

What Kind of Money do We Want?



*A guide to understanding how money works and how
new technologies can help us build an abundant
society*

Aran A. Dunkley
aran@organicdesign.co.nz
www.organicdesign.co.nz/writing

Copyright © 2017 Aran A. Dunkley

Version: 1.4, 2018-03-05 [9d154ea]

This booklet is derived from the *Trustless Mutual Credit* paper.

Use this link to download this booklet or the original paper and other writing:
www.organicdesign.co.nz/writing



This work is licensed under a
Creative Commons Attribution-NoDerivatives 4.0 International License
(You are free to copy and redistribute this work in any medium or format provided it
is not modified, given appropriate credit and is not used commercially)

“Money is merely an abstract representation of the real credit of the community, which is the ability of the community to deliver goods and services, when, and where they are required”

– C. H. Douglas [1]

“Money cannot meet modern needs by descending to the people; it must rise from them.”

– E. C. Riegel [2]

1. Introduction

There can be no true democracy when the issuance of money is in the hands of the few, regardless of what type of money it is or who those few are. Money is the fundamental energy of society, analogous to the role blood plays in a living organism.

There are a number of important properties that are associated with various forms of money:

- It's used as a **unit of account** which simply means that we're able to exchange apples for oranges, valuing everything in terms of a single standard unit makes trade and accounting much simpler.
- It's used as a **medium of exchange** which means that two people can trade with each other even if only one of them has something the other wants, because money can be used in the place of something of real utility since it can be exchanged for something of utility at a later time.
- It has to be a **store of value** which means that we can keep an amount of it aside and rest assured knowing that it will still have the same **purchasing power** in the future.
- It must be **portable** and **durable**, but this doesn't necessarily mean it has to be physical, for example digital money can fulfil these requirements.
- It has to be **divisible** so that payments of any amounts can easily be made.
- It must have **fungibility**, which means that no matter the origin of a unit of money (e.g. a five Euro note) or the condition it's in, it's just as acceptable and valuable as any other unit of the same type and denomination of money.

There is much difference of opinion amongst specialists as to which of these properties something can, must, or must not have in order to be called "real" money. For example some say that for something to be able to be considered as real money, it must have *all* of the properties listed above such as gold and silver coins do. Others say that to be real money, it *must not* have any inherent value of its own, it must be purely a medium through which things of value are exchanged. Yet others say that some of the properties, particularly *medium of exchange* and *store of value*, are *incompatible* with each other and so different kinds of money should have different selections of the properties.

I'm not going to get into any arguments about what's *real money* and what's not. I'm going to focus this discussion on three different kinds of money, and I'm calling them

all *money* by using hyphenated names to distinguish them. These three kinds of money are *commodity-money*, *credit-money* and *fiat-money*. I'm also going to talk about a fourth thing that many people think of as money too – I'll be talking about *Bitcoin*; what it is and how the technology behind it could help us make better money.

2. Commodity-money

Bartering is the simplest model of exchange, but it severely limits the capability to trade due to the *coincidence of needs* problem, i.e. that both parties need to be offering what the other wants at the same time for any exchange to be able to occur.

History shows us that many early communities realised that some goods, such as salt or tobacco, were so widely used that they could be used as a *medium of exchange* that vastly increased the community's potential to trade.

Eventually specific weights of gold or silver became the dominant medium of exchange used as they were found to be more widely accepted and durable than all other forms.

The advantage of using commodity-money is that the seller need not have trust in the money system or the buyer's reputation since nobody's ever indebted to anyone else. When someone pays for a good or service with commodity-money the seller has received something of equal value directly in return, so the transaction has been completely settled right away.

The main problem with commodity-money is that it relies on a supply of a physical resource to facilitate exchange, which means that the value of the money, and therefore the prices, are not stable.

It's also easy for the wealthy to manipulate the supply by owning sizeable proportions of the commodity, which offers various means of gaining power over the common people, for example by controlling prices.

3. Fiat-money

Fiat-money is a form of money that's **issued by the state** and obtains its acceptance by decree, which is the aspect of the money that the name refers to – the term *fiat* is a Latin word meaning “let it become”. Fiat money is debt-based and is either partially backed by gold or not backed by anything at all. The fact that its issuance is controlled by the state rather than by those involved in the process of exchange gives rise to the potential for severe corruption and exploitation of the people who use it.

Since most modern governments also outlaw the use of any other forms of money, fiat-money is essentially money that obtains not only acceptance, but a monopoly position by *force*. This means there is little incentive to ensure it fulfils the role of “sound money”; the true incentive behind it is to enrich those who control its supply.

There is however, some tolerance by the state towards community currencies as long as they remain local and do not compete with the state money – these days the term *complementary currency* is normally used to keep it on the right side of the state. If a community currency becomes too successful or widespread, it risks attracting hostility from the state¹.

3.1 The origins of banking

Fiat-money and the banking system go hand-in-hand, so I’ll first give a very brief and simplified introduction to the origins of the modern banking system. For a more in depth look at this, I recommend watching “*The Money Masters*” which is an excellent documentary covering the history of banking and how it led to the the global financial situation we have today. Two other documentaries I recommend go into more detail about the current state of the system: “*The Secret of Oz*” and “*The Inside Job*” (See the documentaries section at the end of the paper).

The story of banking starts with the money changers who had secure vaults for their gold and other valuables. Other wealthy people didn’t want to risk all their savings by storing it insecurely themselves, so they would store it in the money changer’s vaults for a fee. The money changer’s would give the gold owners certificates proving how much gold was stored in their vault which they could use to claim their gold at any time.

This became very popular and before long it was realised that these gold certificates could be exchanged for goods and services directly instead of going to the money changer, getting the gold and exchanging it in trade, and then the seller going straight back to the same money changer to deposit the gold and get another certificate. In other words the gold certificates had become a *medium of exchange*.

As time went by, the money changers noticed that since people rarely collected their physical gold, since it wasn’t used directly in trade any more, they could write their own *fraudulent certificates* that would be accepted in trade even though they didn’t represent any real gold at all.

1. See for example the *Liberty Dollar* story, which can be found on the new replacement project site: [<https://shiresilver.com/history>]

The ironic thing is that this cheating was actually essential to the progress of civilisation because our potential to exchange had been severely limited by the supply of gold. Perhaps we could have resolved the problem ourselves by having the power of money issuance in our own hands using a credit-money system. I personally think that it would not have worked, because without the help of technology it's a system that's just as corruptible as gold unless it's restricted to the small community scale.

Eventually the money changers had so much power that state regulation was called for to bring it under control. Unfortunately this turned out to be a jump from the frying pan into the fire; money is a function of production and needs to be controlled by the producers.

Being regulated by the state didn't weaken the power of the wealthy families, who controlled the gold and silver, because they had already been consolidating their power for centuries. Rather, it just gave them legal sanction to continue their fraudulent practices by covering them with the official veneer of **state-issued fiat-money** and the status of a **bank**.

3.2 Fiat-money is created out of thin air

Even if it were originally implemented with the best of intentions (which is doubtful to say the least [3]), the natural law of corruption of power always degrades fiat monies over time until they exhibit the most atrocious qualities, such as having interest attached to their issuance and deliberately using inflation to extract the real wealth out of the population. As John Maynard Keynes, one of the principal architects of the modern financial mechanism once noted:

“By a continuing process of inflation, government can confiscate, secretly and unobserved, an important part of the wealth of their citizens.”¹

Fiat-money is literally created out of nothing – most of it is *loaned into existence* by banks as **interest-bearing debt**. When somebody goes to the bank to get a loan, or extend an existing loan, the money is simply added to their account balance, it doesn't come from any other account or deplete any sort of reserve. Over 97% of today's money is bank account balance that has been created in this way².

Sounds crazy right? What, you don't believe me? Here's a few quotes from some people who've known the system pretty well from a few different countries throughout the last century.

1. John Maynard Keynes, “The Economic Consequences of Peace”, 1919

2. See this video tutorial about money creation and its limits: [<http://positivemoney.org/how-money-works/banking-101-video-course/>]

“Banks create money. That is what they are for.. The manufacturing process to make money consists of making an entry in a book. That is all... Each and every time a Bank makes a loan... new Bank credit is created – brand new money.”

— Graham Towers, Governor of the Bank of Canada from 1935–1955¹

“When a bank makes a loan, it simply adds to the borrower’s deposit account in the bank by the amount of the loan. The money is not taken from anyone else’s deposit; it was not previously paid in to the bank by anyone. It’s new money, created by the bank for the use of the borrower.”

— Robert B. Anderson, Secretary of the Treasury under Eisenhower, 1959²

“Do private banks issue money today? Yes. Although banks no longer have the right to issue bank notes, they can create money in the form of bank deposits when they lend money to businesses, or buy securities... The important thing to remember is that when banks lend money they don’t necessarily take it from anyone else to lend. Thus they create it.”

— Congressman Wright Patman, 1964³

“When banks extend loans to their customers, they create money by crediting their customer’s accounts.”

— Sir Mervyn King, the Governor of the Bank of England from 2003–2013⁴

Most people attribute the main problem with fiat-money to the fact that it’s no longer backed by gold⁵, that if banks could only lend based on a percentage of the real reserves they have available in gold, then the most pressing problems with the financial mechanism would be resolved. There are some movements around with the aim of returning to the gold standard or another true reserve system such as *Positive Money*⁶ or Ron Paul’s *End the Fed* movement⁷.

1. Standing Committee on Banking and Commerce, Minutes of Proceedings and Evidence Respecting the Bank of Canada, Ottawa, 1939 (p238) [<https://www.scribd.com/document/9525141/Standing-Committee-on-Banking-and-Commerce-1939-p248-315-May-3-1939-CANADA>] (Most of the evidence quoted was the result of interrogation by Mr. “Gerry” McGeer, K.C., a former mayor of Vancouver, who clearly understood the essentials of central banking)

2. Interview reported in the August 31, 1959 issue of *U.S. News and World Report*

3. Money facts 169 questions and answers on money – a supplement to a primer on money with index: Subcommittee on domestic finance Committee on Banking and Currency, House of Representatives, 88th Congress, 2d session, Sep. 21, 1964

4. Sir Mervyn King in a speech at a business conference:

[<http://www.bankofengland.co.uk/publications/Documents/speeches/2012/speech613.pdf>]

5. The last remaining thread connecting the USD with Gold backing was removed by Richard Nixon in 1971

6. [<http://positivemoney.org>]

7. [<http://ronpaulinstitute.org>]

It's true that having some physical backing to fiat money forces it to stay a little more honest, but as has already been discussed, commodity-money is also a big problem for society. Trying to fix the problems of fiat-money using commodity-money is just using a lesser evil to try and fix a greater one.

3.3 Scarcity & Interest

Interest on debt makes sense within the context of *scarcity* such as is the case with commodity-money, because there is an *opportunity cost* associated with lending it out. For example if I had some gold, I would certainly not want to lend it to anyone unless I was going to be paid a fee for putting it at risk and losing the ability to take advantage of other investments I could otherwise make with it.

The compounding aspect of interest follows logically as well, because the fee should obviously be in proportion to the amount lent and the length of the term. If after an initial term one chooses to extend the duration of the loan to another term, then the same conditions apply but the amount of the second term's loan is the same as the initial loan but also includes the first term's fee.

This also applies in the context of fiat-money because it's also scarce like a commodity, but in this case the rationale for interest is a little more dubious because the **scarcity is artificial**. Since the money is created out of thin air, it would be trivial to ensure that all of our potential for exchanging goods was actualised just as it would be if we issued it ourselves using a mutual credit system (see *Section [4]*).

But those with the power of issuance choose not to distribute it in accord with the needs of the people, and instead to issue it unfairly in accord with where the greatest rewards in terms of power consolidation are to be found, which mainly involves keeping as much of the world as they can in a **continuous state of war and poverty**¹.

This artificial scarcity of fiat-money means there's never enough of it where it's needed, and too much of it where it does harm to society and the environment. It's the fundamental reason that our society is competitive instead of cooperative, and is the main reason why billions of people around the world, both in poor and affluent areas, are struggling to make ends meet.

The fact that they make this money out of nothing and then also make it artificially scarce – and then on top of all that it **has interest due on its repayment** is a humanitarian crime so horrendous it defies comprehension.

1. See for example John Perkins, "Confessions of an Economic Hit Man", 2004

The scarcity aspect of fiat-money (and commodity-money) can be clearly seen when we consider a wide-spread problem that occurs in many small communities, especially poorer ones. The residents have almost no fiat-money. This means that even though together they have many different skills and needs, the entire community is at a stand-still because none of them have the government-issued paper that allows any exchange to occur.

The natural role of money is to ensure that a group's potential to exchange their goods and services can be actualised – if people are unable to exchange them solely due to lacking the correct piece of paper, then there is clearly a requirement for them to be issuing their own paper.

3.4 Unlimited growth

It's important to recognise the incentives that are present in a system. Whether they're there by design or not, they're the underlying forces that determine the behaviour patterns of those who use the system.

In our current global financial system there is an underlying growth incentive which comes from interest on debt, which in turn comes from the scarcity of money. The scarcity of money leads to a competitive society instead of a cooperative one, and this creates the psychology of greed and continuous growth.

But having money created with interest attached to it is the main driving force behind unlimited growth because it means that the money supply itself is inherently subject to exponential growth – this is the ultimate disconnection of the money from reality.

Trying to add superficial rules into the system to prevent the unending quest for growth, for example by introducing carbon taxes to try and put the environment first, can't really succeed. It's just seen as an obstacle that can be overcome using devious means such as the falsification of statistics¹. Such superficial add-ons create contradictions where some parts of the system are fighting others, but the fundamental force of unlimited growth always wins.

The only way to truly address the problem is to look at where the incentives in the system come from and create an improved design that eliminates or otherwise accounts for the unsustainable incentives.

* * *

1. [<http://www.bbc.com/news/business-34324772>]

All of these problems with fiat-money – that its debt-based, unbacked, scarce, comes from nothing and has interest attached to it – all come from one common cause. That others have the power of issuance over the money that *we* use – but money issuance is not something that can be delegated out to others, we have to do it ourselves. Issuance of money is naturally a part of the process of exchanging goods and services, separating it out can only lead to suffering.

4. Credit-money

Another method of expanding the potential for trade that was used historically is what can generally be called *credit-money*.

One example of this is cattle owners who made leather discs to represent a single head of their cattle¹. The grain merchants trusted that these discs could always be exchanged for a head of cattle, and so they would be willing to accept them in return for corn.

Note that in this system, the cattle owner is **creating his own money**, but its utility comes from the fact that the corn merchant accepts it as payment for corn. Another way to say this is that, this form of money is **issued by the buyer and backed by the seller**.

There are other forms of credit-money that are issued by a central authority such as “air miles” or “gift vouchers”, but I’ll be focusing on a particular form of credit-money that’s issued by the buyer during the exchange process. This kind of credit-money is called *mutual credit* which is the term I’ll be using from now on.

Mutual credit effectively splits the barter process into two halves. When a buyer wants a good he offers a token, such as the leather disc, to the seller, who recognises and accepts it knowing that he can *redeem*² it for value at a convenient time in the future.

Since the token has no intrinsic value, there is a delay between the first half of the transaction, when the buyer is satisfied by receiving his produce, and the second half, when the seller is satisfied by receiving something of equivalent value in return.

One important thing to note about mutual credit is that it’s all **created as a debt**, it would be just as valid to call it debt-money, it’s just a matter of perspective.

1. So strong are the historical ties between cattle and money, that the origins of two words commonly used in finance today are connected to cattle. The word pecuniary derives from *pecus*, the Latin word for cattle, and the word capital from the Latin word for head, *caput*.

2. This word “redeem” is used with all forms of credit-money because during this delay one of the parties in the trade is not satisfied. This dissatisfaction is the money’s “fault” and therefore it’s the money’s job to redeem itself by eventually ensuring that all parties are satisfied.

Compare this to the use of a commodity that has its own intrinsic value. When a person receives a good from a seller and pays with a commodity like gold or tobacco, the transaction has been completed at that point. There is no splitting of the transaction with a delay before the seller is made whole, he is already satisfied because he has already received something of equivalent value from the buyer. The fact that what he received is something that he'll exchange later for something else is an altogether different matter, a new transaction of its own. Commodity money involves no debt because everyone is whole at all times. The debt aspect of mutual credit creates the disadvantage that it relies heavily on trust in the issuer, so it's really only successful in local communities or other trust networks.

Another disadvantage of mutual credit is that it's not a good *store of value*, because the more people hoard it, the less of it is available to the rest of the community, and the less able to facilitate exchange it becomes. Ideally we'd be using a mutual credit system to facilitate exchange in the community, and a commodity-money system for our savings.

Mutual credit's big advantage, which is why I'll be focusing on it herein, is that communities, especially poorer ones, that would otherwise have no means to actualise their potential for exchange at all, can begin to flourish from nothing using it.

It's the most natural grass-roots form of money that any community can use to build independence and abundance for themselves, without requiring any external resources or specialist knowledge.

4.1 Mutual credit explained

The first thing to understand about mutual credit is that it's just an administrative tool allowing a group to settle accounts amongst themselves more easily. So let's first look into what's involved in the general settling of accounts between some members of a community.

Imagine you're a member of a small community and you produce some fruit, vegetables and eggs each month. Imagine for simplicity's sake that all your monthly living requirements are obtained from the general store and that the store is also happy to buy your produce whenever you have some to offer. Of course since you deal with each other every month you have an *account* with them, whenever you buy anything from the store, the owner simply adds a debit entry to your account, and when you sell some of your produce there he adds a credit entry.

Let's say you settle the account on a monthly basis, this is a process of adding up all the credits and subtracting the debits. If what you produce is similar in value to what

you purchase each month, then very little money will ever change hands. In fact you could even decide to deliberately adjust the amount of work you do, or the amount you buy, so that your monthly account is always fairly balanced and you never need to exchange any money at all. Some months you may fall a little short, but the store owner knows you can make up the short fall over the next month or two so he doesn't worry about it. This method could of course carry on indefinitely, there's nothing mystical about it. Many businesses, large and small, regularly settle their accounts amongst themselves this way to avoid making unnecessary monetary transactions.

Now imagine that one month all your blueberries were destroyed by ants and you had quite a large short-fall with the general store owner. Rather than working hard to make up this short-fall with your vegetables and eggs, you decide to help your neighbour build an extension to his house at a certain agreed upon rate.

Since you owe a lot to the general store and your neighbour also sells his produce and has an account there, the three of you all agree that the easiest way to settle your debt with the store would be for the store owner to make a transfer of an agreed amount each month from your neighbour's account to yours.

In reality everyone in the community would be trading with many others, not just the general store – and the general store owner would be trading with many others too. So this process of settling accounts would be made simpler by electing one person in the community to fill the role of accountant.

Rather than calling the accountant every time a transfer is necessary, each sale in the community would be associated with a *cheque* signed by the buyer to authorise the debiting of his account, and given to the seller to present to the accountant when convenient – e.g. maybe each day when passing by the accountant's house, or for those living further away, each time they come into town. On receipt of a cheque, the accountant debits the account of the signatory and credits the account of the bearer.

This is mutual credit – an accounting system where every sale involves the transfer of ownership of something of real value, and an associated transfer of credit involving a debit from the buyer's account and a credit to the seller's account.

The cheque itself is nothing special, it could be nothing more than a table napkin showing the amount to debit, and a signature to prove that the account holder authorised it. After the accountant completes a transfer of credit in accord with a cheque, it is marked clearly as having been processed, and is filed for future reference in case of a dispute.

Notice that every cheque is created by someone who has an account during the process of buying something. The cheque is inherently worthless, it's just a table napkin, but the seller gives it value by believing in it and exchange his goods of real value for it.

This can be said in a more precise way: credit-money is *issued* by the *buyer* during the act of buying, and *backed* for value by the *seller* due to his acceptance of it as payment for goods.

4.2 Paper money in a mutual credit system

Directly authorising transfers between accounts with cheques or personal visits to the accountant is one way of enabling money to flow, but it's not as simple and handy as having paper money for common everyday transactions.

Paper money has the advantage of allowing people who don't have accounts to participate in the community economy. For example a back-packer may wish to do some work while she stays for a few days. The sellers in the community wouldn't be comfortable backing napkin-cheques issued by someone they don't know, but they'd be happy accepting the community's paper money from her. The seller's acceptance of the notes in turn means the backpacker is happy to accept them as payment for her work while she's staying there.

Paper money is implemented in the community simply by giving the accountant the ability to print it when anybody wishes to *withdraw* some of their account balance into paper form. Note that in this process, the accountant isn't printing the money out of thin air, as is often happening in fiat systems, she's changing money that already exists as an account balance into a physical form.

Every person with an account has the freedom to hold as much or as little of it in the form of physical notes as they wish. If they decide to deposit some of the notes they hold into their account, they can present them to the accountant, who then credits their account balance and removes those notes from circulation.

The reason the sellers are happy to accept the notes from anyone even though they lack any reputation or account, is because they know that all the notes in circulation originally came from one of the trusted member's accounts and was authorised by them for withdrawal.

One of the main purposes of paper money is to facilitate exchange amongst people who don't know each other; it's the notes they trust, not the person presenting them.

But if the notes are not tied directly to an account, or the money in the account itself is not directly connected to the system of production and consumption, then the trust in those notes is misplaced and can only lead to trouble.

4.3 LETS

Mutual credit systems are used by thousands of small communities around the world, most of them being based on a model called LETS (Local Exchange Trading System)¹. When implemented well, it is extremely beneficial for the community.

Most LETS participants don't like to look at their system as a form of money, they see it more like doing favours for one another, but keeping a record of how much everyone has given and received. This record-keeping is important so the members can all help to keep the system in balance together. A common LETS slogan referring to this aspect is that it's "*keeping score, nothing more*".

A trade is recorded by the seller (LETS uses the term "giver") filling out a triple-section receipt. One part for their own records, one part for the buyer and one for the administration office. It's up to the seller to hand in the office section of the receipt so that the account balances are updated.

The accounts in the office are usually maintained using a simple spreadsheet that allows the balances of any participants to be easily viewed, and basic reports to be generated for viewing information such as turnover or most wanted services.

A physical LETS system doesn't involve any more than that as far as the money (or favour points) goes, but there is a lot more to it in terms of keeping it active and building up membership etc. James Taris' book "*The LETSaholic Twist*" [4] covers all these down to earth aspects of a LETS group really nicely.

4.4 Corruption of power

The corruption and abuse of centralised points of influence in society is a natural and expected phenomenon, and the most influential aspect of society is its money issuance.

The fact that it's expected is certainly not saying that it's acceptable in any way. It's just that centralisation of power, corruption and greed are all examples of "forces" that exist in the environment of the social mechanism, similar to how friction and rust exist in the environment of a physical machine.

1. [<http://www.lets-linkup.com>]

Without any effective means of fighting corruption, it's inevitable that these corrupt powers will continue to consolidate and expand unabated. Protesting or imposing bad-behaviour taxes is like trying to prevent rust in a machine by sticking a "rust prohibited" label on it! Authorities do not control natural laws, they can only be accounted for in the design of the systems that are affected by them.

All the aforementioned monetary systems fall prey to the corruption of power, even LETS, which can only keep it in check by restricting its operation to small groups who know and trust each other.

I believe the only workable solution to this problem of corruption of the money power requires an open global-scale communications infrastructure and strong encryption accessible by the common people.

"A complex weapon makes the strong stronger, while a simple weapon – so long as there is no answer to it – gives claws to the weak."

— George Orwell¹

The strong encryption we have today is accessible to nearly everyone on the planet, and yet is unbreakable even by the state. This encryption gives us our "claws", and used in the right way it can provide, for the first time in history, a practical solution to corruption in the mechanisms of our society. Bitcoin is the first monetary solution that uses encryption to overcome this problem of corruption of power.

5. Bitcoin

It's very difficult to classify whether Bitcoin is a commodity or a form of credit-money because it's not really backed by anything, and yet it does have a market value. One could argue that it's backed by the important service that it provides which no other form of money can claim to provide: the ability to move value anywhere in the world in a totally secure, independent and unforgeable way.

In the context of this discussion I'm referring to it as a form of commodity-money, because the only practical way you can get some Bitcoin is to exchange something of value for it – i.e. to buy it.

Something I've been hearing a lot recently is that Bitcoin is a "CIA operation". The evidence for this is not very compelling², but let's say for the sake of argument that it's true.

1. George Orwell's 1945 essay "you and the atomic bomb"

2. [<https://cointelegraph.com/news/op-ed-no-bitcoin-wasnt-created-by-the-cia>]

Even then, it's still no reason to throw the entire concept out the window. Why? Because **Bitcoin is libre software!** It's impossible to hide anything in the programming, because we, the people, own Bitcoin and any of us can see every part of it ourselves¹. If there's any part of it that any of us don't like, we can just copy it and change it into a new form of money that we do like. It's already been written in many different programming languages by different teams, and has been changed thousands of times to work in different ways for different projects. It's the concept itself that's important, not a single specific instance of the concept.

5.1 Why is it so important?

So what is the Bitcoin concept? If it's just another form of commodity-money, then what's the big deal about it?

Bitcoin is the first successful example of a system which solves one of humanities deepest and most long-standing problems: **corruption of the authorities we've placed our trust in.**

You see it's not *what* Bitcoin does that's so important, but rather the *way* it does it. We can apply this same *way* to all sorts of different ideas. Many of the things that we've traditionally needed to rely on governments or other institutions to do for us, we can now do ourselves without needing any *trusted third-party* to mediate the process for us.

In a nutshell, Bitcoin is a *peer-to-peer* network – a network of computers in which there is no central computer governing the system. Bitcoins are created and given to the people who expend their computing power to validate the transactions in the network. The amount that is created is **stable and predictable** – Bitcoin's money supply *will* expand by about 4% this year, down from about 7% last year. A specific number of coins are created every ten minutes (called the *reward*). The reward halves every four years – it was initially fifty Bitcoins when the network was launched in 2009 and is currently 12.5 Bitcoins.

For a more detailed introduction to Bitcoin, see Andreas Antonopoulos' book "Mastering Bitcoin: Unlocking Digital Cryptocurrencies" [5], or the original technical white paper by the anonymous² author Satoshi Nakamoto [6].

1. The Bitcoin core project's code is in GitHub at [<https://github.com/bitcoin/bitcoin>]

2. Many now claim that Craig Wright is the identity of Satoshi Nakamoto, but he has never revealed any solid evidence for this to the public. See [<http://www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair>] for an in depth look into the Craig Wright story.

People had been trying to create a fully decentralised money system for many years before Bitcoin was developed. It started with the *Crypto-Anarchist Manifesto*¹ by Tim May in 1988, which said:

“These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions.”

The core problem which is needed in almost any decentralised system and that nobody had been able to solve before Bitcoin is called **distributed consensus**. This is a *messaging protocol* – a means by which all the peers in the whole network can arrive at unanimously agreed upon decisions together by passing messages around to each other.

This doesn't sound like much of a tough problem until you hear the conditions that it's required to work under.

Not only must it deal with the normal peer-to-peer issues such many peers coming online and going offline spontaneously (a network property called *churn*), but this protocol must still allow the network to quickly make unanimous decisions even if up to 50% of the peers in the network are deliberately *lying* in their messages to try and sabotage the system.

Being able to continue operating reliably under these conditions makes the Bitcoin network extremely resilient. Many methods have been tried to destroy or cripple this system by governments and special-interest groups who see it as a threat to their power. They've tried clogging it up with too many transactions or other messages, tried creating malicious peers that falsify information in subtle ways, tried buying huge amounts of Bitcoin and then dumping it on the markets, tried slapping legal regulation on it – they've even tried bribing some of the programmers who work on the code to sabotage the project from the inside!

At the same time as these attacks, there are always thousands of people trying to figure out ways of hacking it to create free Bitcoins or steal other people's Bitcoins. None of this has ever worked, **Bitcoin has never been hacked**.

You may have heard about “huge Bitcoin hacks” in the media such as the infamous *Mt. Gox*² hack, but it's important to realise that these hacks happened to Bitcoin *exchange web sites*. Such sites are vulnerable because they just use standard centralised web site technologies running on centralised servers.

1. [<http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html>]

2. [<http://falkvinge.net/2014/02/28/the-gox-crater-crowd-detectives-reveal-billion-dollar-heist-as-inside-job/>]

Attributing such a hack to Bitcoin is like saying your gold coins were badly made, because someone was able to break into your vault and steal them! The security issue is clearly with the vault, not its contents.

There are now many projects based on this new Bitcoin technology, and the general concept has become known as a **trustless system**, because it's a system that works without requiring any *trusted third-party* in its operation. The word "trustless" has a very negative ring to it because trust is such a positive attribute, but in the context of a resilient and secure system, the *dependence* on trust is a severe weakness.

Trustless systems allow us to create systems that return the power to the people, even though the *status quo* may not approve of them, and may react to them with hostility as they have with Bitcoin.

6. Trustless mutual credit

The two big problems that have been identified in this paper are, first that money issuance needs to be part of the process of exchange itself, and second that money issuance is the greatest attractor of corruption and authoritarian control.

Since *mutual credit* is a solution to the first, and *trustless systems* are a solution to the second, it seems natural that we should look into the possibility of combining these two things together: a new type of money could be made that works the same way as *mutual credit*, but in the form of a *trustless system*.

"[Community currency] represents some (very) old wine that could play a broader role if served in the new bottles that today's technologies make available."

— Bernard Lietaer, pioneer in community currencies [7]

Trustless mutual credit would also overcome another major problem; if a new global money were created that really began to empower the common people, it would attract corruption and control like a magnet and would be the focus of a lot of hostility from the *status quo*, so it's essential that it's designed in the form of a trustless system.

Note however, that the idea of *trustless* mutual credit doesn't imply that there's no trust involved in the system at all. Mutual credit is founded on "trust groups" – local groups of people connected by trust relationships. The *trustless* aspect is purely about decentralising the money aspect that the trust-groups use so that it can't be co-opted by corporations, governments or special interest groups.

There are already some instances of mutual credit and crypto-technology being merged, such as *Ripple*¹ and the *Holochain* project² which shares this very vision for currency. I think we'll start seeing a lot more projects focusing on this kind of thing in the coming years as the problems with the current mechanism become more apparent.

6.1 Transactions

A trustless version of mutual credit would be storing all the transactions and account balances in a decentralised database like Bitcoin. The easiest way to facilitate transfers between accounts is to use QR-codes. It doesn't require that everybody have a smart-phone and carry it at all times, for example a community could continue to operate in the classic LETS style with paper receipts and then the office accountant could process the receipts through the database on their behalf. Using a decentralised system would also allow some transactions to be done with smart-phones directly and others with receipts without things getting disorganised.

For those unfamiliar with QR-codes, they're basically a modern form of bar-code that look like the example image to the right. It's an open standard so anyone can easily create them, decode them, and incorporate them into their applications. Bitcoin software already uses QR-codes to make its payments much easier.



Fig. 1: An example QR code

For example, if you want to pay for your coffee with Bitcoin in a café that accepts it for payment, you'll see a QR-code on their screen which has their Bitcoin address and the amount of the transaction encoded into it. You simply wave your phone in front of it, check that the amount looks about right, and click "accept", your phone will then broadcast the transaction to the Bitcoin network, and within a second or so the seller sees that payment has been made³. The transaction did not have to be approved or processed by any bank, organisation or central computer, the Bitcoin peer-to-peer network takes care of everything without the need for any kind of central authority.

1. For example see this historical article on the origins of Ripple, "Medieval banking with a digital twist" [<https://www.coindesk.com/ripple-medieval-banking-digital-twist/>]

2. See this article on the Holochain vision for currency at [<https://medium.com/holochain/beyond-blockchain-simple-scalable-cryptocurrencies-1eb7aebac6ae>] and the Holo currency white-paper for more detail: [https://files.holo.host/2017/11/Holo-Currency-White-Paper_2017-11-28.pdf]

3. It takes a lot longer for the network to *confirm* that the transaction is legitimate, but for small transactions like coffees and cell phone top ups, *unconfirmed* transactions are usually accepted since even creating a fraudulent unconfirmed Bitcoin transaction is extremely difficult and only worth the trouble for large transactions. For average transactions three confirmations are normally wanted, and six for large transactions.

When someone wants to purchase some goods with *trustless mutual credit* the process would be similar; the seller would present the sale with an associated QR-code to the buyer, who then acknowledges receipt of the goods and authorises the debit from his account by scanning the QR-code on his smart-phone and selecting “accept”. The transaction encapsulates the two necessary aspects of mutual credit money:

- The seller has backed it for value by creating the transaction to indicate his acceptance of the mutual credit money in return for his produce.
- By scanning the QR-code and clicking “accept”, the buyer indicates that he’s received the goods and confirmed the details of the transaction are correct, and so has authorised the transfer of credit from his account to the seller’s.

Note that in this example it was the seller who initially created the transaction, but it could have been created by the buyer – or indeed by anyone. It’s just a matter of a buyer and seller both confirming (which technically means *digitally signing*) the facts about the transaction, that goods have been transferred and that credit will transfer between their accounts in return.

6.2 Printing money

It’s important to remember that money is not simply printed out of thin air like it is in our current fiat-money systems – and unfortunately this is done in many community currencies too, usually resulting in their collapse shortly after. In *Section 4.2* I discussed how paper money is merely another form that already existent account balances can take. In this section I’ll give a basic description of how this paper money aspect could be implemented in a trustless mutual credit system.

In a trustless system any member can print their own money! They simply select the denominations they wish to print and as long as they have enough available credit in their account, they can *withdraw* balance into a paper money form. Each withdrawn and printed note would have a unique QR-code on it that proves the note represents an authorised deduction from the member’s account balance. Anyone could scan the QR-code and see when it was created, and whose account it had been deducted from.

Having credit-money in paper form means it can be exchanged easily without the need for technology, and can be used by people who don’t have accounts in the system. There’d be no need to scan paper notes during every physical exchange for validity, but a general practice to scan money sometimes would be advisable to ensure that counterfeiting would always remain very unlikely.

7. Reputation & Group decision-making

Two concepts which are fundamental to a community in order for it to manage itself are a **reputation system** and a **group decision-making system**.

As we can see from all the successful online market places from the early ones such as *eBay* and *Craig's List* to the modern examples of the “sharing economy” such as *AirBnB* or *Task Rabbit*, a reliable reputation system is an essential ingredient. Without the ability to build trust there simply is no community, because the fundamental relationship connecting the members is *trust*. That's why I've simply called the communities that compose the trustless mutual credit network “trust groups”.

If the community wants to govern itself, then a reliable means of *group decision-making* is just as important as a reliable reputation system. The community needs to have a process by which they can arrive at objective information about the best courses of action available to them, who the stakeholders are and who's for, who's against, and why.

I've deliberately left out details about these two important topics herein because, while I believe they're critical to the successful execution of a trustless mutual credit system, they're outside the scope of this short paper which is focused solely on the credit mechanism itself.

However I'm writing another paper now that's specifically focused on the group decision-making aspect, and I'll be joining all these concepts together with a reputation system in “*The Libre Society Foundation Ontology*” [8], paper which is also in progress now.

8. What can we do now?

This text has talked mainly about an idea that we'll likely see in the near future, but what can a community do now?

The best thing to do is to begin working with a normal mutual credit system like LETS. The most important aspect of a community currency (which mutual credit does very well) is to *encourage exchange* and expansion of use of the money.

Getting familiar with using a community currency and understanding the mutual credit concept is the best preparation you can do for integrating trustless mutual credit solutions when they become available. Using a mutual credit system that's smart-phone based will help the transition go more easily too.

For a more in-depth look into this subject, I recommend reading the paper that this booklet was derived from: *Trustless Mutual Credit* [9]. It exposes key concepts to operate a trustless mutual credit system in a precise and balanced way, for example not just arbitrarily printing money every time some runs out as many communities are doing.

9. Conclusions and further work

I've covered here the reason why a mutual credit would be a better form of money for facilitating a society's day to day exchanging needs, and the attributes this money would need to exhibit in order to be made into a trustless global protocol.

This system relies on a decentralised design, not only by the fact that the trustless system itself is decentralised, but also by the way the communities (trust-groups) are structured and interact together to form a whole holistic system.

This booklet is a preliminary text that forms a foundation for another forthcoming paper called "*The Libre Society Foundation Ontology*" [8], which describes how the decentralised structure introduced herein could form the basis for a holistic social mechanism whereby all the trust-groups composing the system are formed from two aspects: *Governance* and *Economy*. This present paper is an introduction to the form that money takes in the *Economy* aspect of the *Libre Society* concept. Another introductory paper will be written shortly that covers the *Governance*, or group decision-making, aspect in more detail.

For those interested in further reading and learning about these concepts, have a look at the references listed in the next page, which also includes some excellent documentaries about money and the financial system.

References

- [1] Clifford Hugh Douglas, “Social Credit”, 1927
<http://douglassocialcredit.com>
- [2] E. C. Riegel, “Private Enterprise Money”, 1944
- [3] G. Edward Griffen, “The Creature from Jekyll Island: A Second Look at the Federal Reserve”, 2002
- [4] James Taris: “The LETSaholic Twist”
<http://www.jamestaris.com/ebook-TheLETSaholicTwist.htm>
- [5] Andreas M. Antonopoulos: “Mastering Bitcoin: Unlocking Digital Cryptocurrencies”, 2014
<http://www.mises.org.br/Ebook.aspx?id=99>
- [6] Satoshi Nakamoto: “Bitcoin: A peer-to-peer electronic cash system”, March 2009
<https://bitcoin.org/bitcoin.pdf>
- [7] Bernard A. Lietaer, “Community Currencies: A New Tool for the 21 st Century”
<http://www.transaction.net/money/cc/cc01.html>
- [8] Aran Dunkley: “The Libre Society Foundation Ontology”
<https://www.organicdesign.co.nz/writing>
- [9] Aran Dunkley: “Trustless Mutual Credit”
<https://www.organicdesign.com.br/writing>

Documentaries

Here are some excellent documentaries about money and the financial system.

[1] **The Four Horsemen**

A documentary about the current state of our social mechanism, how it got this way, how capitalism and democracy were meant to work and how we could change it.

<https://youtu.be/5fbvquHSPJU>

[2] **The Inside Job**

A must-see documentary showing how the financial system has gotten into the corrupt state it's in now by taking over government and corrupting the law, ratings institutes and educational system.

<https://youtu.be/5nCvO6qEbJw>

[3] **The Money Fix**

Money is just information, a way we measure what we trade, nothing of value in itself. And we can make it ourselves, to work as a complement to conventional money. It's just a matter of design.

<http://topdocumentaryfilms.com/money-fix/>

[4] **The Hidden Secrets of Money**

Mike Maloney from goldsilver.com uncovers the mysteries of money and explains the details of the greatest transfer of wealth in human history and how to survive and even prosper from it in this seven part series.

<https://youtu.be/DyV0OfU3-FU> (Part 1 of 7)

[5] **The Secret of Oz**

The world economy is doomed to spiral downwards until we do two things: outlaw government borrowing and outlaw fractional reserve lending. Banks should only be allowed to lend out money they actually have and nations do not have to run up a "National Debt". Remember: It's not what backs the money, it's who controls its quantity.

<https://youtu.be/swkq2E8mswI>

[6] **The Money Masters**

An educational documentary about the fractional reserve banking system; a subject around which discussion is usually heavily obfuscated due to its foundation in fraud.

<https://youtu.be/B4wU9ZnAKAw>

Money is one of the most commonly spoken words: everyone talks about money and spends much of their lives struggling for it. But what is money? How is it made? Does it need to be scarce? What is the function of money? Has it fulfilled this function? What is the relationship between money, corruption, wars, environmental degradation, competitiveness and extreme social inequality?

This text responds simply and directly to each of these questions and offers us a solution that can only be realized nowadays, with the new technologies of the peer-to-peer network and the cryptography.

“This artificial scarcity of fiat-money means there’s never enough of it where it’s needed, and too much of it where it does harm to society and the environment. It’s the fundamental reason that our society is competitive instead of cooperative, and is the main reason why billions of people around the world, both in poor and affluent areas, are struggling to make ends meet.”

“The strong encryption we have today is accessible to nearly everyone on the planet, and yet is unbreakable even by the state. This encryption gives us our “claws”, and used in the right way it can provide, for the first time in history, a practical solution to corruption in the mechanisms of our society.”



This work is licensed under a

Creative Commons Attribution-NoDerivatives 4.0 International License

(You are free to copy and redistribute this work in any medium or format provided it is not modified, given appropriate credit and is not used commercially)