



Biom: A Biometric Currency A new approach to banking

Charaf Ech-Chatbi

► To cite this version:

| Charaf Ech-Chatbi. Biom: A Biometric Currency A new approach to banking. 2020. hal-02975798

HAL Id: hal-02975798

<https://hal.science/hal-02975798>

Preprint submitted on 23 Oct 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Biom: A Biometric Currency

A new approach to banking

Charaf ECH-CHATBI *

Sunday 20 September 2020

Abstract

Our modern financial system traces its origin to the ancient Babylonian banking system. The same fractional lending idea that is used today was used by merchants in the regions of ancient Babylonia, Assyria and Sumeria around 2000 BC. Later, the idea found its way to ancient Greece, the Roman Empire, China, India and then to us. The fractional lending concept was not the fruit of scientific research like what is done in other scientific endeavors where most of the best ideas are the result of a long process of trial and error. Is it not time to rethink the way we do banking in this digital age and try other ideas?

The last 40 years of cryptographic research culminated with the creation of Bitcoin currency system in 2009. We would like to expand on this and introduce three ideas to help rethink the banking system of the 21st century: 1) the concept of a biometric currency, 2) the concept of being your own bank and issue your own loans with zero-interest rate 3) and redefining the fractional reserve lending.

We propose a biometric currency concept that will enable people to self finance and to safely store their money in their hands. Contrary to cryptocurrencies that are issued by blockchain miners and Fiat currencies that are issued by bankers, Biom will be issued by everyone. The goal is to create from human life a precious asset like Gold that will benefit all.

Keywords: Biometric Currency, Fractional Reserve Banking, Bitcoin, Cryptocurrency, Digital Currency, Banking System, Fractional Lending, Quantitative Easing.

*One Raffles Quay, North Tower Level 35. 048583 Singapore. Email: charaf.chatbi@gmail.com. Twitter: @_sharaf_. The opinions of this article are those of the author and do not reflect in any way the views or business of his employer.

1 Introduction

1.1 Motivation

The idea of Biom came to us from Bitcoin[6]. Over the last 11 years, we saw the raise of many cryptocurrencies[5, 6, 7, 8, 9]. Bitcoin uses cryptography to create a digital scarcity. Biom will use biometric technology to create an alternative digital scarcity.

Bitcoin limitation 1: Bitcoin experiment showed that it is difficult for the common people to understand its working. And many of those who were adventurous lost their money through wallet thefts, exchange hacks and other fraudulent schemes[11, 12, 13]. If one loses his/her private key, the coins are lost forever. There is no recovery mechanism which is unfair for people to bear such a burden.

Bitcoin limitation 2: Bitcoin created through a process called mining. A bitcoin is created as a reward for the miner who is the first to resolve a hard cryptographic puzzle. The mining process in the early stages is not computationally expensive as in the later stages. Satoshi Nakamoto, the inventor of Bitcoin, was alone able to mine over 1.1 million of Bitcoins. Today, the same amount cannot be mined by most sophisticated miners. The early entrants had huge advantage over the late entrants. This is also unfair for a system that claims to free mankind from an unfair banking system. This was also one of the reason why Bitcoin was accused of being a pump and dump scheme[11].

However, on the technological front, Bitcoin blockchain is probably the most significant invention[14] since the Internet. Bitcoin invention showed that people are looking for new ways of doing banking.

Today, Gold coin is mined by mining companies. Bitcoin is mined by blockchain miners. And Fiat currencies are created by bankers. In all these forms of money creation, the common man is excluded.

Now, how to create a digital currency that 1) includes all people in equal manner in the money creation and 2) has a recovery mechanism in case of loss of keys and 3) at the same time it is not particularly attractive to criminal activities?

While trying to answer this question, we had the idea of creating a Biometric Digital Asset where its Biometric coin, that we call interchangeably Biomcoin or BMC, will be created by everyone including the common man in fair manner. In order to answer this question, we asked ourselves what is the thing that everyone has and at the same time it is scarce and precious? One answer to this question is: Human Life. Everyone alive has it and Human Life is scarce and precious. Not everyone can mine Gold. Not everyone can mine Bitcoin. Not everyone can be a banker and create Fiat currency. But everyone alive has a life in him/her. So everyone will be able to create Biomcoin. The idea of Biom is to create an asset that is inherently linked to human life. The goal is to make from human life a precious asset like Gold, Real Estate, Commodity, etc. And then put this asset into service for man. The more strong the currency, the more everyone will benefit from it. One can consider his/her investment

in Biom as a way to give back to the society. In fact, by owning and using Biom, you will help the currency to become a good store of value and therefore spread the wealth to everyone. The potential of such an asset is great. Contrary to Bitcoin that is held by a relatively small number of sophisticated investors, Biom, by design, will be held by everyone, which will enable everyone to have a strong vested interest in it, and this in turn will make Biom an attractive store of value.

The issuance of Biom will be based on biometric technology and the cryptographic digital signatures. The Biomcoins will be issued to a person only if the system is able to uniquely identify him/her biometrically. The biometric technology besides that it will drive away the criminal activities, it will secure the issuance of Biom: every coin will be associated with a unique and traceable person. The use of biometric technology will make Biom naturally compliant to the standard of compliance set by the different banking regulations. And this will help its integration within the banking system and help speed its adoption.

1.2 Centralized versus decentralized mode

Nakamoto wrote about Chaum's eCash[1]: *a lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990s. I hope it's obvious that it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system.* Nakamoto clearly linked the failure of eCash to the fact that it was built around a central authority. A great example of a government intervention against a competing currency system is E-gold¹.

The historical truth is that the money creation is a highly sensitive matter. And for any new coming currency technology, the risk of it disappearing is real. It is not an Uber versus Taxi corporation type of competition. This makes the decentralized mode as probably the only possible option² to effect change in the way we do banking today. If Bitcoin was built around a centralized authority, there likely wouldn't be any cryptocurrency today. Along the same lines, Y. Elmandjra[18] expands further in "Bitcoin: A Novel Economic Institution" on why the trust-based model falls short.

1.3 Why Biometric Technology

Can the same objective be achieved without using Biometric Technology?
We can actually implement a recovery mechanism for the lost coins with-

¹E-gold[10] was a digital gold currency that allowed users to open an account denominated in grams of gold and the ability to make instant transfers to other e-gold accounts. In 1996, E-gold built the first internet payment network before PayPal. E-gold originality was that it was built outside the banking system while PayPal was built on the top of the banking system. At that time, Internet was new and many internet-based payment services, including PayPal, operated without license. In December 2005, FBI agents raided E-gold offices and the whole E-gold system collapsed.

²Nakamoto wrote Bitcoin paper during the same period of the highly publicized trial of E-gold and its CEO Douglas Jackson, July-November 2008. This is probably why he wrote it under a pseudonym.

out using a biometric technology. However, the great benefit of using a biometric technology is that users won't even need to remember their passwords. The users money will be literally "stored" in their fingers, Irises and facial features. This will resolve the dilemma of either storing your private keys with an exchange³ and being exposed to the exchange risk or storing them at home and being exposed to your own risk of misplacing them. The other great benefit of a biometric technology is for the system to be able to uniquely identify users even if they use multiple cryptographic keys. This feature is needed to avoid the system from being exploited as all users will need to repay their loans in schedule and, in general, it will enable the system to eliminate any bad behavior including from suspected nodes and super nodes. Plus, the biometric technology is a natural deterrent to criminal activities. So, this will help create a safe environment around the currency.

2 Biom Currency

2.1 User registration

2.1.1 Biometric Data Registration

The user will need to supply his or her biometric data to the biometric recognition technologies like:

- Fingerprint recognition technology.
- Facial recognition technology
- Iris recognition technology.
- Finger vein recognition technology.
- Other robust biometrical technologies.

The goal of the registration step is to uniquely identify the user and register him or her in the BMC database (BMC Bank).

2.1.2 Safety of Biometric Data

Biometric data will not be stored in its original form. What will be stored in BMC Bank is an encrypted version of the original biometric data.

2.2 Biomcoin creation

2.2.1 Issuance model

The biomcoins will be created according to the following rule:

- *Each user in BMC Bank will receive X coins every Y days during a period of Z years starting from his/her registration date.*

³The case of Mt.Gox exchange [12] and many other similar cases showed that it is not safe to store your private keys with an exchange. It is also unsafe to store them at home as the risk of misplacing them is quite high.

Where X is the number of coins, Y is the frequency of distribution. Y can be one day, one month or any number of days. Z is the biomcoin issuance period. X, Y and Z are model parameters that can be adjusted according to money supply needs.

2.2.2 Default issuance model

In a daily model where $X = 1$, $Y = 1$ and $Z = 100$. The user can expect to receive 36500 units of BMC if the issuance model remains the same during the whole 100 years' period. The table 1 shows some examples of issuance models.

Table 1: Issuance models for $Z = 100$ years period. The table displays the number of biomcoins issued to each user for each configuration of X and Y.

Y/X	Day Y=1	1M Y=30	6M Y=182	1Y Y=365	100Y Y=36500
$X = 1$	36.5k	1.2k	200	100	1
$X = 0.1$	3.65k	120	20	10	0.1
$X = 10$	365k	12k	2k	1k	10
$X = 100$	3.65m	120k	20k	10k	100
$X = 250$	9.125m	300k	50k	25k	250

In 2019, the Money Supply M2 of the world reached US 90.6 trillion[15]. If Biom were to only capture 10% of that, Biom system would need to issue 9.06 US trillion. If we assume that BMC Bank has 7 billion users like the size of the world population. And If we want to create the equivalent of only 8.4 trillion biomcoins, Biom system will need to issue 1200 biomcoins to each user. Which is equivalent to issue 5 biomcoins monthly to each of 7 billion users for a period of 20 years. Based on this conservative⁴ scenario, we suggest the default issuance strategy for Biom to be the following:

- *Each user will receive 5 biomcoins monthly for a period of 20 years from the date of his or her registration.*

2.3 How Biom works

We designed Biom to work for both modes: Centralized and Decentralized.

2.3.1 Centralized mode

The central BMC Server will manage and update user accounts, issue and recover biomcoins and BMC transaction tasks: verification, approval, cancellation, rejection, double spending, transfer, etc. The BMC Server and

⁴Because in 20 years from now, the world M2 money supply will probably double or even triple thanks to all the stimulus packages introduced by countries around the world in response to COVID19 economic lockdown.

database will have replicas and redundancies distributed in different countries across the globe to guarantee great safety of database, continuous and reliable service and minimize operational risk.

2.3.2 Decentralized mode

This is the default mode. For performance and low-cost energy reasons, this mode will be based on an approach similar to AT2 model developed in 2009 by R. Gerraoui and his team[20, 21, 22]. During this mode, new biomcoins will continue to be created as BMC Bank will be distributed and users will still be able to be biometrically identified even if they possess multiple cryptographic keys. The issuance of biomcoins is uniquely associated with the biometric digital identity and not the cryptographic keys. A user can have multiple cryptographic keys but only one unique biometric identity. The BMC backup servers will play the role of the super nodes like in Bitcoin blockchain.

In theory, this mode should be used only when the centralized mode can no longer work safely. However, in practice, Bitcoin experiment showed that this mode is essential⁵ for the currency survival. The great news is that with AT2 breakthrough we can achieve safe transactions on a large scale and with low energy cost. “roughly equivalent to that of exchanging emails” said Professor Guerraoui in an interview. This makes the centralized mode not needed.

2.4 How to recover the lost biomcoin

Chainalysis⁶ found that around 20% of all Bitcoin is missing. The most common issue that leads to lost Bitcoin is the loss of access to the wallet by forgetting the seed or misplacing the private key. Since Bitcoin works in decentralized mode, no one can re-issue the lost bitcoins to their owners.

To resolve this issue we make BMC database also distributed. Every public key belongs to a unique biometric identity. The lost biomcoin will be added to the Deadcoin database and a new biomcoin of equivalent value to the lost biomcoin will be issued to the owner with a new pair of key or with one existent key of the owner. The Deadcoin database will also be distributed to avoid spending the declared lost biomcoins.

2.5 Anonymity

Biom anonymity is not as absolute as Bitcoin anonymity. As example of an extreme case scenario, we can imagine a government order to identify individuals who hold biomcoins. In such scenario, individuals will be forced to share their biometric digital identity and hence being able to be

⁵With a centralized mode, Biom system is vulnerable to interventions from governments and targeted attacks from competing groups and hackers. History is full of lessons[18] where corporations intervened against their competition. For survival reason, the decentralized model is essential. Like what has happened with Uber versus Taxi corporation, similar resistance to change is expected from the traditional banking corporation. The struggle that Bitcoin went through and the disappearance of its inventor S. Nakamoto is a great example.

⁶A blockchain analysis firm based in New York City

identified in BMC Bank. However, such a scenario is unlikely for most transactions. For criminal transactions, users will most likely prefer using Bitcoin as Biometric technology will be a natural deterrent to them.

To strengthen the anonymity, an additional PIN code of less than 6 digits can be used to create different biometric identities of a user and avoid him or her from being easily linked to identifiable transactions.

3 Redefining the fractional reserve banking

3.1 Being your own bank and Zero-interest rate

Much like Uber that enabled everyone to become a Taxi driver. And Amazon that enabled everyone to become an online seller and a self-publishing author. And Youtube that enabled everyone to create their own TV Channel. Today, we think that everyone should be able to be his or her own Bank. Everyone should be able to issue his/her own loans and at least be able to self finance his/her housing, education and issuing his/her personal loan.

If I want to buy a house, I should be able to issue my own loan⁷ and finance my house purchase. The possibility of issuing one's loan and then work to pay the loan off is an empowering tool. In such a system, I feel like I am working for myself and not for the banks. The small fee⁸ paid on the loan will be the fee to pay⁹ to verify my ability to create my own money like what the banks are doing today with credit scores. This will empower people instead of letting them feel that banks owe them something.

Today, banks are creating money out of thin air thanks to their license. We propose that this "out of thin air" action to be extended to individuals to empower them. The feeling to be able to finance oneself is empowering while the feeling of having to go to a bank is not empowering as it creates a feeling of lack within oneself.

3.2 Fractional reserve lending

3.2.1 Money creation with guarantors

In Fiat currency fractional reserve banking¹⁰, banks accept deposits from customers and makes loans to borrowers while holding in reserve an amount equal to a fraction of the bank's deposits. Bank reserves are held as cash

⁷Own loan is a loan with zero interest rate.

⁸This is different from the concept of interest rates used in today banking system. However, this is equivalent to have a loan with zero interest rate which is a real need for many religious communities like the case with some christian, jewish, and muslim communities that are struggling to reconcile an interest-based economy with their religious laws that reject usury[17].

⁹The loan fee will be paid to Biom Bank in the case of the centralized mode. In the case of the decentralized mode the loan fee will be paid to the blockchain node that validates the loan transaction with the list of guarantors and the needed reserve from each guarantor.

¹⁰The fractional lending idea was a trade secret for many merchant families throughout history from the house of Egibi in Babylon, to the house of Medici in Medieval Italy, and to the house of Rothschild in Victorian England.

in the bank or as balances in the bank's account at a central bank. The central bank determines the minimum amount that banks need to hold in liquid assets, called the "reserve ratio". Banks usually hold more than this minimum amount, keeping excess reserves.

In Biom banking system, the currency is issued directly to the general population. Therefore, we propose that individuals themselves make loans to banks, businesses and individuals while holding in reserve an amount equal to a fraction of the amounts lent. This will keep the general population more involved in businesses and this in turn will create a more resilient economy.

The Biom Policy (code) will determine the minimum amount that individuals need to hold in reserve. For all loans, individuals will need a list of guarantor(s)¹¹ to guarantee the loan repayment in order to be able to create money for their loan. The number of guarantors is not limited. So, an individual may use as many as he/she wants of guarantors to secure his/her loan. And guarantor(s) will need to hold reserve against the amount guaranteed in loans. In case of a loan default, each guarantor(s) will need to pay the guaranteed amount, otherwise his/her(their) credit score(s) will be affected. In an worse case scenario, an individual maybe banned from using Biom banking services.

In practice, the loanee, the person who receives the loan will provide the guarantor list.

Case study : Let's take a user with a deposit of 1000. Let's assume the reserve ratio is 10%. The user can lend up to $\frac{1000}{10\%} = 10000$. Now imagine, if the user can lend all his 10k to his bank at 1%. The user can get $10\% * 10000 = 1000$. Which is 10% of his initial deposit. In today fractional reserve lending, the banks are paying 1% on the deposit 1000 and not the amount lent 10000. Which is 10. There is a factor of 10 between the two systems.

A company can be viewed as a group of individuals (company executives) who run the business. Therefore, a company can also issue its own loan as long as its executives are in the list of the loan guarantors. An executive may leave a company but his or her credit score will stay with him or her. So, including company executives in the guarantor list will make them have more skin-in-the-game and therefore being more accountable.

3.2.2 Guarantor list concept

The concept of guarantor list will resolve the subjectivity issue in the process of loan issuance. Today, in the business loan area, if you have a good connection or a good family name, your business loan can be approved easily. However, if your name is obscure, then you will need to prove yourself to the bank in order to get your loan approved. With the concept of guarantor list, if you want a loan, you will need to ask people in your network to guarantee you and then your loan can be approved in less than 1 minute in the system. No need to prove that you studied in

¹¹This is equivalent to a syndicated loan with zero interest rate in the traditional banking.

a good school or your father is a rich man. No need to show payslips or bank statements.

4 Conclusion

The idea behind Biom is not to create yet another currency alongside the 200+ Fiat currencies and 1500+ cryptocurrencies. The currency ecosystem is well established and serve well its many purposes.

The Fiat currency system with its different variants and metal based money were and still are the dominant forms of money since the ages. However, since 2009 things have changed, Bitcoin[6] proposed a cryptographic form of money and started the cryptocurrency movement.

We have proposed a concept for a biometric form of money. We have proposed an empowering alternative form of money creation and offered an opportunity to rethink the way we do banking in the digital age, in ways that can be more empowering for individuals and businesses alike.

A Appendix

A.1 Open Question

How to lend money in a non trust-based model like Bitcoin ?

A.2 Biom Money Supply and Inflation

The way to create new coins is by 1) adding new users to BMC Bank, or/and 2) adjusting X, or/and 3) adjusting Y, or/and 4) adjusting Z.

If there is no new user addition to BMC Bank, the rate of Biomcoin creation is fully controlled by the parameters X, Y and Z. The money supply can then be adjusted through the parameters X, Y and Z.

The rate of population increase is less than 1.1%, therefore an inflation rate of 1.1% is to be expected. In contrast, the rate inflation in gold is around 1.35%, as the yearly Gold production rate is around 1.35% of the total gold over ground in the world. Therefore, under constant issuance policy, Biom will protect against inflation better than Gold.

A.3 What is the intrinsic value of a Biomcoin?

When speaking about the intrinsic value, people always speak about the precious metals and other commodities. The argument is that the precious metals like Gold and Silver are used as jewelries and also in other industries. So their intrinsic value is their usefulness.

What is the intrinsic value of a thing like Bitcoin? Contrary to Gold and Silver, Bitcoin has no value of itself. However, Erik Voorhees in debate with Peter Schiff[16] argued that today Bitcoin has a good network. And this network in itself is the intrinsic value. Schiff argued that such

networks can disappear quickly and gave the example of Myspace that once had a big network and nevertheless got replaced by Facebook.

So, what is the Biomcoin intrinsic value?

Biom, by design, will be held by everyone at any time. People will receive coins over their life time. This will enable everyone to have a strong vested interest in it.

So the Biom intrinsic value is the value that it creates for all people and its ownership by everyone at all time.

A.4 What is the potential monetary value of a Biomcoin?

In this paragraph, we will assume that $X = 1$ and $Y = 1$. Every user will receive 1 Biomcoin daily.

To estimate the potential value of Biomcoin, we will use the world population number and the global median average age.

The United Nations estimated the global median age to be 30.4 years for 2019 and the world population of 7.8 billion as for September 2020.

Therefore, the total number of Biomcoins is:

$$30.4 * 365 * 7.8 * 10^9 = 86.54 \text{ trillion} \quad (1)$$

According to the CIA, the total amount of money in circulation in the world in 2017 was USD 80 trillion. This includes broad money. In 2019, this amount raises to USD 90.6 trillion[15]. So, we can estimate the value of BMC to be¹²

$$\frac{90.6}{86.56} = \text{USD } 1.04 \quad (2)$$

If we count the value of the world investments and derivatives, the world wealth can be estimated to USD 1.2 quadrillion. Based on this, a Biomcoin is valued at

$$\text{BMC } 1 = 1.2 * \frac{1000}{86.54} = \text{USD } 13.86 \quad (3)$$

The Biomcoin value will ultimately be determined by market forces.

References

- [1] D. Chaum. *Blind Signatures for Untraceable Payments*, 1983.
- [2] T. Okamoto et al. *Universal Electronic Cash*, 1991.
- [3] T. Okamoto. *An Efficient Divisible Electronic Cash Scheme*, 1995.
- [4] L. Law et al. *How to Make a Mint: The Cryptography of Anonymous Electronic Cash*, 1996.

¹²For instance, we can approximate the value of BMC by the minimum amount of money needed for a person to survive in a day. According to Business Insider, about 1.1 billion people in the world survive on just 1 USD a day. 1 USD a day is a lower bound even by third world standard. In USA, the amount one needs for daily food is 10 USD.

- [5] W. Dai. *B-money* <http://www.weidai.com/bmoney.txt>
- [6] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.
- [7] V. Buterin. *A next-generation smart contract and decentralized application platform*, 2013.
- [8] S. Siddiqui et al. *BitcoinF: Achieving Fairness for Bitcoin in Transaction-Fee-Only Model*, 2020.
- [9] Nick Szabo. *Bit Gold* <http://unenumerated.blogspot.com/2005/12/bit-gold.html>
- [10] Kim Zitter *E-Gold* <https://www.wired.com/2009/06/e-gold/>
- [11] Bill Harris. *Bitcoin is the greatest scam in history* <https://www.vox.com/2018/4/24/17275202/bitcoin-scam-cryptocurrency-mining-pump-dump-fraud-ico-value>
- [12] Wikipedia. *Mt. Gox* https://en.wikipedia.org/wiki/Mt._Gox
- [13] Akshay KS. *Biggest Ponzi Schemes in the History of Crypto* <https://eng.ambcrypto.com/biggest-ponzi-schemes-in-the-history-of-crypto/>
- [14] Marc Andreessen. *Why Bitcoin Matters* <https://a16z.com/2014/01/21/why-bitcoin-matters-nyt/>
- [15] Varun Kumar. *How Much Money Is There In The World* <https://www.rankred.com/how-much-money-is-there-in-the-world>
- [16] Peter Schiff, Erik Voorhees *Is Bitcoin the Future of Money? Peter Schiff vs. Erik Voorhees* <https://www.youtube.com/watch?v=q8R71WGO3qU>
- [17] Wayne A.M. Visser, Alastair McIntosh. *History of Usury Prohibition* http://www.alastairmcintosh.com/articles/1998_usury.htm
- [18] Yassine Elmandjra. *"Bitcoin: A Novel Economic Institution ARK Invest*
- [19] Chainalysis Team. *60% of Bitcoin is Held Long Term as Digital Gold. What About the Rest?* <https://blog.chainalysis.com/reports/bitcoin-market-data-exchanges-trading>
- [20] Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, Dragos-Adrian Seredinschi *AT2: Asynchronous Trustworthy Transfers*
- [21] Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, Dragos-Adrian Seredinschi, Yann Vonlanthen *Scalable Byzantine Reliable Broadcast*
- [22] Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, Dragos-Adrian Seredinschi *The Consensus Number of a Cryptocurrency*