# Cryptocurrencies from an Austrian perspective[*]

Alistair Milne[†]

First version April 4th, 2017; this version 18th May, 2017[‡]

Abstract

Placing bank and fiat money *off balance sheet,* using the distributed transaction technologies of Bitcoin and other cryptocurrencies, avoids the need for centralised payment settlement (in central bank money). Just like earlier proposals for 'narrow-banking' or 100-percent reserving this prevents bank failure disrupting monetary transactions. Unlike those earlier proposals banks can continue using fractional reserving with '$x$-percent reserving' offering fine-grained control of unsustainable money and credit expansions. This reform helps achieve monetary outcomes desired by the Austrian school of economics: reducing the need for bank regulation, lender of last resort and bank bail-out. (93 words)

JEL codes B53, E42, G21

Keywords: 100-percent reserved banking, Austrian school, bank payments, bank regulation, bank reserves, Bitcoin, blockchain, central banking, central counterparties, the Chicago plan, clearing and settlement, credit money, cryptography, commodity money, decentralised counterparties, digital currency, distributed ledgers, electronic currency, fiat money, fiduciary media, financial crises, financial stability, fintech, fractionally reserved banking, funding liquidity, the gold standard, laissez-faire economics, lender of last resort, macroprudential, maturity mismatch, medium of exchange, monetary arrangements, monetary policy, monetary technology, money markets, money substitutes, mutual payments networks, narrow banking, payments infrastructure, payments systems, ring-fencing, systemic risk, Volcker rule

Citation: Milne, Alistair, Cryptocurrencies from an Austrian Perspective (April 17, 2017). https://ssrn.com/abstract=2946160 or http://dx.doi.org/10.2139/ssrn.2946160

[*] The hospitality of the Department of Banking and Finance, Monash University, Melbourne, has given me the best possible supportive environment for writing this paper. I am grateful for comments from Denys Firth, Charles Goodhart, Harry Leinonen, David Mayes, George Selgin and seminar participants at the Reserve Bank of Australia and Australian National University.

[†] Loughborough University, UK; email: a.k.l.milne@lboro.ac.uk

[‡] This is a substantial revision of draft released on SSRN on 17th April, 2017, with the detailed material on cryptocurrencies (previously Section 2) in Appendix A and a new section 2 on bank payment and settlement.

## Contents

## 1. Introduction and motivation

This paper proposes using the technology used for recording cryptocurrency transctions as a way of preventing bank failures disrupting bank payments or access to bank money. This protects payments and bank money from systemic risk, without the interference in the commercial decisions of banks such as that caused by risk-fencing in the UK or the Volcker rule in the US.

This would be a fundamental change in monetary arrangements. Importantly, central bank reserves would no longer be required for settlement of bank payments, instead all bank payments however large or small would be finalised by a near-real time updating of the transaction – the sender and the recipient—on a state-sponsored mutual distributed ledger, a time-ordered and immutable transactions record.

Why is this an Austrlian perspective? Some have argued cryptocurrencies are 'Austrian' because they are potential competition for fiat currencies, independent of the state, that can operate effectively alongside state fiat currencies and so undermine state exploitation of monetary arrangements.[1] These arguments are not very persuasive. Cryptocurrencies have effectively demonstrated that it is possibile to have decentralised recording of transactions. Still, the substantial volatility in the prices of cryptocurrencies such as Bitcoin and Ether , the limited scalability of cryptocurrency networks, and the lack of liquidity in cryptocurrency exchanges suggest that there c an be no meaningful adoption of cryptocurrencies in daily corporate, government or personal transactions.

This paper offers a different Austrian perspective. It is argued that using the technology of cryptocurrencies as proposed here can achieve two of the major objectives of Austrian monetary thought: limiting state support for banks from lender of last resort and bank bailout; and discouraging fractionally-reserved unsustainable money and credit expansion, while still retaining the valuable elasticity of money and credit that fractional-reserved banking supports.

The proposal is as follows. Abank payment transaction works by debiting a transaction account (an account that offers payment facilities) and crediting another account and are finalised by a settlement of the transaction through an accompanying transfer of bank assets, nowadays almost always reserves held with a central bank.

With the technology of cryptocurrencies these transaction accounts no longer need to be held on bank balance sheets. Instead they can be placed off balance sheet on a single mutual distributed ledger (a 'blockchain' similar to that used by Bitcoin and other cryptocurrencies, but state sponsored not private). This is actally much simpler than the bank payment arrangements evolved over the past two centuries. With all bank money and government fiat money recorded off-balance sheet on a single distributed ledger there is no need for subsequent settlement. Should a bank fail, the bank's customers maintain uninterrupted access to their money, receiving salary, business receipts and other income into their transaction accounts and make payments from them for goods and services.

Will the transfer of all money onto a single ledger shared by government, banks and all their customers not undermine confidence, leading to a 'dollarisation', a turning away from state

[1] For example (Koenig 2015), an entertaining but rather proselytising introduction to Bitcoin and its supporting Blockchain ledger, explicitly invokes the link to Austrian economics in both title and text. His book – as well as describing the technology for non-specialists and documenting some of the viewpoints of those involved in the 'Bitcoin movement' – espouses the radical position that these technologies will prove to be a more profound technological development than even the internet, replacing the malign role of the nation state in both economics and politics. A wealth of websites and internet forums share similar viewpoints.

supported money on the distributed ledger to the use of something else? The analysis made here suggests that transfer of all money onto a single mutual distributed ledger can increase not undermine confidence. This is because it provides a better framework than we presently have for preventing such unsustainable money and credit expansion.

How does it reduce the role of the state? It also allows a reduction in the role of government in the intrusive and costly business of micro-prudential regulation, and resulting perennial conflict with the banking industry. The regulatory arms of the state can be privatised, becoming industry self-regulatory organisations. There will still be a role for a central bank as 'lender of last resort' to maintain liquidity and confidence in short term money markets, but this can be restricted to temporary provision of funds at time of panic and access to lender of last resort does not have to be automatically given to the bank or banks whose difficulties initially trigger the loss confidence.

Why is this arrangement better at preventing unsustainable increases of *fiat* money? The answer is that is not any better, but it is no worse. Just as now the issue of fiat money is controlled by an independent monetary authority (and could be fully backed by a commodity such as gold).[2]

Why is this arrangement better at preventing unsustainable increases of *bank* money and credit? A 'triple-lock' prevents banks engaging in unsustainable money-financed credit expansion: first, the obligation of the bank borrower to repay the money to the ledger; second, if the borrower defaults, the obligation of the bank to repay in place of their customer; third, if the bank itself defaults (which triggers bank resolution and loss of shareholder ownership and control), an obligation of the entire banking industry to repay to the ledger, in turn ensuring firm and effective self-regulation.

Why has this not been considered already, many years ago? The answer is technological change. Before the emergence of distributed ledger technologies this mutualisation of transaction deposits would have required a centralised institution responsible for maintaining account operations. Now it can be fully decentralised, with 'smart contracts' automatically executing participant commitments.

The resulting guarantee on obligations is similar to that already provided by central counterparties in OTC derivative markets but with no central point of failure. It is robust even in the event of such a devastating external shock (e.g. a nuclear holocaust) that the entire banking industry fails. Money on the ledger is not lost, it then becomes fiat money without any further obligation of repayment. Provided that the hardware and software remains intact (and appropriately designed it could even survive a nuclear holocaust, although individual access might still be a problem if the 'private keys' used to access the ledger are lost) monetary exchange continues.

If – despite the 'triple lock' and consequent monitoring and regulation by other banks – further limitation on fractional-reserved banking is desired, then simply amend the rules of ledger toward 100-percent reserved banking proposals to any desired degree.[3] This $x$ -percent reserving can be implemented, with $x$ anything from 0 to 100, by requiring banks to provide $x$ -percent of the funding of a loan on the ledger using existing money that the bank already has on the ledger.

This argument draws on three literatures: cryptographic security used in cryptocurrency networks (translating these methods from the technical language of computer science so they can be better understood by non-specialists); the network economics and systemic risk of money and

[2] (Leinonen 2016) emphasises the possibility of using distributed ledgers to support commodity backed money.

[3] The 'Chicago plan' proposal by Henry Simons and economics colleagues circulated from Chicago University in the 1930s and periodically supported by many prominent economists since (for example as 'narrow banking').

payments and bank credit (a topic on which the present author has written); and Austrian monetary analysis (to which the present author is sympathetic but has not actively contributed).[4]

The paper is organised as follows. Section 2 provides a critical historical review of our current arrangements for execution and settlement of payments, noting how these impact on the operation of monetary policy. Section 3 outlines the proposal for a single ledger for all fiat money, bank-money and bank loans. Section 4 discusses how it can support Austrian policy objectives. Section 5 concludes. Appendix A reviews the key features of cryptocurrency networks such as Bitcoin, explaining their operation without misleading analogy and correcting a number of common misperceptions.[5] Appendix B summarises the different views of money of scholars working within the Austrian school of economics and their varying proposals for improving monetary arrangements.

[4] To date there has been only limited work within the Austrian tradition on cryptocurrencies. Contributions discussed here are (Dowd 2014; White 2014; Selgin 2015). There are also a number of student dissertations exploring the links between Cryptocurrencies and the Austrian school (e.g. Potashnik 2015; Ólafsson 2014).

[5] This section, which took a considerable effort to write because of the author has no background in computer science, seems to be a contribution in itself; providing a succinct statement without unnecessary technical detail of cryptocurrency operation for regulators, central bankers and payments professionals.

## 2. Bank payment and settlement

The overwhelming proportion of payments by value in developed countries are transfers of money from one bank account to another. A variety of instruments and payment schemes are available to execute these bank to bank payments.[6] These all debit of the bank account of the sender of money (the 'payer') and credit the bank account of the recipient of the money (the 'payee'). If the two bank accounts are held at different banks then the payment also requires a matching interbank settlement i.e. a transfer of the same value from the payer's to the payee's bank.[7] Nowadays this settlement is almost always in central bank reserves.

While arrangements for bank payment and settlement are a fundamental part of the institutions of money and banking, they attract little attention either in money and banking textbooks or in the research literature. This section provides a short description of bank payment and settlement, before describing the potential reform set out in the remainder of the paper i.e. using decentralised cryptocurrency technologies to remove the need for centralised settlement of bank payments and so clearly separating monetary deposits from potentially risky retail investment in banks.

### The evolution of bank payments and settlement: a short historical review

Settlement is *not* an inherent and indivisible aspect of payments. For example non-bank payments using notes or coin, the physical transfer of money is final payment. Some bank payment instruments do not require settlement either. Historically, where not prohibited, banks often issued their own private notes which could be presented for redemption in non-bank money i.e. precious metal or coin. These privately issued bank notes passed from hand to hand and were used in payment without requiring transaction by transaction settlement. Similarly bills of exchange – i.e. documents issued by merchants promising to pay a stated sum of money at a stated future date – when 'accepted', i.e. the payment guaranteed by a bank, circulated as a form of bank endorsed money. Even today 'endorsed' cheques sometimes circulate as a bank money without need for transactions settlement.

[MOVE TO INTRODUCTION By using cryptocurrency technologies, all bank to bank payments can be carried out without any need for settlement, just as was the case historically for payments made using privately issued bank notes. From the customer perspective nothing much changes – they continue to use the same card, online and telephone instructions to initiative payments as they do today. They continue to receive statements of their balances in transaction accounts and of previous payment transactions. But the implications for banking stability are profound. There is no longer any possibility of settlement failure, i.e. a bank having insufficient monetary assets to fulfil its settlement obligations. As a result, it is argued here, it then becomes possible to withdraw much of the state support currently provided banks, through deposit insurance and the implicit 'safety net' provided by too-big-to-fail. ]

[6] For example in the UK a bank to bank payment can be made using the traditional paper instrument the cheque using the cheque and credit clearing scheme (CCCS); through a variety of instructions (direct debit, standing order, bulk payment instructions) via the bank automated clearing system (BACS), a card payment via either the Visa or Mastercard systems; an immediate direct online or telephone instruction via the faster payments scheme (FPS) or using the large value real time scheme( CHAPS).

[7] Settlement can be either at the same time the payment is made i.e. when the payer's account is debited and the payee's account credited ("gross settlement") or later ("deferred settlement"). If settlement is deferred then until it takes place the payer's bank has a liabirvlity for subsequent settlement to the payee's bank.

Interbank settlement emerged as a response to historical circumstance and technological change. Holding money in a bank rather than as precious metal, notes or coin offers advantages of both convenience and security. Even if the money must be withdrawn in order to make payments, fractional reserving by individual banks allows deposit-taking banks to provide monetary services with less opportunity cost from holding the unremunerated medium of exchange. Further convenience and cost reduction can then be achieved through payments that transfer directly from bank to bank, without requiring withdrawal at all. These efficiencies are maximised when the assets used for settlement can be centralised.

From the earliest history of banking, bank-to-bank payments have been possible through one bank holding a bilateral clearing account with another, the balances eventually and as necessary settled by transfer of a non-bank money.[8] Something similar to this arrangement continues today in international correspondent banking, where a bank can provide its customers with payment facilities outside its own domestic realm of business by holding a correspondent account with another bank overseas.

In the 18th and 19th century such correspondent relationships were also important part of domestic bank payments, with smaller regional or country banks holding accounts with institutions in financial centres. Examples include English and Welsh country banks holding accounts with clearing banks in London and local banks around the United States holding accounts with money centre banks in New York, Chicago and other ‘money centres’.

During the later 19th and 20th century these bilateral correspondent relationships  evolved into the now standard centralised holding of bank reserves as deposits with a central bank used for settlement of bank payments. Under the gold standard as first established in the UK with the restoration of convertibility of Bank of England notes in 1821 these reserves were claims on gold. Holding reserves of gold centrally supported a money market allowing banks to lend reserves amongst each other (in London the ‘discount market’ which operated by the sale and purchase of discounted bills of exchange) and hence made the most efficient use of limited metallic reserves.

A related parallel development was the growth of centralised cheque clearing. For example in London a formal bank cheque clearing organisation was established by 1833, allowing cheques between a group of banks to be periodically collected together and sorted in order that a large number of payment instructions could be settled together with a few interbank payments. From 1854 – with the volume of cheques cleared rising rapidly -- the London cheque clearings was settled through transfers of deposits at the Bank of England.

This shift to settlement of bank cheque payments using central bank deposits was the first step in the evolution from a pure gold standard in which domestic and international reserves were held as gold specie and coin, to a gold-exchange standard in which reserves were instead claims convertible into gold. A further development was a decline in the use of gold coin in day-to-day payments replaced by token moneys (state issued notes and coin in which the metal content was worth much less than the face value) and bank payments.

The shift to monetary exchange using token money, paper notes and bank deposit instruments settled in central bank reserves, facilitated the replacement of metallic monetary standards by ‘fiat’

[8] One early example described by (De Roover 1942)is that of the money changers operating in Bruges from the late 13th century, whose activities are recorded by the preservation of two of their account books. As De Roober, page 63, describes oral instructions for bank to bank payments could be financed by a corresponding debit or credit to a clearing account held by one bank with the other.

standards in which the reserve assets were no longer even convertible into gold. The abandonment of convertibility occurred three times: first as a consequence of the fiscal pressures of war finance in 1914; then again – after restoration of convertibility from 1925 – during the international financial crisis that commenced in 1931; and then finally and permanently – after the Bretton Woods fixed exchange rate system established convertibility in 1958 -- with the 1971 breakdown of fixed exchange rates amongst the industrial countries.

A further stage in the evolution of bank payments and settlement over the past half century has been the shift from paper-based and manual processing (cheque, giro, manual teller services for deposits and withdrawals) to the automated processing of a wide range of electronic and card payments in use today. This automation has supported another key development: today it is bank deposits rather than previous metal or government issued notes and coin which are effectively the medium of exchange; few adult citizens in developed countries are now without bank accounts, even those who rely on state benefits as income are nowadays paid electronically. Associated with this shift has been the widespread provision of bank deposit insurance, with an explicit or implicit state backing. Nowadays it appears to be a political imperative on government, regardless of where they are on the political spectrum, to protect the money held by citizens as bank deposits. Limiting the exposure of the tax payer to bank losses then requires close regulation and supervision of banks in order to limit their risk-taking.

## Central bank reserves and monetary transmission.

Accompanying the shift to settlement of bank payments using central bank deposits and the abandonment of convertibility into gold has been the increasingly important role of the central bank in determining short-term money market rates of interest. Figures 1 and 2 illustrate:

Figure 1: fractional reserved banking with central bank settlement

General Government/ Central bank

| *Assets* | *Liabilities* |
|---|---|
| Real assets | Reserves |
| C bank repo | Notes |
| | Bonds |

Commercial banks

| *Assets* | *Liabilities* |
|---|---|
| Bank Loans | Deposits |
| Reserves | C bank repo |
| Money market | Money market |
| | Bonds/ Equity |

Non-Bank private sector

| *Assets* | *Liabilities* |
|---|---|
| Real assets | Bank loans |
| Bonds/ Equity | |
| Deposits | |
| Notes | |

The right hand panel of Figure 1 shows a simplified balance sheet of the non-bank private sector. As discussed, most payments nowadays are bank to bank using bank deposit payment instruments, notes accounting for only a small proportion of the stock of money and of the value of payments.[9] Bank deposits include both transaction deposits used for making payments and other term or saving deposits, though the dividing line is not clear-cut for example savings deposits that allow immediate withdrawals can be regarded as money.

The middle panel shows the balance sheet of commercial banks. There are many competing commercial banks providing monetary deposits and payment facilities to the non-bank private sector. A deposit paid from Bank A to Bank B is settled through a matching transfer of reserves from bank A to Bank B. If Bank A loses reserves from an outflow of deposits, it can replenish them by money market borrowing; or by issue of bonds or equity purchased by the non-bank private sector using deposits from other banks.

[9] in the UK notes in circulation are around 3% of broad money including all bank deposits.

From an accounting perspective an extension of credit by commercial banks can always be financed by creating deposits. The resulting loss of deposits to other banks though imposes a discipline on individual banks engaging in such money-financed lending: an individual bank will only do this if it is confident of being able to replenish its reserves through money markets or security issuance at a funding cost that justifies the risks being taken in lending. The same discipline does not however necessarily apply to the banking sector as a whole: the practice of fractionally reserving makes it possible for the sector as a whole to increase its lending without needing to raise funds in money or security markets and they will do so provided they perceive sufficiently profitable lending opportunities on a risk-adjusted basis to cover any additional regulatory and liquidity costs of credit expansion.

The left hand panel of Figure 1 is a simplified consolidated balance sheet of general government and the central bank. This presentation highlights the role of central bank reserves (deposits with the central bank) as a source of government funding, something that was a principal reason historically for governments chartering central banks and has again become important with the policies of quantitative easing adopted since the 2007-2008 global financial crisis. The abandonment of convertibility though means there is a major difference from central bank funding of government in the 18th century and today: then the central bank deposits could be withdrawn by conversion into specie, now central bank reserves are inconvertible and can only be transferred to other banks as settlement of bank payments.

Figure 2: central bank reserves and overnight interest rates

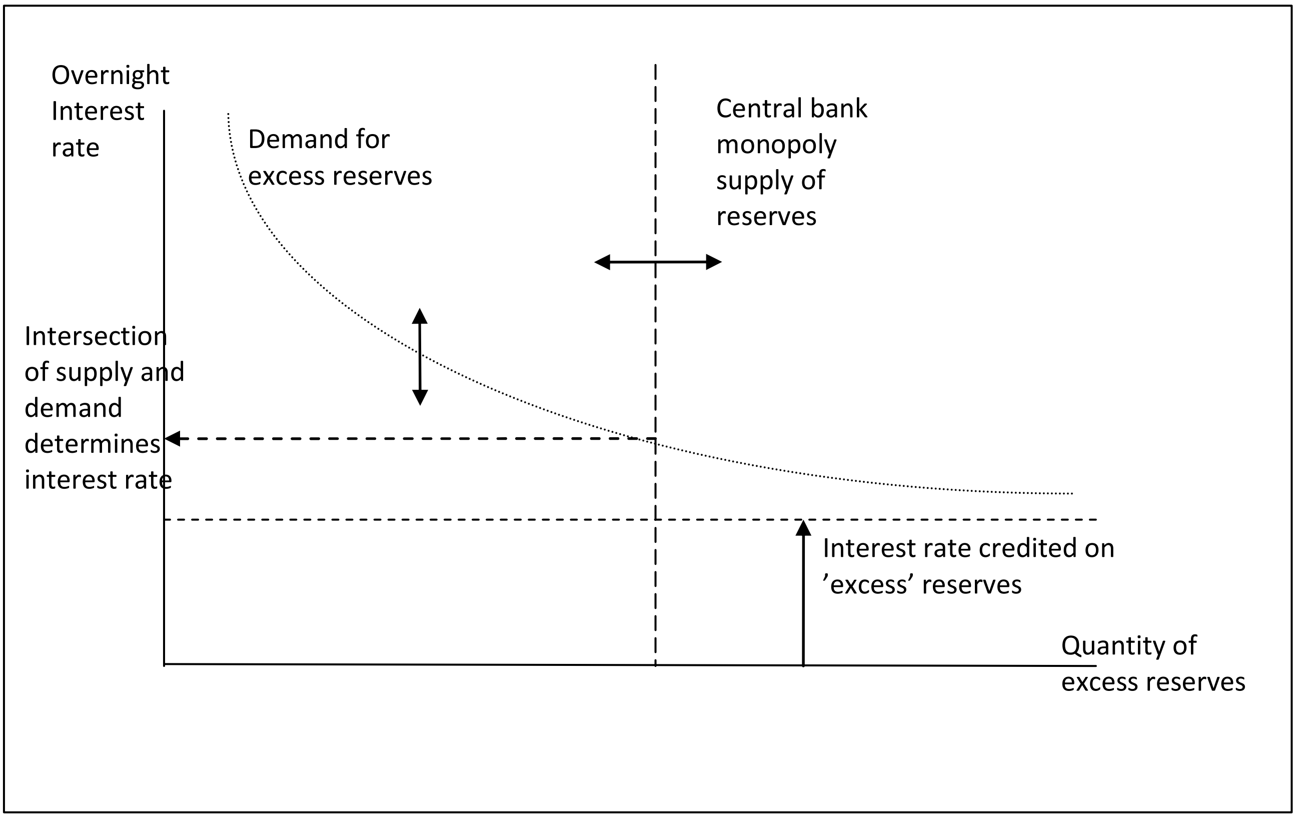
Overnight Interest rate
Demand for excess reserves
Central bank monopoly supply of reserves
Intersection of supply and demand determines interest rate
Interest rate credited on ’excess’ reserves
Quantity of excess reserves

Figure 2 illustrates the resulting demand and supply for reserves and the consequent determination of overnight interest rates. The horizontal axis is the quantity of excess reserves held by commercial banks (in excess of any minimum reserve requirements should these be applied).[10] The central bank may choose to offer remuneration on central bank reserves, as indicated by the horizontal dotted line. The demand for reserves is an aggregation of desired reserve holdings by individual commercial banks. This demand arises because of the role of central bank reserves in settlement and depends on the overnight money market rate of interest as measured on the vertical axis.[11]

Each day every commercial bank faces a choice between investing excess reserves in the money market or holding them in anticipation of unanticipated settlement of payments and earning whatever interest rate is credited by the central bank. The higher the money market rate of interest the more willing the bank is to lend reserves into the money markets, managing with a smaller margin of excess reserves and the possibility of having to pay an additional  cost of last minute borrowing of reserves (from the market or the central bank) in order to settlement unanticipated payments.

The vertical dashed line in Figure 2 shows the supply of central bank reserves which is determined by the central bank. The intersection of supply and demand determines the overnight interest rates. In practice, under the orthodox monetary operations that preceded quantitative easing, the central bank chose a target level for the overnight interest rates and adjusted the supply of reserves to ensure that overnight interest rates was at or close to this target.

The supply of central bank reserves is provided through ‘open market operations’ i.e. purchase or sale of securities such as government bonds or (not shown in Figure 1) foreign exchange assets; and, most important for short term operations, through repo (sale and repurchase agreements) with commercial banks, a form of secured lending in which the central bank creates and loans reserves to commercial banks.

The reason for controlling money market interest rates rather than control of the quantity of reserves is that the demand for reserves is highly variable, influenced amongst other things by the credit worthiness of individual banks and the rate at which they can borrow in money markets; trading activity and price fluctuations in securities, derivatives and foreign exchange markets which can result in large unexpected payments flows; political and economic uncertainties which may affect customer payments, doubts about the ability of other banks to return money market borrowing because of either  credit or operational problems. So a policy of maintaining a fixed target for central bank supply of reserves results in unacceptably large fluctuations in overnight interest rates.

As result – because of this shift to bank payments settled in central bank reserves over the past century and a half -- central banks now conduct monetary operations by controlling short term money market rates of interest rather than of any measure of the stock of money and, in the past three decades, have largely lost interest in targeting any measure of the stock of money.  One reason for considering using cryptocurrency technologies to eliminate the need for settlement in central bank reserves is that this might allow a return to monetary operations based on the quantity of money rather than the price paid for borrowing and lending of money in short term money markets.

Two further points that can be made using Figures 1 and 2. The first is that ‘quantitative easing’ i.e. large scale expansion of central bank reserves matched by acquisition of government bonds does

[10] Historically reserve requirements have been an important source of government finance. In advanced countries reserve requirements are now very low and have been abolished altogether by some central banks.

[11] An also on longer ‘term’ rates of interest not illustrated in tbohe diagram. p

*not* , as many suppose, inevitably result in a large increases in private sector expenditure, bank lending and ultimately inflation. The reliance on bank balance sheets for transmission of monetary policy operations means that, without reducing money market rates of interest (and the scope for so doing is perceived as being limited by a zero- or near-zero lower bound on the interest rate offered on central bank reserves).

The immediate impact of quantitative easing can be illustrated in these figures: a shift of the vertical dashed line, the supply of central bank reserves, to the extreme right of Figure 2 and a resulting decline in money market rates of interest. As indicated by Figure 2, short term money market interest rates fall until they are very close to the interest rate offered by the central bank as remuneration on excess reserves. The increase of reserves liabilities of the central bank is matched by a corresponding increase in government bonds held by the central bank (not shown in Figure 1 because of the consolidation of the general government and central bank balance sheets) and a rise in bank deposits and corresponding reduction in government bonds held by the non-bank private sector.

Quantitative easing has further impacts on the prices of financial assets, rates of return on a wide range of financial assets, as the private sector adjusts its portfolio of assets to accommodate the central banks actions. The returns on both government issued and private assets can be expected to fall and their prices to rise.

The impact on bank lending, private expenditure and inflation is though far less certain. The portfolio shift into short term assets will make both bank and non-bank private sector balance sheets more liquid and, where they already hold long term assets, increase net worth. But this of itself can only effect spending if banks or private sector are 'liquidity ' or 'collateral' constrained facing difficulties in financing current expenditure out of future cash flows. It is also possible that quantitative easing can result in exchange rate depreciation and as a result raise both output for export and expectations of inflation which in turn increase the demand for borrowing from banks to take advantage of the consequent decline of real interest rates. Finally a commitment to quantitative easing may directly affect expectations of future inflation and hence lower anticipated real interest rates, increase aggregate demand and lead to rising pricdes. But these effects are quite modest, especially in large economic areas such as the Eurozone or the US. These limited transmission channels explain the comparatively modest responses of bank lending and private expenditure to the large scale expansions of central bank balance sheets conducted under the various central bank programs of quantitative easing.

A further point to be taken from Figures 1 and 2 is that current proposals for 'helicopter money' expansions, put forward by e.g. (Turner 2015) are, under current settlement arrangements, simply another version of quantitative easing with the same limited economic impact. A transfer of funds to individual citizens is a fiscal transfer. Even if the money is handed out as physical notes the money would be deposited in banks, the total of notes in circulation adjusts to meet demand (in practice it would of course consist of credits to individual bank accounts), and the outcome would be identical to that achieved through quantitative easing: an increase in central bank reserves and in bank deposits. There may be an accounting difference – the two policies are only exactly equivalent if the government issues debt in order to finance the helicopter transfers, which are then acquired by the central bank with their increased reserves. The accounting could matter. It is possible that, were rules on central bank accounting amended allowing the central bank to simply create money de novo for transfer to citizens (requiring a matching reduction in its own recorded equity since there is no matching asset acquisition) then the transfer using helicopter money could have a larger impact on the exchange rate and inflation expectations. The new 'money' might be more clearly seen to be a permanent and irreversible monetary expansion. But this would be controversial. A weakening of the central bank's equity based would undermine central bank independence and does not guarantee that general government will not seek to subsequently reverse the policy through a subsequent fiscal tightening.

Noteworthy also is the absence, under modern bank based monetary arrangements, resting on settlement of bank payments using central bank resources, of any equivalent of the 'real balance' effects that were a central part of classical quantity theory of money. According to those theories increases in the quantity of money in excess of what was demanded for transaction purposes, would result in increased spending and this would continue until prices had risen sufficiently for the transactions demand for money to increase until it once again matched the supply of money. An obvious but surprisingly little discussed criticism of current monetary arrangements is that in the circumstances that of relatively large overhang of public and private debt in many industrial economies, the obtain today the only monetary tools available are the lowering of interest rates to encourage an even greater level of private sector debt *or* increased government spending / lowering of taxes that increases the level of government debt (possibly accompanied by central bank acquisition this debt through quantitative easing).

Removing the requirement for settlement of interbank payments using central bank money, can potentially reinstate a transmission mechanism of monetary policy operating through real balances, hence allowing the possibility of a monetary expansion that does not rely on increase public or private sector debt.

## 3. The distributed ledger proposal: payments without settlement

The previous section has outlined and critiqued our current monetary arrangements with settlement of bank payments in central bank reserves. This section outlines an alternative decentralised arrangement using the technology of cryptocurrencies (the 'blockchain' or mutual distributed ledger) in order to make all bank payments immediately final without need for subsequent settlement.[12]

This requires placing both government-issued fiat money and bank money all on a state-sponsored ledger. Also, since banks must also transfer matching assets, bank loans are also placed on the same ledger.

This new arrangement goes well beyond the discussions of possible central bank issue of cryptocurrency made, at least to date, by a number of central banks worldwide.[13] It is not just the issue of a virtual central bank liability, the internet equivalent of a central bank issued banknote, or the use of distributed ledger to support a virtual currency that is completely backed by central bank money.[14] It is a complete redesign of the arrangements for holding and paying fiat and /bank money.

This has several implications:

- A closer match between customers perceptions ('my money' is kept securely and conveniently by a bank) and actual banking operations (the bank has no permission to use this money for purposes of its own)
- Complete protection of bank money and payments from any interruption resulting form bank failure. Since all money is on the ledger, not on bank balance sheets, customer access to bank money and payments services can continue uninterrupted even while a failing bank is being resolved.
- No need for either the central bank lending of last resort or for bank bail-out to protect the payment system (though as discussed below a more limited role for lender of last resort is likely still to be needed in short term money markets, since banks could still face liquidity problems from maturity mismatch, borrowing money short term to invest in longer term illiquid assets).
- Avoids the problem that current proposals for widening of access to central bank reserves could facilitate a destabilising run on banks

After outlining the proposal, the following section then discusses how it can be used to achieve a number of goals for monetary arrangements advocated within the Austrian school of economics.

[12] Appendix A presents a detailed but non-technical review of cryptocurrency technologies.

[13] Central banks have naturally been paying close attention to the technologies of virtual money, see for example (Ali et al. 2014b; Ali et al. 2014a). The central issue in these discussions has been whether there is demand for holding a central bank issued crypto-currency i.e. something like the suggested Fedcoin outlined by (Koning 2014; Andolfatto 2015). Demand is uncertain, users may prefer the guaranteed anonymity of notes and coin and there are already effective means for carrying out most online monetary transfers using bank money. For further discussion see (Fung & Halaburda 2016). Bank of Canada and Bank of England research on this topic – can be accessed through their webpages, various postings on http://www.bankofcanada.ca and http://www.bankofengland.co.uk/research/Pages/onebank/cbdc.aspx. Sveriges Riskbank have also announced they are investigating possible issue of digital currency (Skingsley 2016).

[14] Such as the Utility Settlement Coin or Tibado described above, or the Monetary Authority of Singapore project working with R3 and a consortium of banks to develop a fully centrally backed virtual currency on distributed ledger that can be used in securities settlement and cross-border payments (on this see Monetary Authority of Singpore 2017).

## The proposal: mutualisation of monetary transaction deposits.

A key intuition that can help with understanding this proposal is recognising that demand for liquidity from settling interbank payments is required only by individual banks, not by the monetary system as a whole.[15] Consider in Figure 1 the hypothetical situation where the monetary system consists of a single bank –which is also the note issuer – instead of several competing banks and a note-issuing central bank. There is then no need for settlement, no requirement for liquidity for settling payments between banks and indeed no need for a separate central bank.

It would never be desirable to have only a single bank – such an institution would have unacceptable market power. But it is possible, using the technologies of cryptocurrencies, for all money including monetary deposits to be held on a mutual distributed ledger instead of on bank balance sheets. In this case – because bank transaction deposits and bank notes are all transferable liabilities on the same ledger – there is no need for central bank reserves to settle payments between banks.

Figure 3: Fractional reserved banking without settlement using distributed ledger

General Government/ Central bank

| *Assets* | *Liabilities* |
|---|---|
| Real assets | Bonds |
| Repo to banks | |
| Cryptocurrency | |
| Notes 100% backed by cryptocurrency (off balance sheet) | |

Commercial banks

| *Assets* | *Liabilities* |
|---|---|
| Loans pledged to ledger | Liability to ledger |
| Other loans | Time deposits |
| Money market | Money market |
| Cryptocurrency | C bank repo |
| | Bonds/ Equity |
| Cryptocurrency wallets (off balance sheet) | |

Non-Bank private sector

| *Assets* | *Liabilities* |
|---|---|
| Real assets | Bank loans |
| Bonds/ Equity | |
| Time deposits | |
| Cryptocurrency and notes | |

State sponsored ledger

| *Assets* | *Liabilities* |
|---|---|
| Temporary Bank issue | All money (Crypto-currency) |
| Permanent fiat issue | |

Figure 3, above, illustrates this proposed arrangement. The key difference from current arrangements shown in Figure 1 is that all money is now placed on a state sponsored mutual distributed ledger, shown as the oval on the lower left of the figure. There are as yet no agreed accounting conventions for distributed ledgers. The presentation chosen here emphasises the following points (i) there is only one type of money, whether issued by the state (fiat) or by banks; (ii) state money issue is permanent and irrevocable; (iii) bank money issue is temporary, backed by a promise of repayment secured through bank loans pledged to the ledger

Notes, while still managed an issued by the central bank are now fully backed by cryptocurrency, the central bank is obliged to purchase or borrow cryptocurrency in order to issue notes. The notes and the cryptocurrency backing are now off-balance sheet.

[15] What about international transactions? Again, provided the exchange rate is freely floating, there can be no liquidity shortage for the banking system operating within a single currency area.

Commercial banks no longer hold reserves with the central bank reserves at all. Commercial banks must hold reserves of cryptocurrency, in order to repay maturing liabilities (time deposits, money market borrowing, central bank repo) but these are held directly with the mutual distributed ledger and are no longer part of the infrastructure of payments.

The non-bank private sector no longer holds or uses bank deposits as money, rather all money is now on the ledger. What commercial banks continue to do is provide 'wallet' services, i.e. security, accounting and other money management services for holders of cryptocurrency. From the perspective of the user, little changes, they continue to use their existing banking channels – branch, online, telephone, card payments – exactly as before. The difference though is a transformation of the back office, payment instructions

This proposed arrangement, while conceptually simple, would have been difficult or impossible to operate with older traditional payments technologies available before the emergence of cryptocurrencies such as Bitcoin. The key difference is that these new cryptocurrency technologies support secure but *fully decentralised* payment transactions and payments documentation: while the money is issued on the state sponsored ledger, there is no central institution responsible for maintaining payments records. Moreover it now becomes possible for banks to temporarily issue money onto the ledger, with further protections to ensure repayment, something which could not be practically effected before decentralised cryptocurrency transaction technologies were developed.

Appendix A provides a detailed but non-technical review of the operation of these decentralised payments technology used by cryptocurrencies  and which could support the state-sponsored ledger proposed here. There would have to be major differences from 'the blockchain' (the mutual distributed ledger used by Bitcoin): (i) participation would need to be permissioned, just as it identity must be proven today in order to open a abank account, real world identity would need to be established before an individual or body corporate could have a virtual identity on the ledger in order to hold cryptocurrency; (ii) as a permissioned network extremely low cost and rapid verification of the payments record would be possible, in near real-time subject to being online and able to communicate with some other network participants;

Figure 4, below, illustrated is a little more detail how this proposed arrangement would utilise cryptocurrency technologies. As discussed in Appendix A the essential economic information stored in a distributed transaction ledger is a cryptographically-secured time-ordered immutable transaction record. This is extremely simple – for each 'coin' (a temporary token representing value and used once only in a transaction)  it records its ownership, when it is created and the transfer of value -- who receives its value as another newly created coin – when it is spent. This is illustrated in Figure 4a.  Money first appears (coin creation), then it is used and effectively disappears (though the record remains permanently on the ledger).

This though is only one of two fundamental transaction types that underpin our current monetary systems. The other type of transaction, illustrated in Figure 4b, is a money-financed bank loans. First a debt is created, linking two 'network participants' (the bank and the customer); then subsequently the debt is repaid.

Figure 4: recording monetary and credit transactions

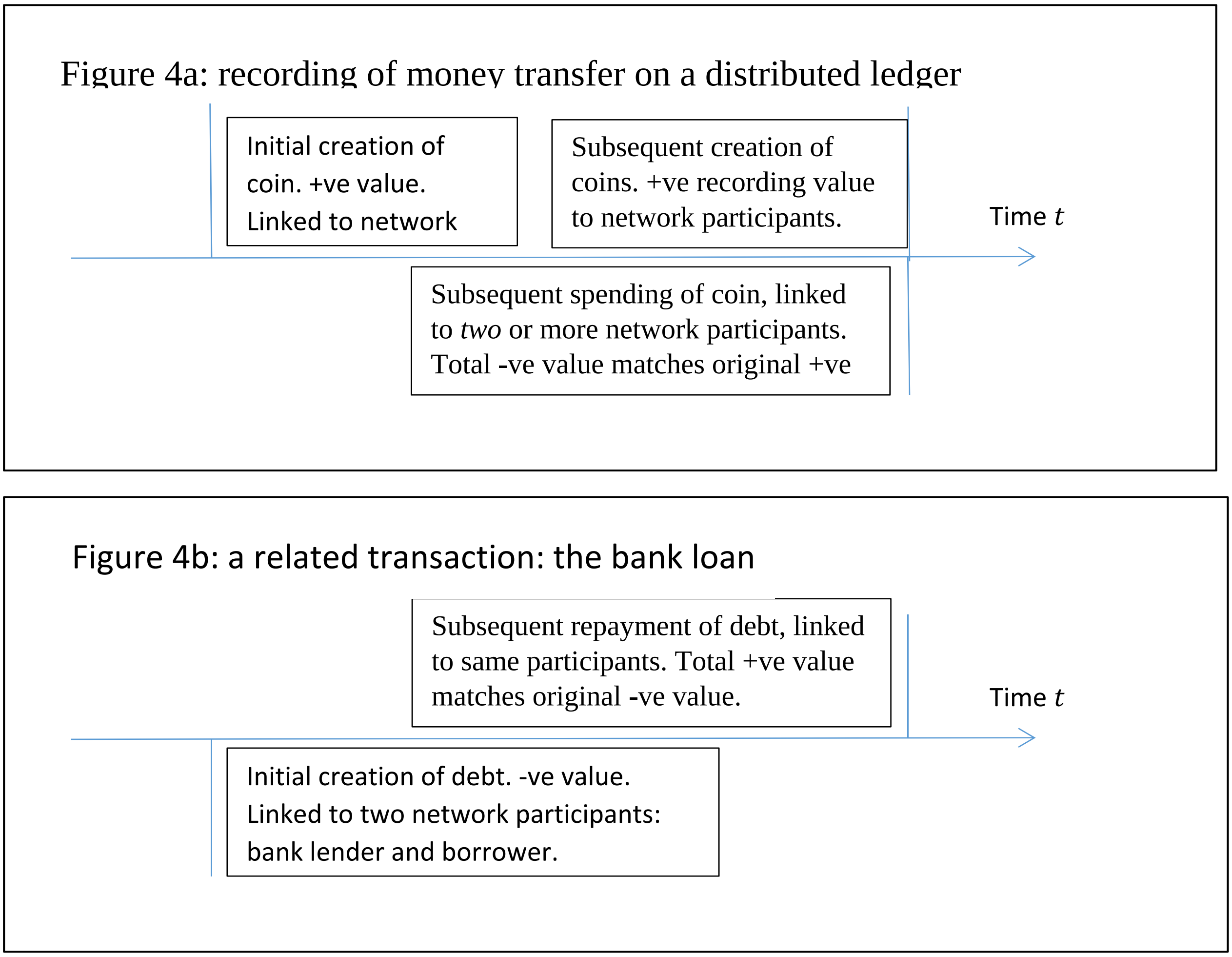

Figure 4a: recording of money transfer on a distributed ledger

Initial creation of coin. +ve value. Linked to network
Subsequent creation of coins. +ve recording value to network participants.
Time *t*
Subsequent spending of coin, linked to *two* or more network participants. Total -ve value matches original +ve

Figure 4b: a related transaction: the bank loan

Subsequent repayment of debt, linked to same participants. Total +ve value matches original -ve value.
Time *t*
Initial creation of debt. -ve value. Linked to two network participants: bank lender and borrower.

Not all debts need be money financed. A debt may be initiated entirely outside of the monetary system – any economic exchange may result in the acceptance of an obligation to make an agreed payment in the unit of account at some future date. But a key feature of our real world monetary systems is that banks – because they are fractionally-reserved – are able to create money that they do not already have by lending. A bank loan creates both money (a bank deposit) and a matching customer obligation to repay this money.[16]

Now a key point. can this be achieved when all money is crated and held on a single state-sponsored mutual distributed ledger shown in Figure 3? The upper panel, Figure 5a, shows the comparatively simple case: state creation of cryptocurrency. This is a permanent creation in the sense that once the coin's value is created it can never disappear from the ledger. The value of the coin can be used without limit in subsequent transactions as shown in Figure 4a.

[16] A separate issue highlighted by (Graeber 2014) – in an informative but rather tendentious history of debt and money – is that credit was used for monetary exchange long before state or bank money. What his discussion does not though sufficiently highlight is that transactions between strangers without a legal or social framework enforcing repayment, i.e. in a permissionless world where identity does not support trust, cannot be credit based. Thus commodity money (silver, gold) were also commonly used in exchange from the earliest times. Moreover the use of credit as a means of exchange requires mechanisms of trust which, nowadays, are usually based on a bank or other institution providing credit which is then used to access bank money.

The lower panel illustrates how banks can be given the right to temporarily create money, provided that this creation is matched by an accompanying loan transaction (as illustrated by Figure 4b) which ensures that the money initially created by the bank is only temporarily available for financing the loan until repayment.

Figure 5: state and bank money creation.

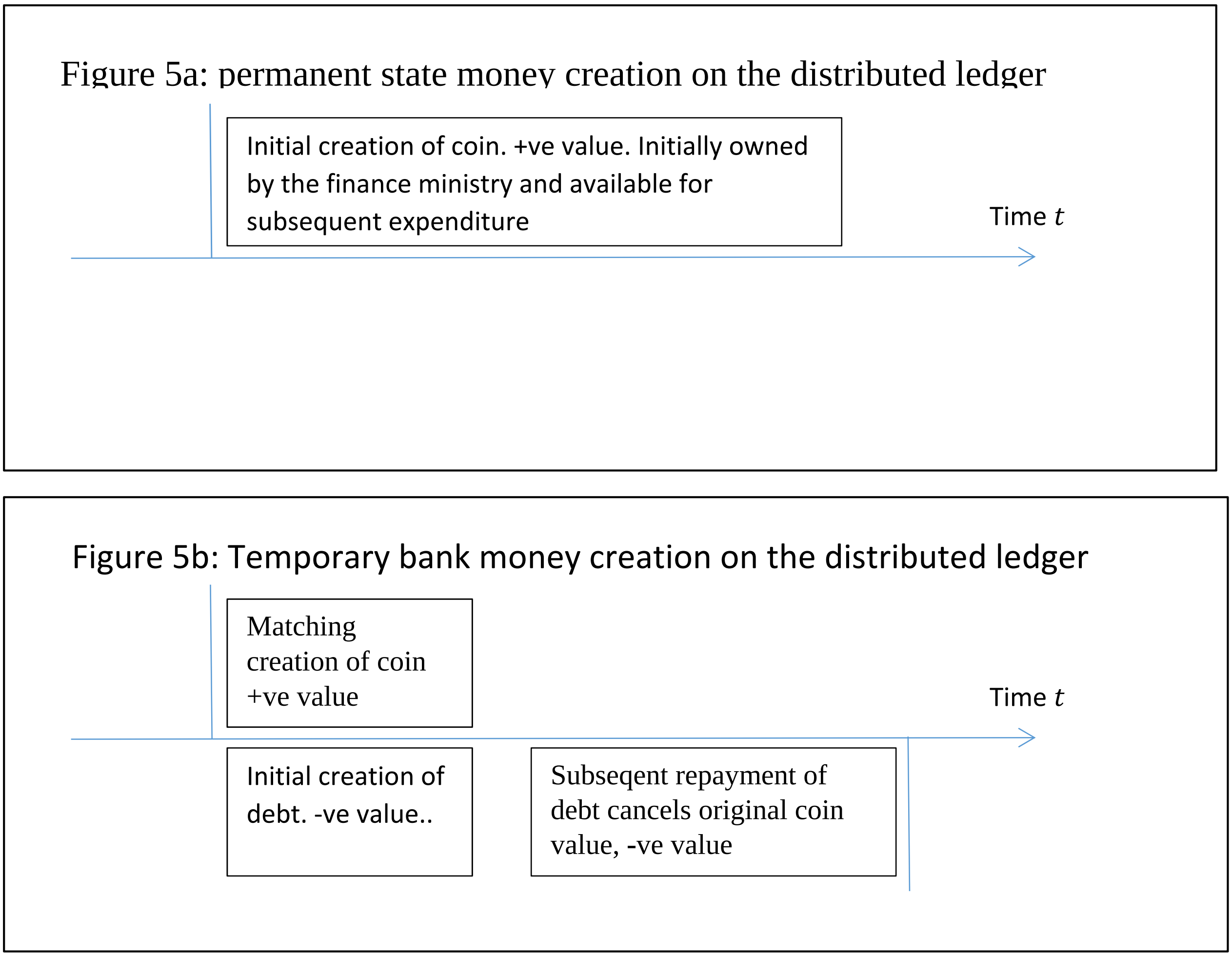
Figure 5a: permanent state money creation on the distributed ledger

Initial creation of coin. +ve value. Initially owned by the finance ministry and available for subsequent expenditure
Time *t*

Figure 5b: Temporary bank money creation on the distributed ledger

Matching creation of coin +ve value
Time *t*
Initial creation of debt. -ve value..
Subseqent repayment of debt cancels original coin value, -ve value

Note that allowing banks to create money to finance a bank loan as illustrated in these figures means that there is no longer any maturity mismatch.

Under our present arrangements with central bank settlement bank deposit money  has a different maturity from the perspective of the holder (the bank customer) and the issuer (the bank). For the holder bank money is a perpetual asset which can be transferred as required to other holders.  As money – while it can be transformed into different forms of money (notes and coin, transaction deposits at other banks, other currencies) – it is never redeemed, it is only spent. For the issuing bank a transaction deposit is redeemable on demand and therefore with a maturity that depends on the receipts and payments of their customers. Transaction deposits  may be withdrawn rapidly – I.e. maturity can collapse to near zero – in the extreme situation when bank customers are worried about possible bank failure that could trap their money inside of the bank while it is resolved and 'run' on the bank.

This is not to say that a 'run' on retail deposits is a usual cause of bank liquidity problems – the protection of deposit insurance usually prevents this happening. Bank liquidity problems are almost always the result of failure to refinance short-term wholesale market borrowing.[17] This was the case both in the global financial crisis 0f 2007-2008 (triggered in many cases then by loss of confidence in mortgage backed securities used as collateral for borrowing) and in earlier financial crises. A liquidity problem for banks could still arise, under the arrangements proposed in this paper, if they could not renew money market borrowing but this would not threaten any loss of access to bank monetary deposits or interruption of bank payment services.

With the comparison of these two transaction types illustrated in Figures 4 and 5, it is now possible to present the proposal of this paper in greater detail. Money creation of both types, permanent state fiat money and temporary creation of money by banks can all be recorded in a single time-ordered mutual distributed transaction ledger shared between all banks, bank customers and other holders of money.

## Some ledger technicalities

It is worthcommenting briefly on some technical aspects of the implementationof this proposal. This subsection assumes readers are familiar with the mechanics of cruyptocurrency operation as described in Appendix A and could be omitted by readers willing to take these technicalities on trust.

Note that this proposal requires a permissioned ledger. In an unpermissioned open-source cryptocurrency network which anyone can join, only the first transaction type transferring money is possible: recording a debt transaction requires recording the real world identity of the debtor, otherwise they can escape the debt simply by leaving the network. In a permissioned network, in which network participants can join only after providing their real world identities, both types of transaction can be recorded. Incentives for the individual to avoid default on their commitment to repay the ledger still rely, as now, on sanctions such as loss of credit standing or legal action to collect collateral.

The distributed ledger as proposed in this paper has no need for proof-of-work. This must be a permissioned ledger so an alternative and near immediate validation scheme can be employed based on validation by trusted nodes.[18] Coin though – while not created by proof of work – can be created by government fiat – a government agency. This could possibly be a division of the central bank (placing this responsibility with a division of the central bank is reminiscent of the British 1844 banking act which distinguished the note issuing and banking departments of the Bank of England, and limiting the unbacked note issue not matched by gold reserves to a fixed nominal sum); or it could be independent of the central bank. This detail – whether creation of fiat money is the responsibility of the central bank or a separate agency is left for further discussion, the appropriate arrangement will depend in part on the need for co-operation between the issue of fiat money on the distributed ledger and the role of the central bank as a participant in money and other credit markets using its own reserves of cryptocurrency.

In either case though, the decisions on issuing fiat money on the ledger to finance government spending should be outside of day-to-day political control. One possibility is an arrangement similar to that currently used for supporting central bank independence, an independent committee that

[17] Retail bank runs do happen occasionally, a renowned example being the withdrawal of retail deposits from the UK mortgage bank Northern Rock in September of 2007, but even this case was triggered by a loss of access to wholesale funding the retail run came later. See (Milne & Wood 2008) for a description of this failure.

[18] The trusted verification nodes can be banks but possibly also other participants. There are many possibilities for the consensus algorithm. This could be based on some form of supermajority, or for blocks containing smaller transaction values random selection based on stake. There will be no difficulty in providing near-immediate finality of all payments.

decides on fiat money issue in order to achieve clearly defined and measureable policy outcomes. Alternatively the issue of fiat cryptocurrency could be according to a mechanical '$k$- percent' rule of the kind advocated by Milton Friedman.

Whatever the rules governing creation of fiat money on the ledger and the accompanying financing of government spending, it should be noted that the central bank no longer has any responsibility for providing payment services, to commercial banks, government departments, or the private sector. All holders of money will either execute payments directly or more likely through the wallet services provided by banks and by non-bank competitors.

Debt contracts, as shown in Figure 4b, lead first to the creation of new money on the ledger, i.e. an increase of the money stock, then to the extinguishing of money on the ledger as the principal of the money-financed loan is repaid i.e. a subsequent offsetting reduction in the money stock. Note also that Figure 5b illustrates the example of a single repayment of principal at maturity – other loan contracts though can just as easily be recorded as a combination of such transactions, one corresponding to each repayment of principal.

## The triple lock: ensuring repayment of bank money on the ledger

A key feature of this proposal is a requirement to ensure, with a very high degree of probability, that the commitment to repay money onto the ledger illustrated in Figure 5b is honoured. The first obligation of repayment will be exactly as with existing bank loans, the loan contract agreed between the bank and the borrower will oblige repayments to be made onto the ledger. The cryptographic coding will automatically take the monetary payment at the agreed time, which can be timed to the nearest minute or second. The borrower will default if, at that moment, they have insufficient ledger money associated with their node from which the commitment to repay principal has been made (this leads to an issue not further pursued in this paper is whether individuals and companies – including both non-bank corporates and banks, can create more than one node on the network. This might be limited to only node for every legal entity or multiple noides might be allowed, but perhaps only where there is a valid legal reason, e.g. an individual of limited capacity who needs a guardian or representative to deal with some of their financial affairs. )

This is a first line of defence against the possibility of the failure to repay money borrowed off the distributed ledger. A second line of defence is the underwriting of the loan obligation by the bank, based on its credit assessment of the borrower. The bank as well as the customer has its own node on the network with associated holdings of cryptocurrency. If the borrower fails to repay principal as agreed, then the algorithm coded on the ledger can automatically take the principal repayment from the bank to pay down the borrowed money on the ledger. Banks would likely have multiple nodes on the ledger, each corresponding to one of the many legal entities within a typical banking organisation, but there should probably be an obligation that any call on payment to the ledger, which cannot be completed by a bank subsidiary because it has insufficient money on the ledger, will be fulfilled instead by a payment out of money held by the bank holding company. These bank payment obligation – along with those of the borrower – should all be coded into the distributed ledger and deductions automatically taken by the ledger algorithms , with conditional branching: if not paid by the borrower, then by the bank subsidiary, if not by the bank subsidiary then by the bank holding company.

If the bank also has insufficient money on the ledger for the required repayment i.e., if its holding company and subsidiary holdings of money on the distributed ledger has fallen to below the required repayment at that point in time, then a third line of defence comes into play. Two consequences follow. First the coding of the ledger calls on all other banks to make the repayment onto the ledger, most obviously with an obligation to make payment in proportion to the amount of money they currently have outstanding on the ledger. Once again this is all undertaken automatically, using the algorithms of the ledger ("smart contracts") without the need for any administrative intervention by either banks or regulators. At the same time the bank that has failed to support it credit underwriting commitment enters a resolution process. The details of this process are not considered here, but this cannot be undertaken automatically on the monetary ledger without administrative and regulatory intervention, because it involves all the other bank assets and liabilities that remain on-bank's balance sheet. Still one would expect that the this resolution process would involve a suspension of various claims, of both debt and equity holders, and a new temporary management with responsibility for determining how to restore the bank to a situation when it can once again command sufficient resources to maintain a sufficient balance of money on the ledger to continue its business and meet any other regulatory requirements.

A further appropriate protection for ensuring confidence that money-financed bank loans are repaid onto the ledger may be to give the claims on the ledger priority over all other creditors in bank liquidation, perhaps including even the tax authorities.

## Prospects for adoption

The operation rules proposed for the ledger are straightforward, but is adoption realistic? This subsection will argue that it is, though ultimately a decision to adopt will depend on much more detailed examination than provide here and  on this proposal obtaining sufficient widespread support, from politicians, households, non-bank companies and banks themselves.

From the perspective of bank customer  this ledger will be operate in the background, with little impact on their day-to-day transactions. With such a scheme bank monetary deposits would then become 'wallet services', much the same as the wallet services currently provided for holding cryptocurrencies. They would help customers manage and use their cryptographic keys and execute payments. Assuming that the immutable ledger records transactions not balances, then wallet providers i.e. banks would also maintain records of account balances for customers. As illustrated in Figure 1b, it is only the original loan and repayment of principal that would be recorded on the distributed ledger. Associated interest payments would also be agreed in the loan contract, but these obligations do not involve repayment and extinguishing of money on the letter and so would be settled by monetary ledger transfers of the kind shown in Figure 1a rather than Figure 1b.

Tax and other obligations for payment to government would have to be settled in ledger money. While legal tender is no longer a major feature of monetary arrangements, the legal tender status which central bank notes have in many jurisdictions (i.e. the legal obligation to accept bank notes in settlement of debts) could be extended to money on the ledger. This would provide further incentives for bank customers to accept the transition of money onto the ledger.

One possible objection to the ledger is that placing all fiat and bank money on a mutual distributed ledger would require the abolition of cash transfers and their associated anonymity. A reduction in anonymous cash transactions might be regarded as good (because it limits tax evasion and criminal activities). It can be regarded as bad because citizens have a right to privacy in their financial transactions and avoiding the prying eyes of the state. Regardless of the position taken on this issue, this is not in any way an objection to putting money on the ledger. The use of cash is a quite separate issue unaffected by the transfer of fiat and bank money onto the ledger. Banks notes would continue to be central bank liabilities and would still be issued as now, on demand, in exchange for money held in transaction deposits, most often through an ATM withdrawal. The only change is that all notes and coin would now be fully backed by money on the ledger. Commercial banks could handle bank notes only as an agent, not directly, when an ATM or counter withdrawal of notes is made, they would be responsible for ensuring that an equivalent customer payment is made to the central bank. Alternatively, at greater expense to commercial banks, all note holdings could be 'o balance sheet' in which case a customer cash withdrawal would be matched by a customer payment of an equivalent amount of distributed ledger money to the bank. When returned to the central bank notes could be held for inventory purposes or exchanged with the ledger authority (possibly another division of the central bank) in exchange for an increase in central bank holdings of money on the ledger.

Banks would continue to provide the full existing range of banking services to customers. Payment instructions would not be altered (only the subsequent processing of those instructions). Loans could be either money financed (Figure 1b) or they could be financed directly using the bank's own money (in which case they would be coded in the ledger according to Figure 1a, with obligation only on the borrower to pay, and the further 'lines of defence; not required; or some mixture of the two mechanisms. Where banks provide lines of credit, rather than loans with fixed repayment schedules, then they will need to maintain sufficient balances of ledger money to allow customers to draw down on their credit lines. As described here, it would be relatively difficult to record lines of credit on the ledger (though a further extension of the ledger coding could be considered to handle lines of credit, allowing customers to use ledger instructions rather than bank systems to draw down on their credit lines.)

The major perceived difference for bank customers, between existing monetary arrangements and those proposed here, will be the changed status of non-monetary bank deposits without transaction facilities. A fixed term deposit with a bank must be presented and understood as a loan to the bank, money which the bank is not keeping but itself lending on to customers. To guide customer expectations, in particular to support withdrawal of the bank safety net, it would be necessary to end government backed deposit insurance for bank time deposits. These could still be backed by private deposit insurance. It would though be essential to make clear that state support of these deposits, in the event of failure of the deposit insurance fund being exhausted, would not be forthcoming. The integrity of transaction monetary deposits achieved by transferring them onto the mutual ledger means that the bank could be allowed to fail without consequences for bank money and payment system.

A likely consequence might be much greater retail investor interest in 'peer to peer' lending, also known as market place lending, where investors can directly invest in a diversified portfolio of unsecured personal and small business loans, with repayment relying on repayment by these borrowers and (unlike the loans financed out of the ledger) not supported by the balance sheet of the bank. Withdrawal of deposit insurance on term deposits would effectively put bank time deposits and peer-to-peer loans on a level playing field. Customers would likely prefer peer-to-peer investment because it allows them to match their exposures to their willingness to accept portfolio risk and not accept a leve of default risk determined by thebank and not directly controlled by them as investors.

Banks though will be able to provide some investments that cannot be so easily provided on a peer-to-peer basis. These are savings deposit with an option for early withdrawal. These are similar, from the bank's perspective, to a line of credit. The bank must hold sufficient money on the ledger in order to be confident of meeting is commitments for early withdrawal. They would have some comparative advantage in providing these deposits because of their access to money market borrowing. Some requirement on notice e.g. one or two days, might be still be imposed in order to give the bank time to borrow money as necessary in money markets for customer withdrawal from instant access non-monetary deposits.

While the new arrangements would operate in a very similar fashion for both banks and their customers, they would require a substantial re-engineering of bank payment operations. A possibly extended period of transition would be necessary, before its full operation, during which banks would have a choice of maintaining bank monetary deposits on balance sheet or on ledger to test the proper functioning of payment instructions put through the ledger. Once it became compulsory for all transaction deposits to be on the ledger

Might banks resist such a proposal? This is unlikely, though their attitudes must depend on the entire package of reform not just the creation of the ledger. Liquidity management would become simpler under the new arrangement. A possibility would be to code also into the ledger arrangements for managing the collateral security (government bonds, corporate bonds, structured credit securities or even equity in short term bank repo) that can support such bank extensions of credit, with the collateral passing into the ownership of banks in the event of borrower default.

Banks would obtain a new source of revenue as they take over the role of central banks providing elastic increase in monetary deposits needed, for example, when there are large demands for means of payment arising for either seasonal reasons or because of large financial market transactions. The ledger would also offer banks new tools for monitoring borrower repayment. By placing all loans on the ledger, whether money financed or not, they then have a standardised and automated system for dealing with bank payments.

The main reason for banks objecting to transfer of monetary transaction deposits onto a mutual distributed ledger is the substantial costs of re-engineering their payments operations, replacing the current systems of netting and settlement with direct execution of customer payment transactions on ledger. To sugar this pill, it would be advisable to accompany the introduction of the ledger with the substantial reduction of burdensome regulation that would no longer needed once banks can be allowed to fail without disruption of bank money and payments.

Could banks resist such a proposal? This is unlikely. Even if banks are lukewarm, it is doubtful that that they would be able to continue providing an alternative payments service outside of the ledger.

Central bank reserves would be transferred as bank assets onto the ledger and no longer be available for settling of transactions in existing payment schemes (ACH services, debit card, ATM withdrawals, direct debits, credit transfers). These schemes would migrate to use the ledger and therefore no longer require central bank reserves for settlement. All payments would become gross and real time, but because payments are on the ledger not on bank balance sheet, there would also no longer be any need for the central bank provision of intraday liquidity to banks, in order for them to be able to put large value payments through their balance sheets without danger of lack of balance sheet capacity leading to log-jam .

To avoid using the ledger, banks would have to rely on setting up competing payment schemes with separate arrangements for settlement, i.e. setting up a banker's bank or clearing house replacing the existing central bank role of supplying reserves for settlement of payments. Such off-ledger payment arrangement are conceivable and need not necessarily be outlawed, but implementing them would require extensive investment in underlying operational systems – at exactly the same time as substantial investment is also being made in on-ledger operations – as well and agreement on the alternative asset for settlement and arrangement between banks for provision of liquidity.

Some rules would likely need to be developed on what loans are eligible for money finance, to ensure prospective repayment is not seriously in doubt. It is probably advisable to allow banks to place seasoned loans on the ledger as well as new loans (in practice refinancing will make these difficult to distinguish). There could be limits on maturity or, if it was desired to include longer term loans such as mortgages, a requirement for amortisation. Interest could be payable back to the ledger corresponding to current market rates of interest on the best quality credits, most obviously government bills and bonds – though this would have a major impact on bank earnings. Notes and coin would certainly be issued against the ledger.

In particular it would be feasible and might be desirable to allow banks to substitute loans on the mutual ledger so that loan default and its management can be moved back entirely onto their own balance sheet. This would be recorded in the mutual ledger as two linked transactions, an existing loan being placed on the ledger at exactly the time when the troubled loan faces a potential default of principal repayment, thus fulfilling the bank's obligation to extinguish an entry on the ledger. Borrower consent would though be required for such transactions.

## Bank transactions in time deposit, money and security markets

The mutual ledger will not record everything on bank balance sheets, far from it. Banks would still need to hold reserves of the cryptographic currency and continue to operate a treasury function, in order to manage the inflow and outflow of these reserved, not because of customer payments but because of attracting retail and corporate time deposits and their transactions in money and security markets. Note that all of these bank transactions would appear in the ledger as a transaction of type 1a because they involve no new creation of money, only bank money creation is recorded s type 1b.

Banks would continue to have both debt and equity liabilities on their balance sheet, reflecting short and long term borrowing and shareholder funds (but not monetary deposits). Banks would continue to hold on their own balance sheet both loans that are not funded by money creation, securities and other assets, and credit exposure of loans on the ledger would be an off-balance sheet exposure.

A central bank would still be present, holding its own reserve of the cryptocurrency, which it could lend to commercial banks against collateral as appropriate on occasion to help allay difficulties banks might face in refinancing themselves in short term money markets. This though now would be a discount window operation – lending at above market rates, no longer seeking to control short term money market interest rates. Note that these mechanisms are all ultimately concerned with bridging shortage of credit availability, inability to replace credit is still a liquidity risk, but it is a risk that does not interrupt the payments system, at worst is will limit the supply of bank lending (but provided banks have retained some balance sheet capacity, profitable bank lending can still continue to be financed through money creation on the ledger).

The discussion here leaves open a substantial question: central banks will no longer act as lender of last resort, but will there not still be a need for some central bank intervention in money and bond markets? The logic of the proposal of this paper is no, central bank intervention would be limited to individual institutions, not the market as a whole. A laissez-faire approach avoiding such intervention entirely could lead to some very sharp fluctuation in interest rates, especially at short maturities. But this would be offset by the resulting incentives for banks to create money on the ledger, for example funding collateralised lending using short term government bonds as a collateral.

## Resolution of failing banks, 'shadow banking' and their regulation.

As already discussed, the ledger can make use of 'smart contracts' for loan repayment i.e. repayment by the borrower would be automatically coded into the contract of type 1b; with payment instead coming from the bank if the borrower failed to repay. Then – in the extreme situation where a borrower failed to repay *and* the bank who has loaned the money also having insufficient money on the ledger to make this repayment, then external process of sanction would need to be triggered. This should be a firm response, most likely first giving the bank a short period of grace to rectify the situation, then a move to resolution of the bank with the possibility of shareholders losing their claim on bank assets. In such resolution it will be ideal that the ledger has first call on bank assets, ahead even of the taxpayer, so minimising the possibility of state financed bail out of bank loan losses.

Note further that the history of bank loans on the ledger and their repayments, together with the quantity of ledger held by the bank available for avoiding resolution will all be in the public domain and monitored by bank investors, providing a strong incentive for banks to keep clear of any possible triggering of such a process. This visibility –together with the pressure from other banks who will wish to minimise their own exposure to failure of other banks – should create strong incentives on banks is to place relatively good quality loans on the ledger. Putting relatively poor quality loans on the ledger could undermine their access to unsecured money market and bond finance and hence their ability to manage the rest of their balance sheet.

While resolution should be rare it is still necessary to make it credible. Bank regulation would still be needed to ensure that 'wallet services' – the provision to customers by banks (or indeed by other providers) of payment and account services on the ledger must be easily transferred to third-parties in the event of bank resolution.

With transaction deposits transferred onto the mutual distributed ledger, hence avoiding any necessity for bailing out of bans to protect monetary deposits and the payment system, it would also be possible to radically reduce the both prudential regulation and capital requirements (regulation of conduct of business and for customer protection would though be unaffected, banks would still for example be responsible for ensuring that any loans they extend to retail borrowers are appropriate and affordable).

If free-riding and unsustainable credit expansions can also be avoided – issues addressed in the next two sub-sections – then state backed support for troubled banks would never be required, in turn indicating that there would be no need for prudential capital requirements on banks that choose not to issue money on the mutual distributed ledger.

The problem of setting the appropriate regulatory barrier between banks and shadow banks then disappears. The on-balance sheet business of commercial banks and shadow banks is the same – attracting debt finance in order to invest in relatively illiquid loans, typically employing some degree of maturity mismatch to gain additional interest income. The only difference is that commercial banks, unlike shadow banks, have the right to put money-financed bank loans on the ledger, but this activity is quite separate from their on-balance sheet deposit taking and lending (and as discussed below subject to industry self-regulation). Credit institutions without this right, i.e. pure shadow banks, and commercial bank in their on balance sheet credit provision compete directly on a level playing field.

There is still one issue whicih is not fully dealt with in the proposal as set out here : the continued provision during times of financial stress of short term credit especially for financing working capital, since it is a shortfall of finance for working capital that can have the most marked immediate impact on business activity during a systemic financial crisis. This can be part of the remaining macro-prudential and competition responsibilities of state regulatory authorities (they are no longer responsible for micro-prudential regulation and supervision).

The need to promote competition and ensure the sustainability of short-term business lending suggeststhat short term bank credit should be favoured for financing using money issued on the distributed ledger. Small businesses and larger companies should be an important stake holder in the micro-prudential self regulation of the industry, and this will ideally lead to banks to separate their businesses so that the off-balance sheet underwriting of ledger financed lending is supported by separate balance sheet that can continue in operation even in the devent that the bank as a whole is short of capital and facing a potential resolution (from on balance sheet lending, not losses of loans on the distributed ledger). This in turn would help in providing a 'level playing field' in terms of regulatory capital for remaining commercial bank on-balance sheet lending and shadow banking.

There is no longer any need for state-backed deposit insurance of commercial bank on-balance deposits, in effect the entire commercial bank balance sheet becomes a source of loss absorbing capital, this function is no longer restricted to equity and hybrid liabilities., This in turn can justify a substantial reduction in minimum capital requirements and – for banks that do not issue money on the ledger – possibly their complete removal. Banks though will not become grossly undercapitalised, they will need to retain the confidence of investors. At the same time privately funded deposit insurance and direct securing of deposits on underlying loans (i.e. P2P or market place lending) will become widely used as a way to protect uninformed retail depositors.

All this suggests that a relatively lenient approach should be taken to the establishment of banks, although the licensing regime would be very different for intermediaries ('shadow banks') that did not wish to be able to create money on the distributed ledger. For off-balance sheet banks there need be relatively little concern about capital and prudential safety (provided that the concerns of unsustainable credit expansion are avoided, as discussed in the next subsection).

For banks seeking the right to create money on the register, it would be important to ensure that they have sufficient balance sheet capacity to do without material risk of failing to repay underwritten ledger financed lending. As discussed in the following sub-section this becomes industry self-regulatory responsibility. One possible restriction, applied to relatively small unestablished institutions that are using the ledger for the first time to finance lending, will be to limit the amount of new money that they can create on ledger. This does not mean they cannot compete for the provision of wallet services or in on-balance sheet lending, but this will prevent reckless monetary creation before the industry supported self-regulators has an opportunity to properly understand the strength of their business.

Even so, there will be a concern that since shadow banking has been a source of vulnerability in many past crises it could, even with money moved onto a mutual distributed ledger, be so again. To properly analyse this threat, it needs to be recognised that 'shadow-bans' have operated historically in two quite different ways. Sometimes – for example the 1973 secondary banking crisis in the UK -- shadow banks have financed themselves by taking loans from commercial banks, who in return have been able to finance their funding of shadow banks through money creation. This will be a self-regulatory issue for the industry and can be addressed directly using the monetary distributed ledger, restricting the use of the ledger to financing customer loans, not loans to other credit intermediaries.

The second form of shadow banking, which played a particularly important role in the global financial crisis of 2007-2008, has been when shadow banks finance themselves using short term unsecured or  collateralised market borrowing, so exposing themselves to liquidity risk especially in the event of loss of marketability of their collateral. This more difficult issue can still be addressed when money is mutualised on a distributed ledger, as a macro- not –micro-prudential concern. . There is really no particular concern about rapid growth of collateralised borrowing by an individual institution, With no threat to the system of money and payments, individual commercial and shadow banks taking on excessive maturity mismatch  and as a result unable to refinance themselves in money markets should be resolved in the same way as commercial banks that cannot maintain their obligations to the ledger.

Where this second form of shadow banking poses a serious concern is when it is part of a general and unsustainable credit expansion, with the risk that the ending of the expansion will trigger widespread loss of confidence in both bank balance sheets and a collapse in the collateral pledged for borrowing by the banks and shadow banks and by their customers.  This is best addressed by further measures to prevent unsustainable credit expansion, the topic taken up in the following subsections.

## Prudential regulation becomes an industry not state responsibility

There is an obvious free-riding problem.  Banks that issue money on the ledger could potentially engage in substantial issue of money on the ledger, far more than can be realistically repaid in real value from the loans pledged to the labour to ensure repayment. The costs of lending then fall on other, on the rest of the industry (because the bank fails) or on the public at large (because of unanticipated inflation).

Allowing banks to mutualise their monetary funding removes an important current market discipline on bank monetary creation. Under competitive fractionally reserved banking, banks must allow for the fact that when they create monetary deposits through lending, they will then subsequently lose some of these deposits to other banks and so – if they expand faster than other banks – must be prepared to shift the balance of their funding from monetary deposits to relatively expensive (at least at the margin) term deposits and money and security market borrowing. Under the proposed mutualisation of monetary deposits of this paper, this discipline vanishes. If the costs of overexpansion then fall on other institutions the result can be excessive expansion of money and money financed-credit.

This free riding problem is the key issue on which the practicality of this proposal stands or falls. Some form of prudential regulation will be necessary for banks that issue money on the ledger, in order to 'internalise' this economic externality and prevent free-riding.

There are two mechanisms for internalising these costs.  There are: (i) the triple lock; -- underwriting by first the borrower, second the bank, third the entire industry; and (ii) x% reserving described in the sub-section below. The effectiveness of the triple-lock will depend on effective prudential regulation that prevents rogue banks exploiting the protection offered by the rest of the industry.

Ensuring the effectiveness of this 'triple-lock' in turn suggest that industry should takeover all responsibility from government for micro-prudential regulation. This is because industry stands ahead of the tax payer in exposure to credit risk on the ledger. Therefore it is the industry not government should agree rules for loans put on the ledger and for the capital adequacy rules to be applied to banks that use the ledger for funding their loan.

What might industry choose to do? This is their responsibility, but they might for example require some form of external rating by a credit rating agency  (which would in turn require the loans to be packaged as a pass-through securitisations) *and* also capital rules for the banks that securitise, since these are securisations with explicit support, not balance sheet remote).

The key point here is though that because the industry is setting these capital rules for themselves, the externality being internalised at industry level, it can be the industry that sets there ruled. No longer will they be able to argue that microprduential regulation is an unacceptably burdensome constraint on their own business (which is what industry thinks of the current Basel III and Dodd-Frank regulations).[19]

This in turn allows the state steps to step back entirely from responsibility for micro-prudential regulation. There are in effect two types of bank: Type (a) who issue money on the distributed ledger; and type (b) those who do not (including 'shadow banks'). Prudential regulation is no longer necessary for banks of type (b): they should be subjected only to rules on customer protection. In the case of banks of money issuing banks of type (a):  all responsibility for micro- prudential regulation can be passed in its entirely from the state to the industry.  Prudential regulators – e.g. the FDIC and the regulatory divisions of the Federal Reserve in the US, the PRA in the UK – can be abolished, or rather they move from being a government department to beome and industry governed self-regulatory organisations.

Government though would still need to be in the background to ensure that self-regulation does not operate to restrict competition. The FDIC and the PRA are privatised, but come under the oversight of the Department of Justice and the Competition and Markets Authority respectively.

The state would also retain a macroprudential responsibility, ensuring tjhat the overall growth of money and credit does not threaten financial stability. The $x$-per cent reserving described below is the most obvious tool for them to carry out this task.

What about international financial regulation? The Basel committee, the BCBS , can also largely be abolished, but would retain some competition role -- making sure that banks from one country do not use their access to the ledger to gain an unfair competitive advantage in other jurisdictions -- and perhaps on safety and soundness in foreign exchange markets (merging with the sister committee CPSS would be appropriate).

## Unsustainable credit expansions

A range of protections – the 'triple lock' of borrower, bank and banking industry obligations to repay money created on the ledger to finance bank loans supported by the prudential self-regulation by the industry – ensure that ledger money does not finance credit that cannot be repaid.  This though does not rule out the possibility of unsustainable credit expansion taking place without monetary finance but supported instead through short term unsecured and collateralised money market borrowing. Such unsustainable credit could be conducted by both commercial banks in their on-balance sheet lending and by shadow banks. As pointed out in the previous sub-section there is really no distinction between the two types of institution in these activities.

The macroeconomic issue this raises are intriguing and only the most cursory of discussion can be provided here. Arguments based the logic of the Modigliani-Miller theorem would suggest no, this is

[19] For example the research and lobbying material of the institute for internatonal finance https://www.iif.com

not a concern, provided any state bail-out of banks is avoided. There will be a subsidy for credit expansion only to the extent that banks anticipate a significant possibility that they will enter resolution with such heavy loan losses that the ledger – even as the first claimant on bank assets – cannot be repaid.

This argument though ignores behavioural and psychological factors, in particular the possibility of a credit and asset price boom, where banks perceive only high returns from all manner of lending and turn to the ledger for funding regardless of how this is perceived by the market. Such an expansion can only end with losses, either from high inflation (because the monetary authorities do not offset the monetary expansion) or credit losses and a severe economic downturn (because the monetary expansion is sterilized by a contraction of fiat money on the ledger).

Such credit and asset price booms are further exacerbated by the externality that arises when an individual bank engages in collateralised lending.[20] The problem is that the bank does not take account of the additional risk exposure imposed on other banks, in the event that there is a loss of confidence and a call to sell collateral (a 'firesale'). Any increase in either unsecured short term funding of collateralised lending – or short term collateralised funding for lending collateralised or uncollateralised -- increases the amount of selling that a bank must do in the event of a financial crisis; and the more selling it must do the greater the fall of collateral values and resulting liquidity problems and credit losses for other lenders.

This is a system wide concerns and this suggests that the appropriate response is preventing excessive asset based lending. Moving money and money financed banks loans onto a distributed ledger provides further additional tools for addressing such unsustainable credit expansions. First and most obviously would be making mortgage lending – either commercial or residential – ineligible for financing through creation of money on the distributed ledger. This is natural anyway because the principal economic reason for allowing banks to create money on the ledger is short term elasticity in the supply of money to deal with the demands for money emerging from seasonal fluctuations in economic activity and substantial financial market transactions. Mortage lending should be easily financed out of long term investment funds e.g. pension and insurance funds.

A further reason for excluding mortgage lending from the distributed ledger is to offset the apparent bias towards housing finance that has emerged across the Western world over the past half century (highlighted for example by (Jordà et al. 2016)). A re-orientation of money financed bank lending towards short term business finances for working capital is arguably desirable for correcting these structural economic imbalances.

### Applying $x$-per cent reserving to limit fractionally-reserved monetary deposits

One way of addressing this concern that money-financed bank lending will lead to unsustainable expansion of both money and credit – by both commercial and shadow banks -- is to limit the extent to which bank-money on the ledger is fractionally reserved.

An offsetting discipline can be imposed by requiring banks, in any transaction of type 1b in Figure 1, to commit $x$-percent of their own money to the funding of the loan. The actual requirement would lie somewhere between the two extremes of -0-percent reserving (banks need keep not reserves against money created against a loan) to 100-per cent reserving (banks can no longer create money at all, all loans must be financed by borrowed money).

[20] A point developed by (Stein 2012)

In effect this is a form of 'overcollateralisation'. Such overcollateralisation also makes it even less likely there will ever be a call on the ledger to finance bank loan losses on any large scale. Making $x$ too large however could limit the supply of credit. Arguably there are some positive externalities from encouraging bank supply of credit, especially for short term business lending and in areas such as trade and working-capital finance. Both research and practical experiencewill have to be taken into account in choosing the appropriate level for $x$.

Limiting fractional-reserved banking in this way will not just reduce monetary financed bank lending, it will also restrict the availability of money for the required refinancing of short term funding, whether on-balance sheet by commercial banks or by shadow banks who are unable to create money on the ledger.

Yet another macroeconoimc issue, that will have to be left for further research, is the possibility that a mutualised monetary ledger could be a useful tool for addressing the potential structural shortage of demand, often referred to as 'secular stagnation'. If excessive overhang of debt is making private sector borrowing and expenditure insensitive to interest rates, then direct expansion of the monetary ledger can possibly raise the money stock, spending and inflationary expectaitons which out requiring increased private sector borrowing.

It is clear macroeconomics of the proposal of this paper – including $x$-per cent reserving – need a great deal of further study and will require more formal modelling of the externalities arising both in bank lending together with additional externalities from mutualisation of bank liquidity risk. Such externalities – both positive and negative – arise easily in a payments networks and are only increased by putting all money on a distributed ledger. Further analysis is needed to help determine an appropriate level of the $x$-percent requirement for internalising these externalities.[21]

[21] See (Stein 2012) for discussion of the loan externality, related to the realisation of loan collateral in a crisis.

# 4. Distributed ledger money and Austrian policy objectives.

This section discusses the proposal of this paper as a means of achieving Austrlian monetary objectives.

## Austrian objectives for monetary arrangements.

Austrian economics – while it can be criticised as inward looking doctrinal scholarship focused on interpreting the almost sacred texts of the great Austrian economists and ignoring some of the practical challenges of policy making – provides an insightful conceptual framework for thinking about broader monetary policy issues. It offers a direct explanation of both the breakdown of the post-war Bretton-Woods fixed exchange rate system based on a 'gold exchange' standard (as the result of its failure to impose sufficient discipline on US monetary creation); and the global financial crisis of 2007-2008 (as the result of unsustainable worldwide price sector credit expansion supported by government policy focused on short term expansion of private spending). Austrian economics is also severely critical of the response to these crises.[22]

Reading the key Austrian analysis of monetary arrangements, four policy ideas standout:[23] (a) an underlying monetary standard in which the supply of the medium of exchange is based on a commodity or other substance in limited supply (the classical gold standard is one possibility, a cryptocurrency standard may be another); (b) 'free banking', with minimal limits on the establishment of banks and market discipline limiting the production of money and fiduciary media, possibly with no central bank at all and possibly with competition amongst currencies;[24] (c) limits on the production of fiduciary media (financial claims such as fractionally reserved bank deposits that are readily accepted in payment and immediately redeemable for the medium of exchange); (d) avoidance of all forms of state subsidy and support for banks so their shareholders not taxpayers bear the costs of bank failure.

While some of these Austrian monetary policy ideas – especially restoration of the gold standard -- are outside of mainstream policy debate, there is more widespread agreement on the objectives that Austrian monetary thinkers have sought to achieve from these proposals. They propose a gold standard not as an end in itself or an exercise in nostalgia, but rather because Austrian thinkers see it as the flawed but only truly effective tool for limiting state creation of money.[25] They propose free banking with state subsidy because deposit insurance, central bank liquidity support and 'bail out' of banks encourage risk-taking and poor risk-management. Some also propose limits on the creation of

[22] Some flavour of the reaction of the Austrian economists and their criticisms of government bailouts at the time of the 2008 crisis can be found at https://mises.org/library/bailout-reader .

[23] The Appendix provides a fuller review of Austrian views on monetary arrangements. The insights of Austrian monetary ideas are sometimes obscured by their terminology – distinguishes the widely accepted medium of exchange (a commodity, fiat or credit money) from fiduciary media, which are immediately redeemable promises to pay the medium of exchange which are widely accepted as a substitute for the medium of exchange in payments. For general understanding this Austrian term 'medium of exchange' can be read as the same as what money and banking textbooks refer to as outside, high-powered or base money; and fiduciary media as the same as inside money.

[24] (Hayek 1978; Hayek 1979) proposes removing government monopoly on the supply of money and having instead only private produced currencies, competing for the trust of the public and each trading at different market determined values; but this was a relatively late contribution within the Austrian School, a consequence in part of Hayek coming round to the view that restoration of the Gold standard was not possible.

[25] Von Mises and Hayek were not slow to recognise the costs and disadvantages of using gold as a monetary standard. For example Hayek writes: 'In a securely established world state with a government immune to the temptations of inflation it might be absurd to spend enormous effort in extracting gold out of the earth if cheap tokens would render the same service as gold with equal or greater efficiency.' (Hayek 1937, pg 405)

fiduciary media i.e. bank deposits or other private sector liabilities that serve as money in order to prevent unsustainable private sector credit expansions (nowadays such restriction has become very mainstream, viewed as part of the 'macroprudential' tool kit,  though as a form of state intervention this is not endorsed by all Austrian thinkers). Austrian ideas are outside mainstream debate not because of disagreement about goals of economic policy but because their particular policy proposals are viewed as unrealistic and impractical.

The proposal developed here, the mutual distributed ledger or 'blockchain' that records transactions, can be used for practical implementation all four of these Austrian ideas for monetary arrangements: in particular supporting 'free banking' without need for a bank safety net; and, as would then very possibly be necessary to some degree, introducing additional limitations on bank creation of fiduciary media. Cryptocurrency technology can bring Austrian monetary proposals back within the scope of mainstream economic policy debate.

## Why an unpermissioned cryptocurrency cannot be a monetary standard

First though two 'Austrian myths' about cryptocurrencies should be dispelled. One myth is that the suggestion that a unpermissioned open-source cryptocurrency, like gold, could be a monetary standard outside of state control.

Such arguments circulate frequently in cryptocurrency communities, with statements along the following lines: a cryptocurrency such as Bitcoin is, by construction, in limited supply and therefore – because it is also durable and divisible – shares many features with gold. This analogy is why the term 'mining' was applied to the cryptocurrency proof of work described in the previous section, which validates payments and for which service can be rewarded with newly created currency.[26] Because of this analogy with gold, so it is claimed, a cryptocurrency in limited supply can be a trustworthy replacement for unsound state fiat currencies.

This possibility, that the medium of exchange could be a cryptocurrency, is sympathetically but critically discussed by (Selgin 2015). He views cryptocurrencies such as Bitcoin as a 'synthetic commodities' i.e. like real commodities such as gold or silver the available stock cannot be increased at will by an issuing authority, but unlike gold or silver cryptocurrencies they have no value in any alternative non-monetary use. There are examples of synthetic commodities which have come to be accepted as media of exchange and successfully avoided the inflationary bias of fiat currency.[27] Still, as Selgin admits, the state adoption of a cryptocurrency as a monetary standard seems unlikely, and the possibility of privately created synthetic commodity money supplanting fiat money seems remote – at best it would seem that they might come to be widely accepted in exchange alongside fiat money. He concludes that 'the possibility of monetary stabilization achieved by means of a synthetic commodity standard remains as hypothetical as it is tantalizing'.

[26] The original white paper describing the Bitcoin protocol (Nakamoto 2008) contains a strong statement of the desirability of having money whose supply is not controlled by the state, but instead determined by a peer-to-peer network. This white paper is also the source of the term 'mining' for proof of work rewarded by issue of cryptocurrency.

[27] As an example of a synthetic commodity money Selgin describes the case of the so called Kurdish Swiss Dinar, which circulated in Iraqi Kurdistan from 1993 to the US coalition invasion of Iraq in 2003. It had value in exchange even though it was governed by no monetary authority, was not legal tender and was not accepted as payment by Iraqi public institutions. Unlike the official Iraqi dinar the Kurdish Swiss Dinar proved immune from the large scale loss of value through inflation under the Saddam Hussein regime, its exchange rate against the dollar was stable and supported by the absolute fixity of its supply (unlike the official Iraqi dinar no new Kurdish Swiss Dinars could be printed).

Another possibility might be fixing the value of fiat currency against a well-established cryptocurrency perhaps Bitcoin, requiring the central bank to build up its own reserve of the cryptocurrency, but this could not be seriously considered until the cryptocurrency was already widely used in exchange and from this had achieved comparative stability of value against fiat currency.[28] This is not a realist prospect, for reasons discussed in the next subsection.

## Cryptocurrencies cannot capture a major share of everyday monetary transactions

Another 'Austrian' cryptocurrency myth is that an unpermissioned opensource cryptocurrency could or compete with established fiat currencies for widespread used in every day domestic exchange.*or* it can effectively with established fiat currencies in economic exchange.

Could a cryptocurrency establish itself as a widely used medium of exchange alongside and in competition with fiat currency? The experience of Bitcoin and of other currencies demonstrates that cryptocurrency has appeal as a relatively risky financial investment, at least a modest scale. This though is driven by a number of special factors: technophile's appreciation of the underlying software; the appeal of private cryptocurrencies to individuals seeking to counteract the extraordinary growth in power of the state of the past century, or to those with the more extremely libertarian views of the 'cryptophunk' movement, seeking to exploit cryptography to establish an entire realm of social and economic exchange beyond the reach of the state. There is also a fundamentl demand driven by the practical challenges of avoid currency controls and other financial regulations or use in illegal transactions.[29]

While state authorities have shown great hostility to local or alternative currencies, closing down many of the most successful examples, the combination anonymous peer-to-peer exchange and protection of identity using cryptography makes it relatively difficult to prevent cryptocurrency transactions.[30] The built in quantity limitations on cryptocurrencies also provide a more credible foundation for competition in currencies than basing these on privately issued commitments to exchange in terms of the value of real commodities.[31] For all these reasons cryptocurrencies now seem to be permanently established as alternative financial assets.

Despite this initial success, the volatility of pricing and limitations of both technology and governance – described in the previous section – suggest that no unpermissioned, open-source cryptocurrency can ever capture a major share of payments activity from established fiat currency instruments, whether these are using notes and coin or transferring bank issued fiduciary media.

The great fluctuations of Bitcoin pricing mean that it is not practical to quote prices in BTC (the small amount of Bitcoin or to use BTC as a unit of account. Where BTC is accepted in payment for goods and services it seems to be rapidly exchanged for conventional nation state currency, so Bitcoin is serving merely as a means of exchange – like Paypal – not as an alternative currency.

[28] This relates to the long standing discussion in Austrian monetary economics of difference between the perceived stability of the gold standard proper and the evident instability of the gold-exchange standards established in the 1920s and then again under Bretton-Woods. The stability of gold standard proper is seen by many Austrian economists as resting on the widespread use of gold in direct exchange, e.g. through circulation of gold coin, suggesting that a prerequisite for the use of cryptocurrency as a monetary standard is the widespread use of the cryptocurrency in exchange. See Appendix for references to the literature.

[29] See (Dowd 2014) for discussion of the demand for holding and using cryptocurrencies and other alternative private currencies.

[30] See (Dowd 2014) for discussion of the closure of both the Liberty dollar and e-gold by US authorities.

[31] See (White 2014) for elaboration of this point and references to earlier work of White and (Taub 1985) on on the lack of credibility of a private currency pegged to a commodity index.

There are other potential problems with Bitcoin. The substantial capacity problems of the Bitcoin network remain far from resolution a year and a half after there were first widely discussed amongst network participants. The totally decentralised Bitcoin governance may prevent a satisfactory resolution ever emerging. It is also far from clear that its relatively costly 'proof of work' can be sustained when the creation of new Bitcoins to reward miners is reduced and eventually ceases.

These particular practical challenges highlight the more general difficulty of unpermissioned open-source cryptocurrency network, their lack of governance mechanisms to cope with change. The lack of institutional structure also creates other inherent problems. For example it is not possible to institutionalise reversal of payments – in contrast to the established payment schemes such as Visa or Mastercard, again substantially limiting use in everyday exchange. This is a consequence of the unpermissioned structure with no real world identity, if identities were known it would be easy to establish mechanisms for reversal of payments.

Finally, if conrtrary to this analysis, idespread adoption of unpermissioned open-source cryptocurrencies was to emerge, this would certainly be accompanied by heavy regulatory intervention to control supporting services such as exchanges and wallets, to prevent their use for illegal purposes or evasion of tax. This would be a further heavy 'headwind' against their widespread use.

These challenges suggest that the future of cryptocurrencies in the medium to long term is a flattening out of activity in unpermissioned open source networks, and possibly their being overtaken by permissioned private sector alternatives –supporting much quicker and more resource efficient processing with more flexible and practical governance that adapts to changing economic and business circumstances.

This though is a quite different model, permissioning means also a need for control of identities and therefore integration into existing banking networks based on fiat currencies; so the outcome is not separate competing currencies but just separate competing means of payment. Such developments may effectively challenge bank market power of banks in payment and transaction services but they are not a fundamental change to monetary arrangements.[32] The main exceptions where unpermissioned open-course cryptocurrency may continue to develop are those countries where governments seek to assert control over economic and social activity, through controls on foreign exchange and other regulatory limitations on financial transactions. There unpermissioned cryptocurrency are likely to continue to be attractive as unregulated and unregulatable alternatives to repressed domestic systems of payments and international transactions.

## How mutualisation of deposit money supports some Austrian ideas

While commonly expressed ideas about the relationship between cryptocurrencies and Austrian monetary economics are ill-founded, the proposal of this paper – the mutualisation of deposit money by putting fiat money, bank monetary deposits and money-financed bank loans all on a single mutual distributed ledger – provides a means of achieving almost all of the key objectives promoted by Austrian discussion of monetary arrangements. These can be discussed in turn:

(a) an underlying monetary standard in which the supply of the medium of exchange is based on a commodity (more specifically gold).

[32] For discussion of the competition implications of new payments technologies see (Milne 2016)

It is not the intention here to make the case for the restoration of the classical gold standard. The mainstream consensus view of the economics profession is that the costs of such a policy outweigh the benefits.

In the case of the mutualised monetary ledger proposed in this paper, the goal of avoiding state interference in the money supply, could well be achieved by fairly standard institutional safeguards, along much the same lines as those developed over the past four decades to support central bank independence in the setting of interest rates. For example an politically independent committee could be responsible for determining the quantity of fiat money on the monetary ledger and the extent to which fluctuations in bank money creation should be offset by opposite changes in the stock of fiat money.

Still, it is also clear that the mutualised monetary ledger proposed here *could* be the first step towards a full restoration of the classical gold standard, if that was so desired. The ledger would be legally required both to back the state issued money on the ledger with gold *and* to freely buy and sell the state issued money against gold in the open market at a defined price (carefully set at the outset to avoid misalignment of exchange rates against other countries also on this gold standard). Since all money would then be either gold backed – or temporarily issued bank supported fiduciary money – this would be a major step towards restoring the use of what would effecgtively be gold, albeit in a digital certificate form, in day to day transactions.

Such a standard could also conceivably, with this monetary distributed ledger, be developed along the lines first proposed by Irving Fisher, backed by a diversified index of commodities rather than a single precious metal. The same commitments would be required, holding the basket as backing of the cryptographic ledger and freely buying and selling to maintain a fixed price against the index.

(b) ‘free banking’, with minimal limits on the establishment of banks and market discipline limiting the production of money and fiduciary media, possibly with no central bank at all

The mutualisation of deposit money allows a substantial reduction in the regulation of banks. It can be seen as a simpler, lower cost and more workable version the ring-fencing proposals of the Independent Commission on Banking (Vickers 2011) no implemented in the UK. Six years after that report, the practical challenges are clear, the ring-fencing requires an extensive system of bank monitoring, especially on the funding of bank balance sheets.

Obtaining license for lending, without the accompanying right to issue money on the mutualised ledger, should be made available fairly freely. Such initiatives are viewed best as investment funds, with some need for protection for investors, especially when offered to unsophisticated retail investors, and for retail borrowers, but the extensive panoply of bank regulation is not needed.

The right to issue bank-money on the mutual ledger should require meeting higher standards, in particular some assurance that the overall quality of the balance sheet does not substantially threaten failure of repayment onto the ledger. But comparatively simple rules can suffice to accomplish this (in addition to the $x$-percent reserving their might also be a maximum limit on the ratio of bank monetary deposits to total bank assets .e.g of 50% or 60%, a ratio that would be easily complied with by existing well established banks, low enough to prevent start up banks pursuing a short term gamble against the protection of the ledger.

The only free-banking proposal that is not supported by the mutual distributed ledger is the Hayek proposal for competition amongst commodity-backed currencies.

(c) avoidance of all forms of state subsidy and support for banks

This is achieved by ensuring that, after moving all forms of money onto a mutual distributed ledger, state support to banks is denied or strictly limited, even in a financial crisis. A bank that faced difficulties in funding itself would be first, in the short term, call on a limited stock of central bank reserves (or perhaps better a bank clearing house), then might exploit some a possibility of delaying payment for a strictly limited period and once this opportunity is exhausted face  liquidation.

This in turn means that bank shareholders, and behind them holders of bank debt, become the sole absorbers of bank risk. State support, beyond some possibly very limited provision of money market liquidity, is unnecessary. When banks are liquidated monetary transfers are not interrupted. Retail depositors, who want to make term deposits in return for interest income, need not be protected by state backed deposit insurance. Their loans would likely in the first instance secured on individual bank assets, as is the case for the emerging practice of P2P or market place lending, and any deposit insurance would be entirely private sector. Retail investors would of course be well advised to diversify their investments and consider carefully their risk exposure, but this is not different than the situation which arises in any form of retail financial investment, short or long term.

(d) limitations on the production of fiduciary media

This has already been discussed, it can be achieved using $x$-percent reserving requirement. Another possibility would licensing plus cap and trade (Milne 2013; Stein 2012).

## 5. Conclusions

The importance of technology for money and payments is indisputable. It shapes the forms money takes, the means of payment and the possibilities of different monetary arrangements. Steam-driven stamping of token coins, which could not easily be counterfeited, and their use for small change was arguably a key condition for the 19th century replacement of bimetallic monetary standards by the mono-metallic gold standard, first in the UK and then in other countries.[33] A more recent example (of many) is the development of 'near field communications' or NFC that has been crucial to the rapid growth of contactless payments at point of sale, and hence to the development of alternative monetary services both using mobile phone (ApplePay, AndroidPay) and on stored value cards (such as the transport cards now used in many major cities).[34]

This paper has examined the possibility of improving our monetary arrangements using a new technology, the time-ordered immutable transaction records (blockchains or mutual distributed ledgers) which have been developed to record cryptocurrency transactions. It is argued here that putting all forms of money, both government fiat money and bank money, off-balance sheet on such a distributed ledger can ensure the integrity of money and payments arrangements in the event of bank failure. This would mean that central bank reserves would no longer be needed for settlement of bank payments. In turn this can allow withdrawal of state microprudential regulation and 'too big to fail' protection of banks.

Section 3, drawing on the detail of how cryptocurrencies actually operate and the simplicity of cryptocurrency ledgers, outlines how distributed ledger technology can protect transactions deposits and payments from bank failure. This is achieved by placing all bank created money and the bank lending that this funds, together with government issued fiat money, onto a single distributed ledger shared by all users of money. This is a permissioned cryptocurrency network, protecting transaction deposits and payment arrangements from the consequences of bank failure (because all money is a claim on the network not on individual banks) while allowing banks to continue funding their loan books using monetary deposits (banking continues to be fractionally reserved ensuring elasticity in the supply of both money and credit).

The distinction between base or outside money and bank or inside money then vanishes. The two forms of money become one, with total supply the combination of the amount created through government unbacked issue and funding for bank lending through bank money creation. Bank money creation cannot increase unsustainably because of the commitment to repay money onto the ledger as loan principal is repaid by borrowers. This is supported by a 'triple lock': if the borrower defaults, the repayment is underwritten in the first instance by the lending bank and behind them by the entire banking industry. Moreover, even if the entire industry fails, the ledger remains intact. Micro-prudential regulation of banks, moreover, can become an industry not state responsibility.

Section 4 explains how this reform can be used to support ideas on monetary arrangements promoted within the Austrian school of economics. The association between cryptocurrencies and Austrian economics is nothing new. Bitcoin, the best known example of such a cryptocurrency, has from the outset, been associated with the libertarian case for radical reduction in the role of the social and economic role of the state. It is argue that the limited supply of Bitcoin and its independence of banks and government can establish a monetary system completely independent of the state. The analysis here suggests this is naïve. For several reasons, not least the weaknesses of

[33] See (Redish 2006).

[34] (Coskun et al. 2013) provide a review of research literature on this technology.

cryptocurrency governance, permissionless open-source cryptocurrencies such as Bitcoin cannot become credible and widely used payment alternatives to established nation-state currencies.

An alternative Austrian perspective on cryptocurrencies emerges here. This is that the technology of distributed ledgers allows withdrawal of the government-backed bank safety net (deposit insurance and other implicit guarantees are no longer need to protect transaction deposits and payments) and reduces the need for the central bank to act as 'lender of last resort'. Furthermore, while bank money is still fractionally-reserved and finances bank lending, it is then possible to limit the degree of fractional reserving by requiring banks to commit a proportion of their own money to the ledger.

There are two supporting Appendices. Appendix A provides a detailed account of the operation of cryptocurrencies, summarising the underlying cryptography, the challenge of achieving of consensus, and emphasising the very simple nature of the records that are stored in the transaction ledgers. It points out that the analogy with physical notes and coin is misleading, value on cryptocurrencies rests on the operation of the network as a whole, the individual records do not have an independent existence. This appendix also discusses the governance challenges of unpermissioned open-source cryptocurrencies and suggests that permissioned ledgers are much better suited to coping with changes in the economic and business environment in which they are used. Appendix B provides a short review of Austrian economics, focusing on Austrian proposals for monetary arrangements.

To what extent is the proposal of this paper Austrian? Austrian scholars have typically argued that the extensive role of the state in money and banking has arisen because of the capture of government by special interest groups, for example incumbent banks who seek the protection of government when expansion of lending results in large scale losses. For them the means of limiting state involvement is ultimately political: persuading society at large that state support of banks is damaging to the general social interest and adopting a range of policies, for example commodity backed money or competing currencies that would limit this state involvement.

The proposal set out here seems to be a promising means for ac hieving this Austrian objective of reducing the role of the state I money and banking. While the end is the same, the means of achieving this end is technological not political. Under the technologies of banking that have held sway from the late 19th to the early 21st century, substantial state intervention in money and banking has become unavoidable because of the central economic role of banks both in the supply of credit (financed from money creation i.e. on a fractionally reserved basis) and in providing the dominant means of exchange (transaction deposits). The consequence is that in a crisis government has had little or no choice but to support banks. The new technology of distributed ledger that supports cryptocurrencies such as Bitcoin can – through mutualisation of monetary deposits – appear to offer a way out of this bind.

In contrast to much Austrian monetary thinking government would, under the proposal envisaged here, retain a central institutional role in the supply of money. The ledger still supports state supported fiat money. There would have to be some government agency – perhaps a division of the central bank – determining the total stock (subject to appropriate governance, such as meeting a monetary target or a '$k$-per cent' rule). So this not a proposal for a purely private money or monies.

Still, placing all money on a distributed ledger could be a staging post to fuller implementation of Austrian proposals. The ledger would for example facilitate replacement of fiat money by money backed by a commodity such as gold and possibly also competition between different commodity backed ledger monies.

Even if not used as a means for implementing these further Austrian proposals, there are Austrian arguments in favour of the proposal put forward here. Austrian school thinking provides some strong and fundamental criticisms of the existing monetary policy consensus. It provides a plausible account of the financial crises, including 2007-2008, as the consequence of both the promise of state bail-out of failing banks and of government efforts to promote private sector spending through expansionary monetary policy, together leading to unsustainable growth of bank money and credit. Austrian analysis also argues that these same state interventions continue today, so there remains a threat of further unsustainable money and credit expansions and future financial crises. If these Austrian arguments are accepted, then the case for mutualising all deposits and fiat money on a distributed ledger is a particularly strong one.

Three final thoughts. First, the case for mutualisation of monetary deposits made here has relied on relatively intuitive arguments. More formal analysis will be needed, for example mathematical modelling of the monetary economics of ledger based monetary arrangements suggested here, exploring mechanisms that are ignored or simplified in the present discussion and check on the consistency of the argument.[35]

Second, note that central bankers, debating the possibility of sponsoring their own issue of cryptocurrencies (a digital dollar, Euro, Yen or pound that can be transferred directly from holder to holder just like Bitcoin) have thought of using cryptocurrency as a digital extension of the current central bank issue of bank notes. As a result they struggled to develop a strong case for central bank issue of cryptocurrency. The demand is not obvious given that existing banks instruments together with notes and coin fulfil most day to day payments both remote and at point of sale fairly well.

The proposal of this paper, combining fiat and bank money together with bank loans funded by money creation altogether on a single mutual distributed ledger, indicates that this is too narrow a way of thinking. Even if this particular proposal is not pursued, it indicates how new technology reopens major questions and debates about monetary arrangements.

Third and last, there are a number of further intriguing monetary-macroeconomic issues raised by the proposal of this paper. The shift to a single monetary ledger would substantially change monetary policy operations. It seems to provide a direct way to get around the constraints of the ‘zero lower bound’ (just issue more money on the ledger). More generally, what is the appropriate operation of monetary policy when money is on a distributed ledger? Would there be any need at all for an interest rate rule such as that of John Taylor? A quantity of money rule might well be more appropriate, leaving market interest rates to be determined by the market not the central bank. Indeed it raises the deeper questions of what, exactly , would the role of the central bank be.

Mutualising money on a distributed ledger might also help provide better macroeconomic instruments for dealing with unsustainable asset price increases and structural imbalances, e.g. persistent and unsustainably low savings ratios. Credit could be restrained through $x$-per cent reserving while monetary expansion is used to maintain aggregate demand. Could the combination of direct control of the quantity of money and $x$- per cent reserving allow pursuit of two macroeconomic targets e.g. price stability and overall structural balance, avoiding excess- or under-savings? These and other monetary-macro questions are left for further research.

[35] One insightful exercise of this kind, related to the present paper, is by (Barrdear & Kumhof 2016)

## References

Ali, R. et al., 2014a. Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, p.Q3.

Ali, R. et al., 2014b. The economics of digital currencies. *Bank of England Quarterly Bulletin*, p.Q3.

Andolfatto, D., 2015. MacroMania: Fedcoin: On the Desirability of a Government Cryptocurrency. *Macromania Blog*. Available at: http://andolfatto.blogspot.co.uk/2015/02/fedcoin-on-desirability-of-government.html.

Badev, A.I. & Chen, M., 2014. *Bitcoin: Technical background and data analysis*,

Barrdear, J. & Kumhof, M., 2016. The Macroeconomics of Central Bank Issued Digital Currencies.

Boettke, P. & Leeson, P., 2003. The austrian school of economics: 1950-2000. *Blackwell companion to the history of economic thought. Oxford: Basil Blackwell Publishers*.

Boettke, P.J. & Palagashvili, L., 2016. The Comparative Political Economy of a Crisis. In *Studies in Austrian Macroeconomics*. Emerald Group Publishing Limited, pp. 235–263.

Butarin, V. & Ethereum Community, 2017. *Ethereum White Paper*, Available at: https://github.com/ethereum/wiki/wiki/White-Paper.

Capie, F. & Wood, G.E., 1991. *Unregulated Banking: Chaos Or Order?*, Springer.

Chaum, D., 1983. Blind signatures for untraceable payments. In *Advances in cryptology*. Springer, pp. 199–203.

Clark, J., 2016. The Long Road to Bitcoin. In A. Narayanan et al., eds. *Bitcoin and Crypto Currency Technologies*. Princeton University Press, pp. ix–xxvii.

Coskun, V., Ozdenizci, B. & Ok, K., 2013. A survey on near field communication (NFC) technology. *Wireless personal communications*, 71(3), pp.2259–2294.

Dowd, K., 2014. New Private Monies: A Bit-Part Player?

Dowd, K. & Timberlake, R.H., 1998. *Money and the Nation State: The Financial Revolution, Governement and the World Monetary System*, Transaction Publishers.

Ethereum Community, 2017. History of Ethereum. *Ethereum Homestead 0.1 documentation*. Available at: http://ethdocs.org/en/latest/introduction/history-of-ethereum.html [Accessed March 23, 2017].

Friedman, M. & Schwartz, A.J., 1963. *A monetary history of the United States, 1867-1960*, Princeton University Press.

Fung, B.S.C. & Halaburda, H., 2016. Central Bank Digital Currencies: A Framework for Assessing Why and How.

Gerring, T., 2016. Cut and try: building a dream. *Ethereum Blog*. Available at: https://blog.ethereum.org/2016/02/09/cut-and-try-building-a-dream/ [Accessed March 23, 2017].

Government Office for Science, 2016. *Distributed Ledger Technology: Beyond Block Chain*, London. Available at: https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review [Accessed January 30, 2016].

Graeber, D., 2014. *Debt: the first 5,000 years* 2nd ed., Melville House.

Hawtrey, R.G., 1919. *Currency and credit*, London, Longmans.

Hayek, F.A., 1978. *Denationalisation of Money–The Argument Refined*,

Hayek, F.A., 1979. *Free Market Monetary System, A*, Ludwig von Mises Institute.

Hayek, F.A., 1937. *Monetary nationalism and international stability*, Longmans, Green.

Hayek, F.A., 1933. *Monetary Theory and the Trade Cycle* 1st ed., Jonathan Cape.

Hayek, F.A., 1932. *Prices and production*, Ludwig von Mises Institute.

Hertig, A., 2017. CoinDesk Explainer: The Bitcoin Unlimited Debate. *Coindesk*. Available at: http://www.coindesk.com/coindesk-explainer-bitcoin-unlimited-debate/ [Accessed March 23, 2017].

Hulsmann, J.G., 2012. The Early Evolution of Mises' Monetary Thought. In *Theory of Money and Fiducary Media: Essays in Celebration of the Centennial*. Mises Institute.

Jordà, Ò., Schularick, M. & Taylor, A.M., 2016. The great mortgaging: housing finance, crises and business cycles. *Economic Policy*, 31(85), pp.107–152.

Knapp, G.F., 1924. The state theory of money. *History of Economic Thought Books*.

Koenig, A., 2015. *A Beginners Guide to Bitcoin and Austrian Economics.*, FinanzBuch Verlag.

Koning, J., 2014. Fedcoin. *Moneyness blog*. Available at: http://jpkoning.blogspot.co.uk/2014/10/fedcoin.html.

Lamport, L., Shostak, R. & Pease, M., 1982. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3), pp.382–401.

Lehmann, A., 2016. Building the trust engine: Collaborating on a better financial system with blockchain. *UBS News for Banks*. Available at: https://www.ubs.com/magazines/news-for-banks/en/products-and-services/2016/building-the-trust-engine.html [Accessed April 15, 2017].

Leinonen, H., 2016. Virtual currencies and distributed ledger technology: What is new under the sun and what is hyped repackaging? *Journal of Payments Strategy & Systems*, 10(2), pp.132–152.

Mainelli, M. & Milne, A., 2016. *The Impact and Potential of Block chain on the Securities Transaction Lifecycle*,

Mainelli, M. & Milne, A., 2016. The Impact and Potential of Blockchain on Securities Transaction Lifecycle. *SWIFT Institute Working Paper*, (2015).

Menger, C., 1892. On the Origins of Money. *Economic Journal*, 2, pp.239–255.

Milne, A., 2013. Register, Cap and Trade: A Proposal for Containing Systemic Liquidity Risk. *Economics: The Open-Access, Open-Assessment E-Journal*, 7(2013–7). Available at: http://dx.doi.org/10.5018/economics-ejournal.ja.2013-7.

Milne, A., 2009. *The Fall of the House of Credit: What Went Wrong in Banking and what Can be Done to Repair the Damage?*, Cambridge University Press.

Milne, A. & Wood, G., 2008. *Shattered on the Rock? British financial stability from 1866 to 2007*, Available at: http://ideas.repec.org/p/hhs/bofrdp/2008_030.html.

Milne, A.K.L., 2016. competition policy and the financial technology revolution in banking. *Digiworld Economic Journal*, (103), pp.145–161.

Von Mises, L., 1949. *Human action: A treatise on economics*, New Haven: Yale University Press.

Von Mises, L., 1953. *Theory of Money and Credit, The* Revised., Indianapolis: Ludwig von Mises Institute. Available at: http://cc10.aubg.bg/faculty/kpetrov/Other/Textbook Downloads/von Mises - Theory of Money and Credit.pdf [Accessed July 9, 2014].

Monetary Authority of Singpore, 2017. MAS working with industry to apply Distributed Ledger Technology. *Media Release*. Available at: http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-working-with-industry-to-apply-Distributed-Ledger-Technology.aspx.

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., et al., 2016. *Bitcoin and cryptocurrency technologies*, Princeton University Press. Available at: http://bitcoinbook.cs.princeton.edu/.

Narayanan, A., Bonneau, J., Felten, E., Felten, A., et al., 2016. *Bitcoin and Cryptocurrency Technologies*, Princeton University Press.

Ólafsson, Í.A., 2014. Is Bitcoin money? An analysis from the Austrian school of economic thought.

Popper, N., 2015. *Digital Gold*, Harper Collins. Available at: https://www.harpercollins.com/9780062362513/digital-gold.

Potashnik, A., 2015. The Virtual Medium of Exchange; The Potential Benefits of Cryptocurrencies in the Reduction of Social and Transactional Costs and the Subjectivist Approach to Money.

Rambure, D. & Nacamuli, A., 2008. *Payment systems: From the salt mines to the board room*, Springer.

Redish, A., 2006. *Bimetallism: An economic and historical analysis*, Cambridge University Press.

De Roover, R., 1942. Money, banking, and credit in medieval Bruges. *The Journal of Economic History*, 2(S1), pp.52–65.

Rothbard, M.N., 2002. *History of Money and Banking in the United States: The Colonial Era to World War II, A*, Ludwig von Mises Institute.

Rothbard, M.N., 1991a. *The case for a 100 percent gold dollar* 2nd ed., Libertarian Review Press. Available at: https://mises.org/library/case-100-percent-gold-dollar-0.

Rothbard, M.N., 1991b. *The case for a 100 percent gold dollar* 2nd ed., Libertarian Review Press.

Rothbard, M.N., 1990. *What Has Government Done to Our Money?* 3rd ed., Ludwig von Mises Institute. Available at: https://mises.org/system/tdf/What Has Government Done to Our Money_3.pdf?file=1&type=document.

Schwartz, A.J., 1989. Banking school, currency school, free banking school. *The New Palgrave: Money. London and Basingstoke*, pp.41–49.

Scott, S. V & Zachariadis, M., 2013. *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): cooperative governance for network innovation, standards, and community*, Routledge.

Sechrest, L.J., 2008. *Free banking: theory, history, and a laissez-faire model*, Ludwig von Mises Institute.

Selgin, G., 2015. Synthetic commodity money. *Journal of Financial Stability*, 17, pp.92–99. Available at: http://www.sciencedirect.com/science/article/pii/S1572308914000722 [Accessed June 7, 2015].

Selgin, G.A. & White, L.H., 1994. How would the invisible hand handle money? *Journal of Economic Literature*, 32(4), pp.1718–1749.

Selgin, G. & White, L.H., 1996. In defense of fiduciary media—or, we arenot devo (lutionists), we are Misesians! *The Review of Austrian Economics*, 9(2), pp.83–107.

Shubber, K., 2014. The 9 Biggest Screwups in Bitcoin History. *Coindesk*. Available at: http://www.coindesk.com/9-biggest-screwups-bitcoin-history/ [Accessed March 23, 2017].

Skingsley, C., 2016. Should the Riksbank issue e-krona? Speech at FinTech Stockholm, 16 Nov 2016, revised 30 Nov 2016. Available at: http://www.riksbank.se/en/Press-and-published/Speeches/2016/Skingsley-Should-the-Riksbank-issue-e-krona/ [Accessed April 15, 2017].

Smith, P. & Atlas, K., 2016. A Brief History of Bitcoin Forks. *Blockchain Blog*. Available at: https://blog.blockchain.com/2016/02/26/a-brief-history-of-bitcoin-forks/ [Accessed March 23, 2017].

Smith, V., 1936. *The rationale of central banking and the free banking alternative (1990 reprint)* reprint., Indianopolis: Liberty Press. Available at: http://www.getcited.org/pub/102882655 [Accessed November 9, 2010].

Stein, J.C., 2012. Monetary policy as financial stability regulation. *The Quarterly Journal of Economics*, 127(1), pp.57–95.

Taub, B., 1985. Private fiat money with many suppliers. *Journal of Monetary Economics*, 16(2), pp.195–208.

Treacher, M., 2016. Announcing Ripple’s Global Payments Steering Group | Ripple. *Ripple Insights*. Available at: https://ripple.com/insights/announcing-ripples-global-payments-steering-group/ [Accessed March 23, 2017].

Turner, A., 2015. *Between Debt and the Devil: Money, Credit, and Fixing Global Finance*, Princeton University Press.

Vickers, J., 2011. *Independent commission on banking: final report*,

White, L.H., 2014. The market for cryptocurrencies.

Wicksell, K., 1898. *Geldzins und Güterpreise*, G. Fischer.

Wood, G., 2014. *Ethereum: A secure decentralised generalised transaction ledger*, Available at: http://gavwood.com/paper.pdf.

# Appendix A. Cryptocurrencies: how they actually work

This paper argues that there can be considerable economic benefits from transferring all money whether fiat or bank issued onto a single mutual distributed ledger, i.e. a 'blockchain' similar to those used by cryptocurrencies such as Bitcoin. The perspective is 'Austrian' because this helps both remove state support for banks and discourage unsustainable expansion of bank money and credit through fractionally reserved deposit taking, two central proposals in Austrian monetary analysis.

The validity of this argument depends on the detail of cryptocurrency and blockchain technologies. Much of the discussion of the business applications and policy implications of cryptocurrencies and their supporting transaction records (blockchains) is high level, based on analogies with physical money such as notes and coin. Analogies can be misleading and lead to erroneous conclusions. This section provides a sounder foundation, describing those key technical features of cryptocurrencies and blockchain needed for understanding their potential monetary application.

Features that are especially relevant include the following: (a) while much attention has been focused on the cryptographic methods used for checking validity of cryptocurrency transactions and confirming them, equally important to potential applications is to recognise the extreme simplicity of what is recorded on the blockchain or distributed ledger (the time-ordered immutable record of cryptocurrency transactions). There are essentially only two types of entry – the first records the creation of a coin (either 'de novo', i.e. entirely new, or as a result of an earlier expenditure of another coin); the second (and necessarily subsequent) records the spending of the coin (conflicting records of spending are prevented by checks carried out by the core computer coding of the cryptocurrency on the entire transactions record). (b) the term 'coin' is misleading, suggesting that a cryptocurrency record cannot be duplicated, but in fact the transfer records can be and are duplicated many times; what is unique is the transfer of cryptocurrency, this happens once and once only with the creation of the expenditure record in the ledger which cannot be subsequently altered or reversed (c) the core computer coding underpinning cryptocurrencies needs to be maintained and updated, creating unavoidable challenges of governance for cryptocurrencies, challenges which are particularly difficult if the network is completely decentralised with no management structure and complete freedom to join the network.

## The major cryptocurrencies

As a preliminary, Table 1 reports the market capitalisations of the 20 leading cryptocurrencies both in absolute dollar amounts and as a share of the total.

Bitcoin is by far the largest cryptocurrency by market capitalisation.[36] It was announced on 30th November 2008 through an email to a cryptographic mailing list with a link to the nine page white paper describing the protocol (Nakamoto 2008).[37] 9th January 2009 saw the posting of version 0.1.0 of the open source code implementing the protocol on the software directory Sourceforge. This protocol did not come out of nowhere, rather it built on two decades of prior effort to create an internet currency that could operate across borders and without government support.[38]

[36] The history of Bitcoin is retold by (Popper 2015), vividly describing the transition of the Bitcoin community from its early roots in the 'cypherpunk' movement to a much broader range of participation. Additional technical history can be found in (Narayanan, Bonneau, Felten, Felten, et al. 2016).

[37] The original mailing to gmane.comp.encryption.general is reproduced here https://ihb.io/2015-08-11/news/word-cloud-the-original-satoshi-nakamoto-bitcoin-white-paper-5638

[38] (Clark 2016) reviews earlier efforts to create the electronic equivalent of notes and coin on the internet, for example the use of 'blind signatures' allowing David Chaum'se-cash to be used for anonymous online transfer.

While Bitcoin attracted little attention initially, interest built up over time.[39] By 2010 the first Bitcoin exchange Mt. Gox was operating, allowing the currency to be used for a variety of purposes (including illegal purchases on the 'dark web' anonymous website Silk Road) and revealing for the first time a market price for Bitcoin in terms of US dollars.[40] By 2011 it was establishing a critical mass of users and credibility as an open source peer-to-peer money. Its success in attracting participation in its network is reflected in the rising market price of Bitcoin in terms of US dollars.[41] 1BTC, the Bitcoin unit of account, which was worth less than 10¢ in 2010Q3, experienced four major price peaks, each successively higher than the one before: $35 in mid -011; $136 in April 2013, $1,120 in Nov 2013, and an all-time peak of $1267 in early March of 2017. There have been substantial price fluctuations between these peaks, for example falling to only $270 in January 2015.

**Table 1: the 20 leading cryptocurrencies as of March 9th, 2017**

| Rank | | Name & link on Coinmarket Cap | Date of launch | Ticker | Market Capitalisation | |
|---|---|---|---|---|---|---|
| | | | | | US dollars | Percent |
| 1 | | Bitcoin | Jan, 2009 | BTC | $18,774,053,810 | 84.66% |
| 2 | | Ethereum | Aug, 2015 | ETH | $1,529,262,607 | 6.90% |
| 3 | | Dash | Jan, 2014 | DASH | $306,741,545 | 1.38% |
| 4 | | Ripple | Sep, 2014 | XRP | $244,556,871 | 1.10% |
| 5 | | Litecoin | Oct, 2011 | LTC | $190,232,580 | 0.86% |
| 6 | | Monero | Apr, 2014 | XMR | $177,583,908 | 0.80% |
| 7 | | Ethereum Classic | Jul, 2016 | ETC | $115,647,290 | 0.52% |
| 8 | | NEM | Mar, 2015 | XEM | $83,963,700 | 0.38% |
| 9 | | MaidSafeCoin | Apr, 2014 | MAID | $63,237,411 | 0.29% |
| 10 | | Augur | Oct, 2015 | REP | $58,390,090 | 0.26% |
| 11 | | Tether | Feb, 2015 | USDT | $34,950,727 | 0.16% |
| 12 | | Zcash | Oct, 2016 | ZEC | $29,366,511 | 0.13% |
| 13 | | Iconomi | Sep, 2016 | ICN | $27,803,634 | 0.13% |
| 14 | | Factom | Oct, 2015 | FCT | $25,156,051 | 0.11% |
| 15 | | Dogecoin | Dec, 2013 | DOGE | $22,053,765 | 0.10% |
| 16 | | Waves | Jun, 2016 | WAVES | $19,751,200 | 0.09% |
| 17 | | Steem | Apr, 2016 | STEEM | $19,360,523 | 0.09% |
| 18 | | DigixDAO | Apr, 2016 | DGD | $18,423,880 | 0.08% |
| 19 | | Golem | Nov, 2016 | GNT | $16,576,956 | 0.07% |
| 20 | | Ardor | Jul, 2016 | ARDR | $15,326,151 | 0.07% |
| | | Total (584 cryptocurrencies) | | | $22,176,297,703 | 100.00% |

Source: Coinmarketcap website https://coinmarketcap.com/all/views/all/ and author's calculation. Coinmarketcap lists some 747 cryptocurrencies of which they had information. The 584 are those for which they had information on both the number of units in existence and a recent transaction price.

Since 2011, a large number of other cryptocurrencies have been launched, all building on features of Bitcoin and of the blockchain, its supporting distributed transaction record. These 'altcoins' have had a wide variety of motives and purposes, improving weaknesses of Bitcoin, developed as a hobby or

[39] Google trends provides a useful indication of the evolution of interest in Bitcoin: https://trends.google.com.au/trends/explore?date=2009-01-09%202017-03-23&q=bitcoin

[40] (Popper 2015) tells much of this story. Mt Gox ceased operating in Feb 2014, due to large scale hacking which resulted in the theft of more than 800,000BTC worth of Bitcoin; Silk Road was shut down by the FBI in October 2013, though successor 'dark net' websites have been established since.

[41] Blockchain.info maintain a historical price chart: https://blockchain.info/charts/market-price?timespan=all

a coding exercise or sometimes in the hope of making a substantial financial gain from rising prices as a currency attracts a critical mass of users.[42]

Ethereum – which like most cryptocurrencies shares the open source philosophy of Bitcoin – is the product of a team of young software developers, Vitaly Butarin, Gavin Wood, Jeffrey Wilcke and others.[43] Unlike Bitcoin it supports an unlimited number of 'blockchains' (or distributed ledgers, the shared transaction records underpinning all cryptocurrencies) within a flexible and fully specified developer application environment that can be used for a wide range of applications, not just the single blockchain for recording of transfers of value (aka 'The Blockchain') that supports Bitcoin.

Dash is the most successful altcoin. Dash is distinguished from Bitcoin by a software based process for supporting community approval of new code and a relatively fast final transfer. Ripple – founded by one of the early Bitcoin pioneers – is a platform and cryptocurrency designed for executing immediate international inter-bank transactions. Litecoin is a variant of Bitcoin, explicitly designed for small value transactions. Monero is designed to support much stonger privacy protection than Bitcoin (where real world identity can potentially be worked out from transaction histories).[44]

## Some distinctive features of cryptocurrencies

A cryptocurrency, such as Bitcoin, is a representation of value that can be transferred virtually over the internet. Alice pays Bob through a transaction that reduces her claim on the Bitcoin network by say 0.1 BTC and correspondingly increases Bob's claim on the Bitcoin network by 0.1 BTC.

Unlike earlier less successful efforts at developing virtual internet currencies, cryptocurrencies have no central issuer. They are decentralised network currencies, removing any concern that they might fail because of the loss of a central node or server. They are also private currencies, with no government involvement or support. They have no intrinsic value – in contrast to some other virtual currencies transferrable over the internet such as e-gold that represent a claim on an underlying commodity and can be redeemed in exchange subject to some fee for the gold it represents.

The representation of value – the coins in Bitcoin – are for one-time use only. This means, in contrast to some earlier virtual currencies such as e-cash, change is not a concern because 'coins' are divided and combined in every transaction, creating larger or smaller coins as needed.[45] For example suppose Alice has a Bitcoin worth 0.3BTC and wants to send 0.1BTC to Bob. Her instruction takes the

[42] While most cryptocurrencies listed in Table 1 are Altcoins, the term is not really appropriate for Ethereum -- which is a decentralised applications platform which happens to support a cryptocurrency – or Ripple – which is not open source or peer-to-peer).

[43] On the concept see the updated version of the Ethereum white paper (Butarin & Ethereum Community 2017), technical implementation is described in hyWood's 'yellow paper' (Wood 2014) while the history of Ethereum is documented by (Ethereum Community 2017; Gerring 2016).

[44] Amongst the other 'Altcoins' Dogecoin – while no longer as popular or valuable as in the first two years after its launch – is often highlighted because its user community is based not on opposition to established institutions and government or commitment to open source coding, but on humour and attachment to a particular 'meme' an rather, cuddly image of a Japanese breed of dog. Dogecoin is perhaps best known for its sponsorship through crowdfunding of the Jamaican bobsleigh team in the 2014 Winter Olympics.

[45] The term 'coin' is now accepted usage, e.g. Bitcoin or altcoin, but 'token' is perhaps more appropriate since the binary strings themselves only have meaning and value within the context of the entire network and its supporting transactions record. The choice of the word coin is though understandable: 'Bittoken' and 'alttoken' would not be so appealing to potential users.

entire coin worth 0.3BTC, extinguishes (or 'spends') it, replacing it with two coins 0.2BTC for Alice herself and 0.1BTC for Bob.[46]

There is no reliable breakdown of the types of cryptocurrency transactions in private, permissionless, open-source networks. The available evidence suggests that few transactions are for purchase of goods and services.[47] Total transaction volumes are low relative to conventional established bank payment systems.

The security of cryptocurrency transfers rests on standard tools of cryptography (see Box 1), notably digital signatures confirming who in the network is making a payment instruction.

Unlike conventional notes and coin, cryptocurrencies come in an (almost) unlimited number of denominations. Values in the Bitcoin network are represented in a unit of account BTC. The value of any given is an integer number of 'Satoshi' ($10^{-8}$ BTC). Since the network has been designed to support 21 million BTC this means that there $21 \times 10^{14}$ different possible denominations of Bitcoin!

Just as with physical currency, transactions in cryptocurrency can be anonymous with no record of who has made transactions (though this depends on the coding supporting the network).

## The immutable time-ordered record of network transfers

Cryptocurrency has no physical existence so how does transfer take place? Transfers are recorded on an immutable and time-ordered record of all past transactions shared between and agreed by all users: what is commonly referred to as a 'blockchain'. Immutable meaning the record cannot be subsequently challenged, e.g. by the payer claiming that they did not make the payment.

While double spending can be can be prevented by recording money on a central server, such central storage creates new problems of security and trust, for example concern that someone might have access to and alter the central record.[48] To overcome these problems of trust and security the immutable record of a cryptocurrency is shared amongst network participants.

Each record of value or coin on a cryptocurrency network consists of at most two quite long binary numbers stored at different locations on the time-ordered immutable transactions record. One number documents the creation of the coin and the cryptographic link to its owner, a node on the network. If and when the coin is eventually spent, a second number appears as part of subsequent transaction record, with a cryptographic link back to the creation of the coin.[49]

[46] One drawback of the word 'coin' is the inaccuracy of the associated mental image, the transfer of an object – a coin – from one holder to another. A more accurate image is the melting down of a coin (or coins), the resulting bullion used for minting new coins.

[47] (Badev & Chen 2014) report, in their analysis of Bitcoin transaction data from 2012 to early 2014, that most biicoin transactions are small value (<$100) and a majority of these were for use in the online Bitcoin gambling site Satoshi dice. A small number of very large transactions increase average transaction size massively, to over $40,000 in late 2013. They also examine transction patters of public keys, to try and determine if transactions are payments related. Turnover of Bitcoin is low. Overall they conclude that, despite 64,000 registered domains accepting bitcoin in payment, there was very little use of Bitcoin as payments for goods and services.

[48] David Chaum's e-cash, one of the forerunners of Bitcoin, had a central issuer Digicash.

[49] This means that every uniquely identified Bitcoin thus appears in *at most* only two transactions. The first in which the 'unspent' coin is created and a second one-time only transaction when it is 'spent' creating other coins. The spent coin is however not destroyed, the record of both its creation and its expenditure remaining forever on the Bitcoin blockchain.

### Box 1: some basics of cryptography

This box explains the cryptography used in computer networks, including cryptocurrency networks. The tools used are easily understood without any knowledge of the supporting mathematics.

Anything recorded on a computer – a written document, an audiofile, a video, an email – is a binary number, possibly very large. Computer records – like any other numbers – can be combined together in many ways to create others numbers (one simple example of many, multiplication of two numbers to yield a third number). These transformations can also sometimes be reversed (in this example, factoring the third number to obtain the original two numbers).

Computer cryptography uses matching pairs of numbers called keys, together with a transformation rule (or algorithm, there are a number of standard cryptographic algorithms), operating as follows:

Encrypt(key, original record) -> encrypted record  
Decrypt(matching key, encrypted record) -> original record

The transformation rule is such that it is effectively impossible (a brute force search would take a very, very long time) to work out the other matching 'private' key from the public key.

*Message encryption.* I release a public key. Anyone can use the rule and my public key to transform any computer record they choose into encrypted form. This is no longer useable until the transformation is reversed, recovering the original record. Thus, provided I have not shared my private key, only I can read the encrypted message (or any other record encrypted in this way).

*Digital signature*. I release three things: the original record, the encrypted record and a public decryption key. Anyone can confirm (by applying the key and obtaining the encrypted record) that the record was encrypted by the 'owner' of the two matching keys. Just like a physical signature, the owner cannot deny having 'signed' i.e. conducted the encryption.

In the case of the unpermissioned open-source network, such as Bitcoin, identity is nothing more than the public key used on the network. Matching private and public keys are created by nodes on the network. Bitcoins are created by 'sending' to a public key. They can only be subsequently spent through an instruction digitally signed by the owner of the matching private key.

*Certification.* What about, when as is often the case in computer networks, participants want to link a public key to a real-world identity e.g. in online shopping (or indeed any form of browsing)? This cannot be done with cryptography alone. The (imperfect) solution is the issue of digitally signed certificates by a 'certification authority', confirming after a process of verification that public keys are associated with particular registered internet domain names. There are different levels of verification and a variety of certification authorities.

*Blind signatures.* What if I want to have an instruction signed as valid without revealing my public key (identity)? This is possible with a central authority using *two* different transformation functions: the first when the authority digitally signs a computer record containing a public key (confirming e.g. that the owner has available funds or the right to vote); the second 'stripping' the record, altering it into a form in which the public key is no longer revealed but the authorities digital signature can still be checked. This technique, first proposed by (Chaum 1983), has been used to support the anonymous transfer electronic currency (including Chaum's e-cash) and in anonymous online voting.

Note that cryptographic keys are effectively both costless to produce and infinite in number. With 256 bit numbers, so there are (nearly) $2^{256}$ possible keys. As a result, to support anonymity and additional security, matching keys may be used on a one-time only transaction by transaction basis.

The coins representing value are for one-time use only but they are not destroyed, the record of both creation and expenditure remaining forever on the Bitcoin blockchain.[50] The length of the numbers representing value on the Bitcoin network allows them to be used as information carriers with information of all kinds stored on the blockchain with no possibility of being subsequently altered. This includes the information required in the time-ordered record (a public key of the owner of the coin, possibly in a 'masked' form so their identity is not revealed, which acts as the link back to the block and location within the block of the transaction that first created the coin). It may also include a lot of other information determined by users, a possibility that supports a great variety of other applications, not just cryptocurrency transfer, and explains much of the excitement about 'blockchain' that has emerged in the business world.[51]

## The challenge of consensus

In the jargon of payments professionals any cryptocurrency transfer, for example the transaction which reduces Alice's holdings of Bitcoin and increases Bob's holdings of Bitcoin by 0.1BTC, is final as soon as it is added to the blockchain. Three things are required to maintain this shared immutable record:

1. The use of digital signatures to verify who is instructing the transfer of currency. Digital signatures are the well-established cryptographic techniques available since the 1970s for ensuring authentication (identifying that sender owns the money), non-repudiation (the sender cannot deny having sent the message) and integrity (the message was not altered in transit).[52] Sending a cryptocurrency is only possible with access to the owner's private cryptographic 'key'; a matching public key serves as the identifier or address of the owner in the network and can be used by anyone to verify that this is the person making the payment instruction.[53]
2. An efficient process for searching through the transaction record to verify that the record of value being input into the transaction exists and is unspent.[54] The Bitcoin protocol has a number of technical features to make this an efficient, rapid search.[55]
3. A process for establishing consensus amongst the participants of the system on an updated version of the immutable transaction record. This is problematic because of *latency*. Were all instruction communications instantaneously transmitted throughout the network then digital signatures alone would be enough to ensure a unique transaction record, simply

[50] This is like the electronic tokens issued in mobile phone NFC applications such as ApplePay, which do not divulge card details to the retailers terminal, instead a one-time cryptographically secured token is communicated and used by the retailer to redeem the payment online only against the owner of the phone.

[51] See (M Mainelli & Milne 2016) for discussion of the application of the Bitcoin and other blockchains in securities settlement. There other applications being explored by developers include secure voting, registration of non-financial assets such as land and housing; health and social security records and many other applications, (Government Office for Science 2016) discuss these other possibilities.

[52] Wikipedia https://en.wikipedia.org/wiki/Digital_signature provides a concise review.

[53] The same combination of private and public key is used in cryptographic encryption, with the public key obtained from the intended recipient and used to encrypt the message before transmission so it can only be read using the private key.

[54] An important efficiency gain in the Bitcoin protocol

[55] For example each Bitcoin transaction contains a references to the block in which the coins spent were first created. This means that in order to check if a Bitcoin is unspent it is only necessary to search subsequent blocks. Further efficiency is obtained by creating a 'Merkle tree' for each block, a logical hierarchy which allows the location of the creation of transactions in the block to be found in an efficient manner (requiring only a further number identifying the path to be traced through the tree to locate the transaction), see (Narayanan, Bonneau, Felten, Miller, et al. 2016) Chapter 1.

ordering them in temporal sequence would then provide enough information to check that a payment instruction used only unspent Bitcoins as inputs. Because of latency the possibility arises of conflicting payment instructions, using the same unspent Bitcoin as an input. A consensus mechanism is needed to determine which amongst potentially conflicting instructions are confirmed.

The reason the transaction record is referred to as the blockchain in Bitcoin and other cryptocurrency protocols is that consensus works by collecting together a number of transaction records together in a block for validation (this is computationally much more efficient than confirming transactions one by one). The consensus mechanism then results in the publication of a number which can be used by anyone to confirm the validation of the block.[56] Each validated block also contains a pointer to the previously validated block and in this way the confirmed blocks form unique chain that can be traced back to the original (or genesis) block which contains the first allocation of the cryptocurrency.[57]

Consensus is a long standing problem in distributed computer systems, something on which there is an extensive research literature and a number of practical solution methods. Without attempting a comprehensive review, here are some key issues relevant to achieving consensus on the transfers of value on a cryptocurrency network: [58]

- Consensus across a distributed network is a particular challenge if some 'nodes' (network participants) are unreliable, faulty or possibly malicious – seeking to alter the state of the network for their own ends. Amongst researchers in computer science this is called the "Byzantine General's Problem", a reference to a hypothetical situation of a number of generals from a Byzantine army surrounding a city who can only communicate through rounds of bilateral messaging, and who must reach a consensus on whether to attack or retreat, when some of the generals may be traitors and send false messages.[59] A particular concern with cryptocurrency networks is the possibility of a what computer scientists call a 'Sybil attack' – if nodes can be freely opened on the network then a malicious attacker might create a sufficiently large number of new nodes to distort the network decisions to their advantage, for example, if the decisions on consensus depend on majority voting then sufficient new nodes (51% or more) could be used to manipulate the currency.
- Consensus is much less of a problem for a network with reliable trusted participants. There might for example be a small number of recognised 'banks' in a cryptocurrency network who maintain records of customer 'balances'.[60] They are then in a position to directly confirm customer payment instructions, ordering the instructions as they reach them and validating

[56] This key is the 'nonce' described in footnote 29.

[57] (Narayanan, Bonneau, Felten, Miller, et al. 2016) provide greater detail. The pointer is based on another key technical element of the Bitcoin protocol, the use of cryptographic hash function. A hash function converts a 'string' (digital file) of any size into a fixed size output the hash at low computational cost. A cryptographic hash function is one with extremely low probability that two different strings result in the same hash (a so called 'collision') and is impossible to reverse (recover the original string from the hash). Each block of the Bitcoin blockchain includes a hash that 'points' to the previous block in the chain (i.e. is the outcome of applying the cryptographic hash function used in Bitcoin ) thus uniquely ordering transactions (only the previous block is associated with pointer) and making it impossible to alter the block chain after the fact. Hashes are also used to logically organised transactions within blocks.

[58] See (Narayanan, Bonneau, Felten, Felten, et al. 2016) chapter 8 for more detailed review of the range of consensus mechanisms used in cryptocurrencies.

[59] This particular example was highlighted by (Lamport et al. 1982)

[60] These are implied balances since only transactions appear on the immutable record the blockchain.

only when the customer has a sufficient balance for a payment to go through. The digital key validating each payment in the chain of payments (or block of payments in the blockchain) can be uniquely associated with the digital signature of the validating bank. Provided this bank can be trusted then so can the record of transactions. Such trust though has to be based on mechanisms outside of the cryptocurrency system itself – the internal management and external governance of the bank and ultimately the law and regulation governing banking operations.

- A key innovation in the Bitcoin protocol is its application of the consensus mechanism known as 'proof of work', demonstrating its applicability to cryptocurrency transfer in the polar situation when none of the network participants can be trusted. [61] In Bitcoin there is no reliable verification of participant identity outside of the network and hence no external mechanisms are available to discipline behavior. In order to provide incentives for this search the successful validation of new blocks is rewarded either through the allocation of newly created bitcoins and/or through a transaction fees offered by the payers of bitcoin. The Bitcoin proof of work protocol is extremely safe from attack *but* has several costs: high energy consumption;[62] substantial delays in validation which can take thirty minutes to an hour or more; under current protocol design an upper limit on the number of transactions that can be handled by the entire network of around 7 transactions per second; and a concentration of mining capacity in a relatively small number of mining pools that have exploited economies of scale to minimise mining costs.[63]
- In cryptocurrency protocols an alternative consensus mechanism used instead of proof of work is 'proof of stake'. This can be thought of as a voting system, in which the number of votes for determining the next  confirmed set of transaction records are given to all network nodes (or a subset of nodes) in proportion to their holding of the cryptocurrency. Proof of stake avoids the resource costs and delays of proof of work. Many variants are possible. To speed up the establishment of consensus the right to determine the transaction record may be randomly allocated in proportion to stake. Stake may be temporarily surrendered for these confirmation rights with the possibility of loss of stake for identified misbehavior.

[61] (Narayanan, Bonneau, Felten, Felten, et al. 2016) chapter 2 provides further detail. Bitcoin mining is the brute force solution of a particular difficult to solve 'hash puzzle'. This consists of finding a 'nonce' – a 256-bit binary number with the property that a hash of a proposed block of the block chain (containing a set of transactions and the hash of the previous block) together with the nonce appended to the block results in a number less than some pre-specified target. For this purpose Bitcoin employs a particular cryptographic hash function, SHA256, that can be used to verify almost immediately that a nonce satisfies the target for the proposed block but it is very difficult to find such a nonce for SHA-256. There is no alternative to brute force searching over the all $2^{256}$ possible nonces until one is found which satisfies the target inequality for a given block. The target itself is adjusted every 2,016 blocks (roughly every two weeks) so that, given the mining power in the Bitcoin network, a new block is verified by the discovery of a nonce about once every 10 minutes. In late 2015 approximately $5 \times 10^{14}$ hashes per second were being made by miners in attempts to find the nonce for new blocks. By March 2017 this had risen to $35 \times 10^{14}$ hashes per second because of increased mining power (https://blockchain.info/charts/hash-rate?timespan=2years).  In July 2012 the mining rate was only $13 \times 10^{9}$.

[62] As a result the energy consumption involved in validation of every bitcoin payment is approximately $2.00 US per transaction. Far from being low cost bitcoin transactions are actually much more expensive in terms of real resources than conventional bank payments. For discussion and references see (Michael Mainelli & Milne 2016) Appendix 1.

[63] (Narayanan, Bonneau, Felten, Miller, et al. 2016) Figure 5.14 indicates that by April 2015 more than fifty percent of Bitcoin mining power was controlled by only four mining pools: F2Pool (17%); AntPool (16%); BW.COM (13%) and BTCChina Pool (8%). This concentration runs contrary to the original conception that a large proportion of network nodes would engage in mining, as a result dispersing decision making power.

Proof of stake can achieve much lower cost and more rapid validation than proof of work but concerns remain about its security. At present no major cryptocurrency open to free creation of new user nodes uses proof of stake, but the Ethereum network – which currently uses a form of proof of work – is planning to move to a proof stake consensus in the comparatively near future.

- What if there are a subset of nodes that are recognised as generally reliable but not completely trusted (for example there is some possibility of a hacker accessing their systems and then behaving maliciously)? Consensus in the Ripple network is based on this approach, distinguishing participating and validating nodes, the validating nodes are recognised participants with known identities and a track-record of behaving appropriately. Consensus on the Ripple ledger requires a super-majority (60%) of these confirmed nodes agreeing on the next iteration of the ledger.
- There is a possibility of a temporary disagreement, with two different blocks validated (even if they contain the same original payment instructions they will still differ because of the rewards made to miners). This can be solved by deferring final validation until one chain is established as longer than the other, simultaneously removing the shorter 'orphaned' block (or blocks) from the block chain. In the case of Bitcoin this validation is ensured by waiting until say three successive blocks have been validated, ensuring a single record but introducing a total elapsed time of around 30 minutes between payment instruction and validation. Such orphaning is of much less consequence when faster consensus mechanisms than the Bitcoin proof of work is employed.

## The Bitcoin Script language

Cryptocurrency networks require a computer programming language, governing the syntax of payment instructions and ensuring that the subsequent processing is carried out rapidly and efficiently on the crytpocurrency network. In the case of Bitcoin this language is the Bitcoin scripting language, Script for short, a simple language with a limited set of instructions designed to support highly efficient execution of cryptographic algorithms.[64] While full technical detail is only needed if you are coder working on Bitcoin applications, it is helpful to know something of this language in order to better appreciate the operation of Bitcoin and other cryptocurrencies and their monetary implications.

Script has a number of features that support the privacy of network participants – not perhaps necessary for secure cryptocurrency transactions but consistent with the spirit of the cypherpunk community from which Bitcoin emerged, seeking to achieve as much protection as possible for the actions of individuals from the scrutiny of outsiders.

A feature of Bitcoin is that most payment instructions do *not* send Bitcoins directly to a public cryptographic key that serves as an address on the network. While this was possible in the first version of Bitcoin the standard instruction is a so called 'pay to pubkey hash', in which the instruction uses masked (or hashed) version of the public key rather than the public key itself as the destination address, and the recipient must then use their public key using a further instruction

[64] (Narayanan, Bonneau, Felten, Miller, et al. 2016) Chapter 3.1 provides an accessible introduction to this language. For those who want to get into all the detail https://bitcoin.org/en/developer-guide is a standard source. Note one limitation of Script often mentioned: unlike standard programming languages such as C$^{++}$ it does not support looping and so not all potential algorithms can be programmed using Script (in the technical jargon it is not 'Turing complete'). A principal motivation for the creation of Ethereum was to offer a language for supporting shared immutable transaction records that is Turing complete and could thus be used for any conceivable algorithmic application.

called ‘script Sig’ to redeem the transaction (a digital signature that confirms that the recipient owns the public key). Why is this roundabout method preferred rather than sending directly using the public key as an address? One reason is security – it offers some protection against the possibility that e.g. through advances is quantum computing someone breaks the elliptic curve cryptographic function that protects the private keys used to send bitcoin instructions, i.e. anyone could work out private keys from public keys. Another reason is privacy, the hash of the public key is unique to the transaction so payments made in this fashion are difficult to associate with particular users.

Another feature of Bitcoin is that when coins are only partly ‘spent’, with a proportion of the coins value sent back to the initiator of the transaction (such as the example of Alice taking 0.3 BTC, sending 0.1BTC to Bob and getting back 0.2BTC herself), then the coin is typically returned to a ‘change address’ a public key which *differs* from the address used to initiate the transaction. The reasons why this is preferred over the (simpler) approach of always using the same public key is again greater security and greater privacy.

As well as paying to a (masked) public key another common payments instruction is ‘pay to script’ – allowing the recipient to undertake their own additional processing when redeeming the Bitcoin (to give one example of many, it may be that a number of many possible recipients are to be required to sign for receipt). The recipient does not need to reveal this script, they just need to send a masked version of the script they want to be used (just like a public key can be masked) and they can then use their public key to redeem the Bitcoin sent to them.

This short discussion should make clear some of the huge range of possibilities for implementing a cryptocurrency network. This in turn means there is a need for a process for effectively maintaining and updating the underlying code in response to user needs and network growth i.e. arrangements for governance of the network.

## Transparency and identity

As already discussed, almost all cryptocurrencies, including Bitcoin itself, are open source and unpermissioned: anyone can download the software and join the network. Such networks are in one respect extraordinarily transparent. Every transaction is immutably recorded on the cryptocurrency blockchain and can be viewed by all network participants, in effect by anyone anywhere. In the case of Bitcoin this means there is an extraordinary amount of transactions data in the public domain and a number of Bitcoin sites that collect and communicate information on the currency and its trading.[65]

This transparency is however limited because it is difficult to work out the real-world identity of participants in any network that is ‘unpermissioned’ – that is without any gatekeeper who checks the identity of persons seeking to join the network and possibly also deciding who can participate and who cannot. This means that the identity of network of participants is at best ‘pseudonymous’ – transacting using an identifier that works only in the context of the network itself not elsewhere e.g. a public key for their network node. Identity in cryptocurrency networks can also be more hidden even than this – for example if public keys are masked as is now common practice in Bitcoin.

Real world identity can sometimes be worked out from the record of transactions in an open-source unpermissioned cryptocurrency network but this depends on the details of the supporting code, as determined by the design of the initial developers along with any updates of coding subsequently

[65] An informative exercise – this a good way to introduce students to cryptocurrencies – is to look at Bitcoin transactions live as they take place e.g. at https://blockchain.info/unconfirmed-transactions . By clicking through on the ‘addresses’ it is possible to see the detail of individual transactions.

agreed upon and adopted by the cryptocurrency community. The use of 'masked' public keys makes it very difficult to use the immutable transaction record of Bitcoin to associated transactions with real world identities.

## Unpermissioned v. permissioned and cryptocurrency governance.

Most cryptocurrencies are 'unpermissioned' with no central authority determining who can join the network. This is a central part of the philosophy espoused by the wave of innovative technologists who pioneered Bitcoin and other subsequent cryptocurrency networks. This choice reflects opposition to central authority and commercial institutions, seeking instead to achieve all the security and trust required by an open source community through cryptographic tools alone.

It is though possible for a cryptocurrency to be 'permissioned' rather than 'unpermissioned' with some authority having the role of gatekeeper determining who may and who may not join the network. They can then insist on the participants revealing their real world identity. One example is Ripple, the cryptocurrency designed for use in international payment transactions.[66] Another proposed use of cryptocurrency technologies, the utility settlement coin developed by UBS and Clearmatics for wholesale transactions in central bank money will also be permissioned (although not a cryptocurrency, it will be fully backed by central bank money).[67] Tibado is another digital currency initiative which like the utility settlement coin will be backed one-for-one by central bank money, but designed to support virtual payments for households and companies outside of the banking system .[68]

It is unsurprising that these initiatives have chosen to be permissioned. This is because they are designed to be used by or complement the payments services of financial institutions who are subject to demanding 'Know your customer' KYC and 'anti-money laundering' AML regulations. Banks cannot realistically use or engage with a service in which network participants do not have real world identities. A digital payment service that successfully competes with bank payments will have to also support compliance with KYC and ALM regulations.

This choice between being unpermissioned and permissioned is closely connected to the challenge of governance in cryptocurrency networks. As a result of changing circumstances and technology, what may have been an appropriate consensus mechanism or transaction instruction at one point of time may well no longer be so appropriate at a later date. This means that no cryptocurrency can avoid the need for governance – an orderly process for maintaining and updating the computer coding supporting the network (something which will be required in any case because of the inevitable presence of bugs and security vulnerabilities). Governance operates very differently in unpermissioned and permissioned networks. Arguably – although we do not yet have sufficient experience to reach a definitive judgement – it may well turn out that permissioned networks are better able to alter and adapt in the face of changing circumstances.

For cryptocurrencies following the strict philosophy of full decentralisation with open unpermissioned participation, governance is a debate amongst the community of users, core developers, miners (when consensus is based on 'proof of work') and service providers. Members of the community can express a need for an change to the coding, core developers (often unpaid,

[66] Ripple is unusual in that the software remains open-source – anyone can download and acquire the supporting cryptocurrency – but a permissioned system controls bank access, transaction validation and governance and development.

[67] An August 2016 press release announced that BNY Mellon, Deutsche Bank, ICAP and Santander were joining UBS and Clearmatics in the next phase of development, see the description and links in (Lehmann 2016).

[68] See http://www.tibado.com/about-tibado .

Bitcoin apparently has only two full time contributors) can introduce and encourage downloading of new code, set up so that it activates only when a sufficient proportion of the community begin using it.[69] The rules for activation can vary – this is something determined by the existing core code – but activation must require that a clear majority of the mining capacity adopts the new code, otherwise there is insufficient commitment to ensure that a unique ('unforked') block chain for the cryptocurrency continues forward using the new code.

Such open-source governance – while democratic – does not easily support change. The difficulty of effecting major change in the underlying code is emerging as a particular challenge for the Bitcoin network now that transaction volume has grown to the point where it is limited by capacity constraints. Overcoming this so called 'scaling problem' to allow further growth in transactions requires a major change in the underlying code. The problem first emerged in 2015, but the appropriate response remains highly contentious more than 18 months later.

One proposal which is being supported by some of the major mining pools is that the Bitcoin Core code should be entirely replaced by a revised coding 'Bitcoin Unlimited', an implementation in which the scaling problem is addressed by allowing the blocksize (currently limited to a maximum of 1MB) to be reset to higher magnitudes provided there is sufficient support.[70] This though is fiercely resisted by others in the Bitcoin community who fear a possible permanent 'hard fork' (a division into two competing cryptocurrencies, such as occurred with Ethereum – see discussion and box below), are worried about a small number of mining pools having excessive power in determining the future of the network and so prefer that the scaling problem is addressed by other means.

An alternative proposal supported by some is amending Bitcoin coding so it supports 'SegWit' or Segregation Witness. This allows the Bitcoin capacity to be increased by 40% by moving cryptographic information supporting the digital signature of coins off the block-chain (these can be checked at the time of block validation but once validated there is not need for these to be maintained permanently on the blockchain). SetWit is already supported on some altcoins such as Litecoin. It will however be only a temporary solution to the Bitcoin scaling problem.[71]

This is unlikely to be the last major governance challenge for Bitcoin. At present mining is highly profitable and the Bitcoin reward for successful mining of Bitcoin blocks is more than sufficient to cover the electricity, hardware and other costs of the leading mining pools. The Bitcoin protocol has though been explicitly designed with a built in limit on the total maximum value of Bitcoin of 21 million BTC. The reward for Bitcoin mining through newly created Bitcoin is coded to gradually

[69] (Narayanan, Bonneau, Felten, Miller, et al. 2016) Chapter 7 contains a fuller description of Bitcoin governance. As they emphasise, Bitcoin follows much the same process as other open source computer coding projects, the code itself Bitcoin Core is freely available, changes can be proposed, and are implemented on a consensus basis by a small team of core developers, with more complicated changes that need fuller discussion appear as BIPs (discussion documents) on the github website https://github.com/bitcoin/bips .

[70] See (Hertig 2017) for a briefing on the issues involved. Bitcoin Unlimited implements an idea known as 'emergent consensus' in which a number of parameters in the code – including blocksize – will adjust when a sufficient number of network participants register support for a change. But this alternative code, while supported by some major minors, has been less successful in attracting the support of the exchanges and wallets that provide services for holders of Bitcoin. The often acrimonious debate can be followed via http://www.coindesk.com/tag/scaling/.

[71] At the time of writing approximately 35% of mined blocks 'support' Bitcoin unlimited and 30% support Segwit. Neither proposal is yet coming close to the level of support required for adoption. See https://blockchain.info/charts/bitcoin-unlimited-share and https://blockchain.info/charts/bip-9-segwit .

reduce down to zero as this limit is approached.[72] This does not mean an end of mining revenues, but Bitcoin miners will then have to rely on transaction fees voluntarily included in payment instructions by the senders of Bitcoin in order to persuade miners to give their particular payment preference in a mining block. It is unclear how well this incentive mechanism will work as the reward for miners from awarding them newly created Bitcoins are reduced. It is therefore very possible that Bitcoin will have to rethink the system of transaction fees at some point in the future to ensure that active mining continues and does not require excessively large fees, especially for smaller payments.

Ripple – because it uses permissioning for bank participation and validation – has been able to adopt a different governance model from other cryptocurrencies, one of mutual governance with a more formal management structure and arrangements to allow representatives of users, the banks who are adopting Ripple in their international payments activities, to be involved in major strategic decisions. A key step was the announcement in Sept of 2016 of their Global Payment Steering Group (Treacher 2016). It is no co-incidence that this announcement was made at the annual SIBOS conference, the major event organised by SWIFT the international payments provider and their 10,000 plus participating banks. SWIFT itself has a governance structure not unlike that being developed by Ripple, with mutual ownership by the banks who use the SWIFT network for transaction messaging.[73] Ripple is developing a governance framework that will be recognisable to its banks users and that they can trust to help develop Ripple to better serve their interests.

This contrast between the structured governance and flat but hierarchical management of Ripple, made possible by permissioning, and the commitment to minimal management structure and completely decentralised governance of the other cryptocurrencies consequent on being an unpermissioned network, may turn out to be a defining divide in the future evolution of cryptocurrencies.[74] A key and still open question is whether and to what extent a fully decentralised governance and unpermissioned membership limits cryptocurrency adoption and use.

The choice between ‘unpermissioned’ and ‘permissioned’ is being further accentuated by the growing business and policy interest in cryptocurrencies the decentralised transaction records (blockchains) that support them. Established businesses find it difficult to deal directly with unpermissioned cryptocurrency networks – if they do accept these payments they must exchange them relatively quickly for conventional currency. Where they are interested in the business application of blockchain this is most often because of the attractions of shared, immutable record, accessed by business partners, not because of the use of blockchain in cryptocurrency tranfers.[75] The most recent developments in blockchain technology – such as the work of the ‘hyperledger project’ or the efforts to develop standards for distributed ledgers led by the Australian Standards Organisation on behalf of the International Standards Organisation, while still supporting open-source coding, will not have any particular philosophical attachment to being unpermissioned.

[72] More precisely the reward for adding a block, which is currently 25BTC, will be halved every 210,000 blocks (approximately every four years). Eventually, the reward will decrease to zero, and the limit of 21 million bitcoin will be reached by about 2140. This detail can be found in many sources including Wikipedia.

[73] See (Scott & Zachariadis 2013) for a history of SWIFT from its origins in the 1960s with an extensive discussion of its governance arrangements.

[74] This is not to say that only one unique governance arrangements is possible in a fully decentralised network or that effective governance is impossible. The example of Dash, described earlier in this section, illustrates one possible variant of decentralised governance that may well, in the long run, prove more effective than that of Bitcoin, amongst other reasons because their revenue model supports some salaried permanent staff.

[75] A prominent example is Eris industries, now rebranded as Monax, which is developing applications of blockchain for business use without any cryptocurrency, see https://monax.io/ .

In the future we may see central banks sponsor permissioned blockchains that allow their own currencies to be used immediately online without the need for a credit card system such as Visa or Mastercard or a bank intermediary.[76] While such a development will not directly compete with cryptocurrencies (the threat to existing business models in bank payments is more immediate; since these will be national not international payment instruments) such central bank sponsored cryptocurrencies will certainly be permissioned, not unpermissioned, and will undermine one of the central use cases of unpermissioned cryptocurrencies, that of providing the internet equivalent of notes and coin.

Despite the success of Bitcoin and Ethereum, the idea that cryptocurrencies will help us develop a libertarian world which has no more need for banks and a much reduced role for governments has as yet little support outside of the active communities of cryptocurrency users.  For many commentators (although possibly biased by lack of understanding of how cryptocurrencies actually function) the future of internet payments is quite different from this utopian vision. It will based on permissioned not unpermissioned networks and with financial intermediaries and government continuing to play a major role, however much of a heresy that may seem to the cryptocurrency pioneers and their followers.

## Forking

Open source changes in a cryptocurrency protocol can result in what is known as a 'fork' (simultaneous use of two versions of the blockchain and supporting code). These can be a serious concern if they are permanent divisions, best referred to as consensus forks to distinguish from temporary creation of orphan blocks in the blockchain already described, something that arises naturally during the process of establishing consensus. Two possibilities can be distinguished: a hard and a soft consensus fork.[77] A hard consensus fork occurs when there is majority but less than complete adoption of new code that is backwards incompatible, introducing new rules (for example on blocksize). This means that blocks are validated that would not have been accepted by the earlier version.

The consequence of a hard consensus fork is two parallel implementations of the currency, miners using the old protocol continuing to add new blocks using the old code and miners using the new protocol adding different chain of blocks using the new code. There are then effectively two currencies with two parallel records of transactions, identical up to the time of the hard fork, differing thereafter, and with holders of currency at the time of the fork becoming holders of both.

A soft consensus fork occurs with majority but less than complete adoption of a new code that prevents blocks being validated which were previously acceptable. A minority of miners of the cryptocurrency may continue to use the old code, but they will be unable to validate, so there is still a single permanent record of transactions even though two versions of the code are being used in parallel.[78]

Hard consensus forking – the much more serious situation – can be anticipated and steps take to avoid it. It may though also arise as a result of an entirely unanticipated software error. This has in fact happened once to Bitcoin, on March 12, 2013 at the time of a supposedly routine upgrade of

[76] i.e. 'FedCoin', as discussed by several observers of cryptocurrencies (e.g. Konig 2014; Andolfatto 2015).

[77] (Smith & Atlas 2016) provides a useful discussion of forking, distinguishing the different types of fork and their occurrence in Bitcoin.

[78] To confuse matters, the term 'hard fork' is also used to refer to any backwards incompatible change in coding – whether fully accepted or rejected by the community – but this is not a hard *consensus* fork since it does not result in two versions of the code being used simultaneously.

the software (to Bitcoin Core 0.8.0).[79] While a majority of miners had adopted 0.8.0 some 0.7.0 Bitcoin nodes unexpectedly rejected blocks validated by the new software, and since about 60% of mining power was on the new code the forking did not automatically correct. The response to the fork was a relatively quick decision, supported even by the miners who had recently earned soon to be valueless Bitcoin from version 0.8.0, to unwind the 0.8.0 transactions and revert to the 0.7.0 software, upgrading to 0.8.1 after the bug was fixed.[80]

A critical event in the history of cryptocurrencies was the hard forking of Ethereum in the summer of 2016 (see box). These events in June and July of that year illustrate a number of concerns about the practical application and security of cryptocurrencies. They also reveal how effective open-source governance depends, critically, on consensus amongst active participants in the cryptocurrency network. In this particular case failure to achieve consensus led to an irretrievable split and has heightened concern that a similar hard forked split could happen to Bitcoin if the solution to the scalability or other problems are not handled well.

## Exchanges, wallets and regulation

This short outline of the key characteristics of cryptocurrencies can be completed with a discussion of those intermediaries providing services to cryptocurrency holders. Some cryptocurrency evangelists envisage a future where cryptocurrency such as Bitcoin residing both outside of government control and independently of conventional banks and other financial institutions becomes the dominant or at least an important means of exchange, as or more important than conventional fiat currencies. One of the biggest appeals of an unpermissioned cryptocurrency is that it is a people's currency, anyone can participate by downloading the latest version of the open-source code. To receive money just give the sender your public key (the key itself or a masked version). To send money create a payment instruction in the software using both your private key, stored securely on your computer or smartphone, and the public key of the recipient. Financial intermediaries have no power with this monetary arrangement.

The reality is that for the forseeable future the development and growth of cryptocurrencies depend on the activities of financial intermediaries, exchanges – who allow the buying and selling of cryptocurrencies using conventional government backed currencies or other cryptocurrencies– and 'wallet providers' assisting users with acquiring, securing and using cryptocurrencies.

In order to use a cryptocurrency as a store of value or as a means of exchange it has to be possible to exchange it for conventional currencies or other cryptocurrencies. This can be done bilaterally as a private arrangement between network members known to each other. Purchase and sale is also done on exchanges. Table 2 shows the ten leading cryptocurrency exchanges, globally, as reported by cryptocoincharts. Some of these --- such as Poloniex, Bittrex and YoBit – offer a wide range of direct exchanges between different cryptocurrencies (hence the large number of currency pairs they support). Other offer only exchange from major cryptocurrencies into conventional currency, the extreme example being Bitstamp which only offers trades in BTC/ USD and BTC / EUR.

[79] This paragraph draws on (Shubber 2014).

[80] This is one of two cases where the supposedly 'immutable' history of Bitcoin transactions has in fact been rewritten. The other was on 8th August , 2010 when an 'underflow error' (mathematical miscalculation) led to the creation of 92 billion bitcoins in a new block, far exceeding the intended maximum level of 21 million!

### Box 2: the Ethereum hard fork.

Governance challenges have emerged in a number of cryptocurrency network. The most serious was the 'hard consensus fork' of Ethereum in July 2016, resulting in two separate cryptocrurrencies. Ethereum itself is *not* primarily a cryptocurrency, rather – as described on their website https://www.ethereum.org/ – it is a decentralised platform for 'applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference', i.e. what are referred to as smart contracts. Proposed applications include creating markets, registering debts or promises, move funds or ownership in accordance with prior instructions (like a will or a futures contract) without involving any other parties or counterparty risk. The Ethereum platform provides its own cryptocurrency (Ether) that may be transferred by its applications, though at least in principal any currency could be transferred on Ethereum if linked appropriately into Ethereum coding.

Ethereum hosted an investment project known as The Dao Hub, which we set up as a mechanism for crowdfunding without involvement of any financial intermediaries. It was instead a so called 'digitally autonomous organisation' i.e. an organisation operating purely as a computer code without any directors or management structure (see its website https://forum.daohub.org/ and https://en.wikipedia.org/wiki/The_DAO_(organization) for detail on the The Dao Hub ).

In May 2016 the Dao Hub raised over $100mn from more than 11,000 investors (including $34mn in real world dollars) – itself the world's largest ever crowdfunding. After conversion of dollar subscriptions it held some 14% of all outstanding Ether. The concept was that investors who joined the hub and held DAO tokens (originally purchased for a fixed number of Ethereum Ether) would vote on proposed investment opportunities, with the execution of these projects in the real world handled by so called 'Dao Contractors', who would both submit projects to be considered for funding and then be responsible for ensuring that these projects fulfilled their obligations as contained in the smart contract code.

Regrettably an unknown hacker exploited security vulnerabilities in the Dao coding on June 17th to transfer 3.6 million Ether, then worth around $50mn and about a third of the 11.5 million Ether held by the Dao, to a separate Ethereum account. The smart contract coding in the Dao however prevented further onward transfer of the Ether for a limited period. The community – the holders of Ether -- had until July 27th to decide how to deal with the hacking – but was split on the appropriate response. After much discussion the lead developers agreed on a proposal to unwind the transaction and restore the Ether to the original investors in the Dao. A minority however took the view that the cryptocurrency coding – even if insecure -- was inviolate, that a record of cryptocurrency ownership should in principle be immutable and therefore could not accept the change in code. The unwinding required the release of a new version of the Ethereum code but . As a result there was a split in the currency, with two incompatible versions of Ethereum and the code that supported it: the new official Ethereum, in which the coins were restored to their rightful owners; and the original coding which continued under the name Ethereum Classic. Ethereum keys usable at the time of the split now gave access to cryptocurrency on two accounts, those on the official Ethereum Ether and those on the unofficial but orginal Ethereum Classic. Ironically – contrary to what might have been predicted by a quantity theory of money -- this doubling of the supply of cryptocurrency did not result in a 50% fall in its market value. At the time of the slit Ether and Ether classic fell in value by only around 20%. The consequence of the split was to increase the aggregate market value of the two cryptocurrencies by around 60%!

Most of these exchanges run a transparent limit order book very similar to that used in most venues for equity trading. Participants can either place a limit order – an offer to buy or sell at a stated price which is added to the book for all to see – or a market order accepting an offer to buy or sell visible on the order book. The exchange then levies a small percentage fee to cover its own costs. In some cases the order book can viewed even if you are not an exchange customers.

**Table 2: the 10 leading cryptocurrencies exchanges as of March 24th, 2017**

| Rank | Name & source link | Headquarters | Number of pairs | 24 hour volume | |
|---|---|---|---|---|---|
| | | | | BTC | Percent |
| 1 | Poloniex | US | 363 | 30,005 | 17.3% |
| 2 | Bitfinex | Hong Kong | 24 | 29,501 | 17.1% |
| 3 | Kraken | US | 57 | 28,403 | 16.4% |
| 4 | Quoine | Japan/ Singapore | 29 | 22,779 | 13.2% |
| 5 | Bittrex | US | 836 | 9,165 | 5.3% |
| 6 | BTC38 | China | 72 | 8,394 | 4.9% |
| 7 | BTC-e | Bulgaria | 26 | 8,360 | 4.8% |
| 8 | Coinspot | Australia | 11 | 6,504 | 3.8% |
| 9 | Bitstamp | Luxembourg | 2 | 6,148 | 3.6% |
| 10 | YoBit | Russia | 784 | 6,101 | 3.5% |
| | Total (leading 10 exchanges) | | | 155,365 | 89.8% |
| | All 31 exchanges with monitored activity | | | 172,982 | 100.00% |

Source: Cryptocoincharts website https://www.cryptocoincharts.info/markets/info and author's calculation. The website lists a further 11 exchanges with no transactions in the past 24 hours. Comparison with the Bitcoininfo estimate of the total value of Bitcoin transfers on the same day (416,515 from https://blockchain.info/stats ) suggests that the 31 exchanges on which Cryptocoincharts monitored activity on this day account for a substantial share, but less than one half, of all global cryptocurrency transactions.

While the order books are transparent, exchanges require deposits of customer funds, both conventional currencies and cryptocurrencies, before customers can trade. This means that – unlike when holding cryptocurrencies directly there is risk of loss (though exchanges are subject to the regulations that require separation of client funds, so in principle even if an exchange failed, customer funds should be returned.) Exchanges are also subject to the usual KYC and AML transactions which apply to cryptocurrency transactions as much as to any other financial transactions, limiting to some degree the extent to which cryptocurrency transaction can avoid regulatory attention (though it is still possible to buy and sell cryptocurrency privately outside of an exchange without being subject to these regulations).

Many cryptocurrency users prefer to use a service provider – a wallet – to manage their cryptocurrency holdings and transactions on their behalf. This is because, while cryptocurrencies are completely open source and can be used by anyone downloading the protocol, executing and managing transactions can be inconvenient and places with the user all responsibility for security (for example ensuring their private keys to the network are not lost or stolen). It can also 0be demanding on computer resources. Installing the Bitcoin protocol Bitcoin core onto your own computer means downloading the entire Bitcoin blockchain, currently approaching 110GB in size.

A large number of Bitcoin and other cryptocurrency wallet services that can be found and compared online. These offer a variety of services and come in many different forms. Some are software installed on desktop computers. Others can be installed on smartphones. Some wallets are web based. Unlike installed wallets these require the user to upload a lot more information, including their private keys, but they are popular because they allow Bitcoin to be used from any internet enable device. There are also offline wallets. Hardware wallets are separated security devices that protect a software wallet taking over the management of private key generation, private key storage, and transaction signing. There are even paper wallets using QR codes for holding the private keys needed for cryptocurrency transactions, though these are bearer instruments, giving full control over the bitcoin they hold to whoever possesses them. Wallet services include keeping track of Bitcoin balances, holding the private keys required for sending Bitcoin, and maintaining user privacy by ensuring that different public keys are used for each and every transaction. Some are orientated towards personal users, others to traders and merchants. Services, such as the scanning of QR codes as a way of inputting a Bitcoin address for payment, are provided by wallets not by Bitcoin core.

To complete this section, it is worth briefly mentioning some of the issues that arise with the regulation of cryptocurrencies. Direct regulation of unpermissioned open source cryptocurrency is difficult. Anyone can freely join the network, there is no central authority that can be directly regulated or instructed, and changes to the supporting code cannot be mandatory since they need to be accepted by the community of users. Regulation of the individual users could be possible, for example cryptocurrency transactions could be made illegal,  subjected to tax, or limited by for example transaction size or destination, but enforcement then relies on the difficult task of tracking the activities of individuals online (it may be able to detect IP addresses connecting to cryptocurrency networks but users could still hide IP addresses using anonymous networks and also the messaging to and from the cryptocurrency network can be encrypted and thus hidden from regulatory oversight). Realistically, therefore, practical regulation of open source cryptocurrency networks will have to be focused on the exchanges and wallets servicing their users.

This is not to say that direct regulation is impossible. Ultimately – if cryptocurrencies come to be perceived as a pressing and severe threat to the established social and economic order – there could be political will for imposing sufficiently substantial penalties on individuals involved in cryptocurrency networks as users, developers or service providers to greatly reduce involvement and undermine the cryptocurrency networks. This though would require legislation, be highly confrontational and quite unnecessary in most jurisdictions where concerns about misuse (such as their potential use by terrorists or in illegal economic exchange) can be more effectively addressed in other ways. Effort to prevent participation in cryptocurrency networks are much more possible by authoritarian regimes seeking to prevent the use of open-source cryptocurrency networks to undermine their own authority, for example for evading controls on foreign exchange transactions.

It appears that cryptocurrency technologies will become increasingly embedded in conventional business processes, in both financial and non-financial industries. This though will likely be based on permissioned rather than unpermissioned networks, making direct regulation possible. Here the bigger challenges are around the consistency of regulation, ensuring that established and innovative business are treated in broadly similar ways that does not unduly advantage one or the other and still achieves regulatory objectives – such as consumer protection, financial stability and promoting competition and efficiency of economic exchange.

# Appendix B. A summary of Austrian views on monetary arrangements

This appendix provides a brief summary of Austrian views on monetary arrangements, for those unfamiliar with Austrian school literature. The paper can be read without reference to this Appendix, but it may help clarify some of the discussion of Austrian positions on monetary policy in the main text.

The objectives of Austrian proposals for monetary reform are far from peculiar to their school of thinking. They are shared by very many participants in mainstream economic policy debate and include: limiting political interference that leads to rapid increase of the money supply for short term objectives; reducing state protection for banks whether through deposit insurance, central bank liquidity support or 'bail out' of banks because these protections encourage risk-taking and poor risk-management; limiting or at least discouraging the creation of 'fiduciary media', in particular bank deposits created to fund bank lending, to prevent unsustainable private sector expansion of money and credit.

What differentiates Austrian economists is their particular approach to achieving these objectives: using an underlying medium of exchange whose total stock is in strictly limited supply and so cannot be increased by political instruction (often arguing that this is best achieved by restoration of a commodity based monetary standard such as gold);[81] and seeking to ensure that banks and bank shareholders are never protected from loss by receiving government support, even in times of crisis. They are also fierce critics of the Keynsian policy proposals to use fiscal policy to counter the buseness cycle, which they see as an entirely monetary phenomena (according to the Austrian theory of the business cycle) and therefore should be addressed through their proposals for monetary arrangements.

These proposals – while they would have been regarded as rather conventional a century ago – have come to be seen as unrealistic and hence well outside of the mainstream of economic policy debate. A system of fixed exchange rates pegged to gold was restored twice after the breakdown of the classical gold-standard in 1914 and each time it broke down. Mainstream discussion believes that in a severe financial crisis there no realistic alternative to saving banks in order to prevent a breakdown of monetary exchange. Hence the only realistic policy is measures such as regulatory oversight of banks and imposition of capital requirements which seek to ensure that banks never get into such difficulties as to trigger a financial crisis in the first place. The mainstream consensus is that fiscal policy should be used to counter cyclical fluctuation, at least in the short-run before structural measures that address problems of unemployment and long term deficits have time to operate.

Austrian proposals for monetary arrangements have always foundered on one central problem, they have never been able to find a practical laissez-faire way of dealing with the potential of loss of confidence and withdrawal of bank deposits arising because from maturity mismatch and fractional reserve banking. A purely metallic gold standard – one without fractionally reserved banking – Is conceivable and would not have this drawback, but would also require a highly interventionist regulatory framework to prevent

[81] The medium of exchange – to use the Austrian terminology – is broadly the same as what money and banking textbooks refer to as high-powered or outside or base money. The terminological difference arises from the Austrian view of how commodity such as gold or silver first emerges as a commonly accepted money used in exchange, without the intervention of any government agency. They prefer not avoid terms such as outside or base money because money is something that arises through human choice within and not outside of the economic system.

## Overview of Austrian economics

The Austrian school of economics, originating with the work of Carl Menger, Friedrich von Wieser and Eugen von Bohm-Bawerk and developed by successive generations of thinkers, including Ludwig Von Mises and Friedrich Hayek, supports many views that are also identified with more mainstream neo-classical economics.[82] It emphasises the necessity of building economic analysis on a foundation of individual choices and actions and the key role of prices in carrying information about marginal costs and marginal benefits. Austrian analysis also highlights the effectiveness of the free market in the allocation of resources and is correspondingly critical of government intervention in the economy.  In contrast to much of neoclassical economics however, Austrian analysis tends to avoid formal mathematical model building and the resulting focus that often then emerges on static economic equilibrium. It emphasises instead the dynamic process of adjustment of production, consumption, investment and market prices in response to individual perceptions of value and the central role of profit seeking entrepreneurs in acquisition of knowledge and overcoming the fundamental uncertainty of economic exchange.

A characteristic feature of the Austrian economics tradition is its close attention to the, necessarily subjective, role of human choice and human action in the economic sphere. In contrast to the rather bloodless approach of modern formal economics research – with its highly abstracted models and focus on mathematically tractable utility and production functions – the Austrian tradition stresses that economics is a study of individuals and their social interaction, just like other social sciences. It must therefore be based on careful study and understanding of individual motivation. Psychological, social and political influences are a central part of the scope of economic analysis, not a peripheral consideration. Contributions to economic understanding come from detailed examination of both historical experience and institutional arrangements, using precise logical argument, not as in the physical sciences the statistical testing of theoretical models.[83]

Murray Rothbard's collection of writings on the history of money and banking in the United States exemplify this approach (Rothbard 2002). He places the political battles over monetary and banking arrangements at centre stage, in deliberate contrast to other histories for example the more technical discussion and statistical focus on growth of monetary aggregates of (Friedman & Schwartz 1963). Even for readers who do not share his hostility to central banking and the creation of the Federal Reserve, Rothbard offers a wealth of insight into the perceptions and motives of those who participated in the major debates and decisions that shaped US monetary arrangements.

The Austrian school is also associated with a fundamentally different account of the business cycle than that offered by Keynsian macroeconomics both in terms of the analysis of the mechanisms of economic boom and bust and in its policy prescriptions. In (Von Mises 1953, first ed 1912) the underlying mechanism of the business cycle is based on Wicksell's distinction between the money rate of interest and the natural rate of interest in (Wicksell 1898). The money rate of interest is the interest rate when borrowing money markets. The natural rate of interest – while not susceptible to direct measurement – is the rate of interest which arises from the natural tendency of the market for borrowing and lending to find a balance between the required return on current saving (the

[82] (Boettke & Leeson 2003) provide useful history and overview, though a proper understanding requires some study of at least of the original contributions, in their original language or translation, especially those of Von Mises and Hayek.

[83] This method is referred to as 'praxeology' – a term preferred by Austrian economics from Von Mises in what many Austrian economists regard as his most important work (Von Mises 1949). Von Mises supposes that from this study it is possible to deduce universal laws of human action that are 'logically anterior' and hence can be used to understand individual historical situations.

additional future consumption desired from consumption postponed to the future) and the additional output from investing this saving (the additional future production of goods resulting from the additional resources devoted to capital investment). When the money rate of interest is kept below the natural rate of interest for an extended period then the outcome is unsustainably high borrowing and investment, with capital investment that does not ultimately prove sufficiently profitable when output is brought to market.

The principal responsibility for preventing or at least containing unsustainable economic expansions therefore lies with monetary policy and ensuring an appropriate level for the market rate of interest, not with fiscal policy. (Hayek 1932; Hayek 1933) develops this explanation of the business cycle further, exploring its impact on the structure of production and arguing that attempts of policy makers and preventing the deflation in the downward phase of the trade-cycle and avoid the necessary adjustment of production back to that supported by the natural rate of interest only serve to prolong the downturn.

This does not mean that Austrian economics offers only a single dogmatic viewpoint. Throughout its development the Austrian school has been characterised by lively, often fierce debate, both with mainstream economists and amongst those identified with the Austrian school. The views associated with the Austrian school have also evolved over time.  This is nowhere truer than in the analysis of money and monetary policy.

## Austrian views on money and credit

(Menger 1892) argued that money emerged naturally as commonly accepted medium in order to facilitate economic exchange (i.e. overcoming what textbooks refer to as the 'absence of double coincidence of wants' limiting the possibilities of direct exchange by barter) without the need for government intervention and moreover naturally took the form of previous metal because of its 'greater saleability'. While Menger admitted a role for the state in improving on commodity money, e.g. through standardisation of coins,  (Von Mises 1953) argued even more strongly that money was whatever was commonly accepted as the medium of exchange regardless of state action. He strongly rebutted the view of (Knapp 1924, first published 1905) that money was a legal construct supported by the state. Von Mises for example argued that the status of 'legal tender' did not make something money, it was money only if it was commonly accepted in exchange for goods.

Two analytical distinctions made by (Von Mises 1953) are of particular importance to subsequent Austrian monetary proposals. He draws a distinction between the medium of exchange itself and other fiduciary media which, while they can be immediately and reliably redeemed at par or stated value medium of exchange (and because of this are also accepted in payment), are not themselves money.[84] Bank notes and bank payment deposits are examples of such fiduciary media.

Von Mises also distinguishes three forms of monetary standard, depending on the form taken by the commonly accepted medium of exchange. One possibility is a commodity standard, where the accepted medium of exchange is a physical commodity such as gold. A second possibility is a fiat standard where the accepted medium of exchange is something declared by the state. A third possibility is a credit standard where the medium of exchange is a financial claim falling due in the future.[85]

[84] The 1934 Batson English translation of the Theory of Money and Credit uses the term 'money substitutes' rather than 'fiduciary media' but the latter seems to better communicate the trust placed on the issuer.

[85] Von Mises argues that, while there are historical examples of both commodity standards and credit standards, a fiat monetary standard may never have existed "It can hardly be contested that fiat money in the

These basic categorisations support key Austrian prescriptions on monetary policy which are the focus of this paper and which will now be elaborated on in turn:

(a) an independent monetary standard (the widely accepted medium of exchange) whose supply – in contrast to current fiat monetary standards – is not controlled by the state (the classical gold standard is one possibility, a cryptocurrency may be another);
(b) limits on the production of fiduciary media (financial claims such as fractionally reserved bank deposits that can be readily exchange for and accepted in payment instead of the medium of exchange); and
(c) 'free banking' with no central bank and with market discipline limiting the production of the fiduciary media.

## The Austrian case for restoration of the gold standard

Von Mises uses the distinction between commodity, fiat and credit standards as the basis for arguing the superiority of monetary arrangements based on gold. His arguments were revised and developed in the three successive editions of his Theory of Money and Credit and in his other writings but this remained a central and consistent element of his monetary economics.[86] His principal reason for supporting a gold standard was his concern about the danger of 'inflationism': the temptation for political intervention in monetary arrangements, pursuing monetary expansion for short term gain.

The Theory of Money and Credit provides detailed discussion of the illusory arguments used to support inflationism and explains why inflationism must ultimately be self-defeating, ending only in price rises. This is of course a widely expressed view, not restricted to Austrian economists. Many economists will agree that some external discipline is needed to prevent politicians from turning to monetary financing of government expenditure and avoid potentially rapid and accelerating inflation. What is less widely accepted is the Austrian view that this external discipline needs to come by the choice of gold as the medium of exchange.

Von Mises was careful to distinguish different variations of the gold standard, for example the gold standard adopted across Europe after 1873 in which gold coin was still commonly used for payment with the gold standard adopted then in India and other countries of Asia and the Americas, where only token coins circulated but which were exchangeable into gold.[87] In his policy discussion in the 2nd edition of 1924 (Von Mises 1953 Part Three, chapter VI.10) he argues for measures to encourage the use of gold currency and in the material on monetary re-construction in the 3rd edition of 1953 (Von Mises 1953 Part Four, chapter VI.10) he takes an even narrower position, suggesting that a

strict sense of the word is theoretically conceivable. The theory of value proves the possibility of its existence. Whether fiat money has ever actually existed is, of course, another question, and one that cannot off-hand be answered affirmatively. It can hardly be doubted that most of those kinds of money that are not commodity money must be classified as credit money. But only detailed historical investigation could clear this matter up." (Von Mises 1953, pg 61).

[86] (Hulsmann 2012) provides a valuable account of the development of Von Mises monetary theory from the initial publication in 1912, through the second edition of 1924 to the 1953 third edition with its added analysis of the challenges of post-world war II monetary reconstruction.

[87] (Von Mises 1953, Ch 3.II). This he further distinguishes (Von Mises 1953, Ch 3.VI) from a gold-exchange standard, the arrangement adopted for the restoration of gold parties in the 1920s (and later in the Bretton Woods treaty) in which the commitment to gold was based not on a commitment to buy and sell domestic currency for gold, but instead for foreign currency, in practice the US dollar, that itself had a fixed parity in terms of gold.

restoration of the gold standard will require a return to token money that is fully backed by gold as well as exchangeable into gold.

A monetary standard based on gold when, as had been the case since at least the mid-19th century, much of the media used for exchange was fiduciary media issued by banks, notably bank transaction deposits allowing payment through cheques or giros. (Hayek 1937) finds in this an explanation the breakdown of the restored gold standard in 1931, which failed to confront the difficulties associated with the practice of centralising national reserves of gold at the central bank, for two separate purposes: for purchase of the national currency at the fixed parity to gold when there was an international capital outflow and as a reserve to be used by the 'lender of last resort' when there was a demand by domestic depositors to withdraw cash from the banking system.[88]

Hayek argues that this arrangement both makes adjustment under the gold standard much more costly than necessary and also encourages larger fluctuation of money and credit, and hence of spending and prices, compared to that which arise under a 'pure metallic' gold standard. This argument rests on the Austrian understanding of the business cycle. The reliance on centralised reserves reduces constraints on commercial banks and leads to much larger response of bank money and credit and hence of investment when the 'money rate' falls below the 'natural rate' . Furthermore, when there is an external imbalance and a resulting loss of gold overseas, the central bank is forced to raise the money rate of interest substantially above the natural rate to stem the loss of reserves. The resulting Wicksellian discrepancy between the market and natural rate of interest in turn reduces investment, creating a recession and unemployment and undermining commitment to the parity.

On this basis (Hayek 1937) fiercely contested the arguments then being made by Keynes and Harrod that adjustment to economic imbalances required floating exchange rates and would only be impeded by fixed gold parities. For Hayek, under floating exchange rates, politicians would be unable to resist the temptations of turning to monetary finance. Therefore the international gold standard should be restored once again, but this time on a sounder permanent footing. This would require greater discipline on commercial banks through having them maintain much more substantial reserves than they had during  the 1920s. This would both curtail the credit cycle and reduce any call they might make on the reserves of the central bank to levels to manageable levels.[89] There should also be a more rigid commitment to gold parities (reducing the 'gold points' i.e. the range around currencies were allowed to fluctuate).[90] While he does not put it exactly this way, it seems that Hayek was arguing that making national currencies closer substitutes  in this way would ensure a large and rapid response of international capital inflows in response to an increase in the money rate of interest, and further reduce the need for disparity between the money and natural rates.

[88] These two separate functions of national gold reserves were already recognised well before Hayek gave these lectures, described for example in (Hawtrey 1919 Ch VIII) as 'external drain' and 'internal drain'.

[89] 'So long as central banks are regarded, and regard themselves, only as "lenders of last resort" which have to provide the cash which becomes necessary in consequence of a previous credit expansion with which, until this point arrives, they are not concerned, so long as central banks wait until "the market is in the bank" before they feel bound to check expansion, we cannot hope that wide fluctuations in the volume of credit will be avoided.' (Hayek 1937 pg 419)

[90] 'If all the central banks undertook to buy and sell foreign exchange freely at the same fixed rates, and in this way prevented even fluctuations within the "gold points," the remaining differences in denomination of the national currencies would really be no more significant than the fact that the same quantity of cloth can be stated in yards and in meters.' (Hayek 1937 pg 413).

The case for restoration of the gold standard has continued to be argued by many economists working in the Austrian tradition.[91] Amongst the most persuasive and influential is Murray Rothbard, e.g. (Rothbard 1991a; Rothbard 1990), criticising both the fixed-rate exchange Bretton-Woods system, which operated in the early 1960s when the original versions of these books were first written, and floating exchange rate regimes preferred by monetarists such as Milton Friedman. Rothbard endorses Von Mises view that money is not what is determined by the state but rather what is chosen in the free market as the medium of exchange.[92] Bretton-Woods, while based on the revalued gold-parity set by President Roosevelt in 1934 (at $35 per troy ounce of 24 carat gold) , was truly a gold standard because it treated national currencies as something different from gold, fixed their exchange rates against the US dollar and provided no mechanism for individual citizens and private firms to freely exchange their money against gold,

For Rothbard, writing from a strongly libertarian perspective, views virtually all interventions of government in monetary arrangement as counterproductive, weakening what would otherwise would be commodity-based market standards for money, giving overreaching government the opportunity to claim resources by stealth and using these resources to benefit favoured interests. As examples he refers to the monopolisation of the right to mint coin (when market exchange readily enforces quality of coinage), outlawing exchange of foreign coin (facilitating debasement of monopolised coin) and encouraging the inflation of the fiduciary media i.e. unbacked government paper and bank deposits, both through the creation of central banks and by encouraging the shift from the use of gold to a combination of government paper and bank deposits in everyday transactions. These developments had already undermined the stability of the gold standard as early as the 1920s and were only reinforced by the subsequent provision of deposit insurance in the 1930s.

## Austrian arguments for placing limits on fractional-reserve banking

Austrian economists from Von Mises onward have focused on the instability associated with fractional reserved banking. In his discussion of money and banking  Von Mises draws heavily on the earlier 19th controversy between the banking and currency schools in the UK (Von Mises 1953, Part Three). Von Mises even describes his business cycle theory as ‘an extension and elaboration’ of the views of the currency school. He shares their concern that the issue of fiduciary bank notes, i.e not fully backed by gold, could result in excessive call on gold reserves, resulting not just in instability of prices, but also in Von Mises’s theory of the business cycle amplification of unsustainable trade expansions.  The views of the currency school prevailed politically -- in the 1844 Banking Act introducing the division between the banking and issue divisions of the Bank of England and placing a legislative limit on the unbacked issue of banknotes by the Bank of England. For Von Mises, however, there is no essential difference between bank notes so this act was made ineffectual as a restraint on fluctuations of money and credit because it imposed no restriction on fiduciary bank deposits.

Von Mises views on the appropriate policy to address the instabilities of fractional reserve banking shifted over time. In the 1912 first edition he argues that ‘Now it is obvious that the only way of eliminating human influence on the credit system is to suppress all further issue of fiduciary media. The basic conception of Peel's Act ought to be restated and more completely implemented than it

[91] Many expressions of the case for a return to gold by Austrian economists can be found amongst the publications on the Ludvig Von Mises Institute https://mises.org.

[92] ‘Money means a certain commodity, previously useful for other purposes on the market, chosen over the years by that market as an especially useful and marketable commodity to serve as a medium for exchanges.’ (Rothbard 1991, pg 24). Rothbard also emphasises what Austrian economists call ‘the regression theorem’, the argument also from Von Mises that historically money could not have emerged either as the fiat of the state or as a credit money (a deferred commitment to repay money in the future) because, in order to be initially accepted as money it must have a recognised prior value in exchange i.e. must have been a commodity.

was in the England of his time by including the issue of credit in the form of bank balances within the legislative prohibition.' He clearly remained sympathetic to this statement, because he includes it as a quotation in the 2nd 1924 edition, but by then his position had shifted and he argued instead the much less interventionist position that control over fiduciary issue of bank notes and bank deposits was best served by entirely removing state monopoly over note issue.

The appropriate response to the instabilities inherent in fractional reserve banking continues to be a point of controversy amongst Austrian economists. Some, e.g. (Rothbard 1991b), argue that withdrawal of all forms of government support for fractional reserve banking – which in his view is essentially a fraud since banks do not have the resources to meet the withdrawal of funds should depositors request them. He argues that recognition in law that a bank deposits are direct claims on gold reserves held by the bank (and with deposits clearly distinguished from all other bank liabilities which must take the form of deferred claims for future payments by bank either as coupon or dividend.) can ensure that bank money is 100 per cent reserved against gold and would in effect become nothing more than a warehouse receipt for the medium of exchange.

Others working in the Austrian tradition disagree, for example (Selgin & White 1996) dispute the need for restriction on fractional reserved banking, arguing (as we have seen does Von Mises in later editions of the Theory of Money and Credit ) that fiduciary media provide an essential flexibility in the supply of money and  the combination of a commodity standard and a competitive banking system with minimal state interference and support for banks will provide sufficient discipline against excessive issue.

## Austrian arguments for free banking

Austrian economists, consistent with their advocacy of the critical role of the free market in allocation of resources and their hostility to state intervention, have always been supportive of 'free banking', banking without regulatory and legal  restrictions and with limited support of a central bank or possibly even abolition of central banks altogether. The views though on free banking within the Austrian school are varied, much more so than on the gold standard or on fractional reserve banking. A full discussion would require an extensive literature review, which does not seem necessary for the present purpose of assessing the implications of cryptocurrency technologies for Austrian proposals on monetary arrangements.[93]  The discussion here will be limited to a brief indication of the some of the main viewpoints on free banking adopted by Austrian economists.

Austrian arguments for free banking can be traced back to the early 19th century English banking and currency school debates and a third group of participants who argued against both schools, in particular against limitations on note issue and its centralisation in a central bank monopoly.[94] While this argument was lost at the time (the 1844 bank act finally and effectively ending private bank note issue) the view that banks should be allowed freedom to operate without state interference features prominently in the work of Austrian school economists.

Many studies of free banking by Austrian economists are examinations of the historical experience of banking systems, suggesting that at least in some circumstances competitive note issue can be stable, even without a central bank acting as a lender of last resort. This leads to many to the view that banks should be free to accept (or create through lending) fractionally reserved deposits, denominated in widely accepted means of exchange, which if this cannot be gold should at least be the national currency (i.e. disputing the need for restrictions on fractionally reserved banking espoused by some other Austrian economists, see the discussion of Rothbard's views above). Left to

[93] See for example the articles collected in (Capie & Wood 1991; Dowd & Timberlake 1998) and the review by (Selgin & White 1994). For another perspective see (Sechrest 2008).
[94] (Schwartz 1989) provides a brief summary and (Smith 1936) a more detailed discussion.

laissez-faire banks can be expected to come to their own arrangements for protecting their liquidity and preventing failure in the event of crisis – for example through suspension of deposit withdrawal. They argue for example that the various banking panics of the US national banking era – before the establishment of the Federal Reserve were far less economically damaging than many suppose.

Austrian school writing, with its suspicion of all forms of state intervention in the market, also strongly criticises the many various and extensive forms of state intervention in the banking system, whether this is central bank control of market rates of interest rather than leaving these to be freely determined by the market or the protection to banks provided both explicitly by deposit insurance and implicitly promise of support in event of crises. Such views are not restricted to Austrian economists, but perhaps most characteristically Austrian is highlighting the shortcomings of policy making at the time of crisis. There are strong political economic pressures on politicians and regulatory authorities to respond to financial crises, treating them as special emergencies and as a result setting aside their usual commitments to the support of market mechanisms. This response hinders the process of market adjustment, hampers recovery and sows the seeds for future financial problems.[95]

Yet another and even more stark statement expression of the case for free banking was made by Friedrich Hayek towards the end of his life. In 1937 he was of the view that strict limitations on fractional reserve banking were necessary.[96] In the late 1970s, returning to monetary economics after more than thirty years devoted to his influential anti-statist writings in the domains of politics, law and psychology, he was no longer expressing his previous concerns about fractional reserve banking and had even abandoned the case for return to the gold standard. He saw instead the restoration of monetary stability as being achieved by allowing free private sector issue of competing monies.[97]

Hayek's scheme envisages a number of banks each offering their own different competing money with a promise to maintain the value of this around some defined commodity index, i.e. there would be not just one medium of exchange but rather a variety of media of exchange with competing rates of exchange between them and competitive forces determining the markets choice of which are preferred for any particular market exchange. While this does sound a little far-fetched, he was able to point to several historical instances of competing media of exchange, and appeals to the use of computer technology as a means of making possible price comparison in several different monies. As discussed in the main text, his proposals remain only speculative, not only are there no real examples of such competition but it is unclear that promises to maintain the value of competing currencies against underlying commodities can ever be credible.

## Liquidity risk: the 'Achilles heel' of Austrian monetary economics

This summary of Austrian economics reveals a fundamental tension, while consistently espoursing the need for the withdrawal of the state from monetary arrangements and other areas of economic exchange, Austrian economics has never been able to provide a satisfactory solution to the challenge of providing liquidity when banks engage, freely and without support of the state, in fractional reserve banking.

[95] For an articulation of this view see (Boettke & Palagashvili 2016)

[96] 'Now it is obvious that the only way of eliminating human influence on the credit system is to suppress all further issue of fiduciary media. The basic conception of Peel's Act ought to be restated credit in the form of bank balances within the legislative prohibition.' (Hayek 1937, pg 408)

[97] (Hayek 1978; Hayek 1979).

To understand the difficulty is is worth explaining a little more of the basic functioning of systems for the clearing and settlement of bank payments. Current bank payments based on fractionally reserved deposits, whether historical paper-based cheque and giro instruments or the variety of modern card and bank transfers, all require subsequent settlement. This settlement of payment between customers of different banks is most often through a matching transfer from the payer's bank to the payee's bank in central bank reserves (though for some transactions a bank-to-bank transfer of deposits held with a commercial bank – a 'correspondent bank' – may also be used instead).[98] Under the classical gold standard the medium of settlement was either gold or bank notes backed by gold. Under later monetary arrangements settlement has been in central bank deposits, possibly exchangeable into gold but then only on a gold-exchange basis.

The use of central bank reserves for settlement of payments from fractionally-reserved bank deposits is what gives central banks their central monetary role. Banks must ensure that they are always able to settle payment instructions. They do this by keeping sufficient 'liquidity' – central bank reserves, or unutilised credit facilities or borrowing opportunities, or marketable short-maturity high-quality securities that can be sold for reliable value at short notice – to be able always to settle their payments. Inability to settle payments on any substantial scale would lead to other banks refusing to deal with it and quickly make it impossible to provide core credit and payment services. Banks must turn to central banks if necessary, as a final provider of liquidity, to maintain operations. This allows central banks to control money market rates of interest, the marginal source of funding for bank funding and therefore the basis for setting all commercial bank interest rates.

Shortage of bank liquidity was at the heart of the global financial crisis of 2008.[99] This demonstrated beyond doubt the need under a fractionally reserved system for the central banks to provide bank reserves on demand, especially at times of crisis when many banks find it impossible to borrow in money markets from other banks or wholesale investors. The obligation to provide central bank liquidity is also the main practical obstacle to implementing Austrian proposal's for 'free banking'.

Austrian thinking would giving banks complete freedom to create fiduciary media (monetary deposits or possibly also their own bank notes) i.e. the type of transaction shown in Figure 1b except that the money created is a deposit on the bank balance sheet not on the ledger. According to Austrian thinking the bank creation of fiduciary media should be effectively controlled by market discipline – unsound banks that issue fiduciary media and use it for funding unsound loans will fail and should be allowed to fail. Liquidity can – it is suggested from the historical experience of banking systems that have operated without central bank support -- can be provided without the need for a central bank through 'suspension of convertibility' i.e. a temporary stay on the ability to access monetary deposits and use their use for payments to other banks.

Even if central bank liquidity is sometimes provided, then according to Austrian thinking only solvent banks should only get access to emergency liquidity, unsound banks should be wound down, to avoid the state support that will encourage banks to take great risks in lending and other activities.

These Austrian proposals are though extremely difficult to put into practice because of the obligation to provide emergency liquidity in a financial crisis. This obligation is unavoidable for several reasons. First, households and many business rely on access to bank deposits for immediate payments needs. Suspension of access to deposits creates substantial economic and social disruption and is not a credible response in a modern monetary system when most monetary

[98] (Rambure & Nacamuli 2008) provide a convenient summary of the mechanics of bank payment systems.

[99] The author's account of the global crisis (Milne 2009) emphasises the role of liquidity.

payments are conducted using bank deposits. This means that it is not realistic to run a modern fractionally reserved banking system without central bank liquidity provision. Second, it is impossible to distinguish insolvency from illiquidity in a financial crisis, so there is no way to distinguish good from bad banks when distributing liquidity. Third, as the financial crisis of 2008 illustrates, political pressure for both generous deposit insurance and – in the event of widespread concerns about bank stability – public guarantees on bank obligations, both retail and wholesale, mean that while a relatively small individual bank might be closed as a result of  loan losses, larger banks or an entire banking system are always protected from the downside consequences of their lending and investment decisions.

The unavoidable obligation on central banks to provide liquidity in a financial crisis has made it practically impossible to implement Austrian free banking proposals. Instead the mainstream consensus has come around to the view that extensive regulations must be imposed on all banks, limiting their risk exposures and insisting on high levels of both capital and liquidity reserves.

The proposal for mutualisation of bank monetary deposits of this paper provides a practical means for protecting this ‘achilles heel’ that has hitherto always prevented practical implementation of Austrian ideas on monetary arrangements.