldsymbol{f} = 1/(\beta \cdot 5) + 0.12$.

This is just an example, to illustrate that it is possible in this way to determine a first reference point for $\boldsymbol{f}$. The choice of $\boldsymbol{f}$ can be refined by trial-and-error, monitoring the way banks use their C-accounts.

Banks can borrow base money through their C-account. They are allowed to have a negative balance on this account. This facility is meant to be sufficiently flexible with respect to credit supply for large investments. Investment and savings are equal by definition ($I = S$), but that does not imply that there is a specific saving that is linked right away to this specific investment. Suppose a machine is bought. As long as the machine has not been paid for, the supplier finances the machine. A possibility is to keep it so, the user leases from the supplier. In that case the investment has found the corresponding saving. But generally it does not work that way. Then it is useful to have a bank that can pre-finance. Banks have to be directed to couple investments with (private) savings. But this takes some time. In estimating the amount of base money that is necessary for this pre-financing, it is necessary to know how long it takes to couple an investment with savings and also how large the investments are. The gross capital formation in the Eurozone is about equal to 20% of the GDP. Suppose it lasts in average 1 year to couple an investment with savings. Then there is $0.2B(t)$ credit space required. That is the base money that is made available through the B-accounts should be equal to $0.2B(t)$. Part of that is supplied by the CB (through the C-accounts). That part can be made (proportionally) dependent on what is made available by other economic actors. This is controlled with the monetary parameter $\boldsymbol{g}$. Trial-and-error can be used to check which factor $\boldsymbol{g}$ is necessary to make the total credit space through the B-accounts equal to what is necessary for the capital formation ($0.2B(t)$ here).

Monitoring the use of $\boldsymbol{f}$ and $\boldsymbol{g}$ is important. If $\boldsymbol{f}$ is too small, one may expect pressure on the credit limit for the C-accounts ($\boldsymbol{g}$)and the tendency to use this credit space also for working capital and for purely financial transactions. If $\boldsymbol{f}$ is too large, one may expect that the superfluous base money is made available eventually to the B-accounts or that actors start to use more base money for the renewal of their investment portfolio. If the credit space through the B-accounts is too large, banks get less sharp in making the pre-financing period small and/or start to use this credit for financial transactions. It is essential to guide this fine-tuning of $\boldsymbol{f}$ and $\boldsymbol{g}$ by estimates of the base money requirement as derived above. Without such reference points, the process gets easily too dynamic.