**American Journal of Computer Science and Technology**
2020; 3(3): 46-56
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20200303.12
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

# Study in View of Development of a National Cryptocurrency

**Georges Bell Bitjoka[1], Bouetou Thomas[2], Ferdinand Yves Mbarga[2]**

[1]Department of Telecommunications, National Advanced School of Engineering, University of Yaoundé I, Yaoundé, Cameroon

[2]Department of Computer Science, National Advanced School of Engineering, University of Yaoundé I, Yaoundé, Cameroon

**Email address:**
georges@bellbitjok.com (G. B. Bitjoka), mbargayves@gmail.com (F. Y. Mbarga)

**To cite this article:**
Georges Bell Bitjoka, Bouetou Thomas, Ferdinand Yves Mbarga. Study in View of Development of a National Cryptocurrency. *American Journal of Computer Science and Technology*. Vol. 3, No. 3, 2020, pp. 46-56. doi: 10.11648/j.ajcst.20200303.12

**Received**: June 19, 2020; **Accepted**: July 9, 2020; **Published**: July 23, 2020

**Abstract:** The study of cryptocurrencies doesn't clearly propose different approaches that provide cryptocurrency development. The purpose of this paper is to determine approaches to cryptocurrency development, in which we select one to develop a national cryptocurrency that will be able to bring out Cameroun from CFA Franc. Developing a national cryptocurrency or bringing out Cameroun from CFA Franc is a monetary issue which is generalized in the problem of commodity exchange. This problem focuses on how to exchange goods and services while ensuring stakeholder satisfaction. To this end, after a brief literature review on the commodity exchange system, money and Bitcoin, we first explored possible approaches to the development of cryptocurrencies. The study in these approaches has enabled us to determine four different solutions: firstly by token development, secondly by hard fork development, thirdly by fork of source code development, and at last by fork of software development. For each approach, we make a summary presentation which lists its stages of development. The comparison of these approaches in terms of development time, development cost dependence on a blockchain platform and solution to exit from the CFA Franc led us to choose fork of software approach. The fork of software approach of cryptocurrencies development best solves our problem, since it offers us a cryptocurrency development solution, but also proprietary currency which is independent of blockchain platforms. Fork of software is a fork approach that observes behavior of existing software, in view to implementing it again and/or customizing it. We proposed an explorative development method which combines: the iterative and incremental method with evolutionary prototype, for application of the development approach retained above.

**Keywords:** Commodity Exchange System, Currency, Cryptocurrency, Bitcoin, Cryptocurrency Development Approach

## 1. Introduction

Since its creation in 1945, the CFA Franc has long been in controversy in the fifteen African countries engaged in a monetary union with France namely the CFA Zone. This monetary union sets: monetary integration, currency convertibility through Euro, and fixed exchange rate. The CFA Franc certainly offer advantages, however many Africans disapproving it and maintain an ardent debate around it. Numerous acts illustrated that, this currency is not acclaimed by all: at the political level, economical level, historical level and in the same way as at diplomatical level. At the diplomatical level for example, the Italian prime ministers have vigorously criticized France which imposes this currency with consequences of migratory flow from Africa to Europe and Italy pays a heavy price [1]. The announcement of Eco, the new currency in CEDEAO countries is the last highlight, that auspicious his dead end, while France plans to adopt law that will abolish it. This law will revise the monetary agreement between France and the West African Monetary Union (WAMU) countries. The new agreement transforms the CFA to Eco, excludes France from sitting in technical governing body of the monetary area; and makes optional the deposit by BCEAO of at least 50% of its foreign exchange reserves in French treasury operations accounts. But, this agreement renews the fixed parity of the Eco with the Euro and the guarantee of convertibility ensured by France [2].

Confinement related to the occurrence of COVID-19 relief the importance of the digital economy, which use not just

electronic services, but also digital currencies or even cryptocurrencies. In fact, the world is moving towards the all-digital through the effectiveness of the digital economy and digital payments. Cryptocurrency is a boon that will allow Cameroon to realize its ambition to develop digital economy. Moreover, it will also make it possible to send the exit of Cameroon from the CFA Zone, whose central African countries are visibly excluded from the recent bill for its abolition in France. Since France is not playing fair and the exit of the CFA Franc by Cameroon is for the moment a dead end, how could our country leave the CFA zone while escaping a new monetary agreement with France? Answering this question amounts to proposing an exchange model, choose in commodity exchanges systems, or proposing a new currency for Cameroun. However, the monetary system itself is not exempt of reproach as declared by Bernard Lietaer: "while these particular features of our money system have permitted the accumulation of capital that enabled rapid industrialization during the modern era, they also have a number of hidden but far-reaching counterproductive side effects" [3]. This is what motivated the forerunners of digital asset and Satoshi Nakamoto, creator of Bitcoin and cryptocurrency.

Can cryptocurrency free Cameroon from the CFA Franc? If so, how can we develop cryptocurrency? This manuscript deals with a study in view of the development of a national cryptocurrency. Our interest will remain focused on the technical aspect of cryptocurrency; we will propose an approach to the development of cryptocurrency with the ambition of developing it for Cameroon.

# 2. Background and Related Works

### *2.1. Problem Statement*

Proposed a solution to exit Cameroon from the CFA Franc currency also refers to offer a means of exchange to economic agents. This problem is generalized as the problem of commodities exchanges. Then, what is the exact meaning of commodities exchange? It results from the incapacity of a man to satisfy or produce all requirements necessary for the satisfaction of his needs. In fact, the market constitutes the meeting point of needs, in which economic agents exhibit their productions and proceed to the exchange of goods and services. Hence, the problem of meeting needs is also the problem of exchange medium. Different commodity exchange models are used to solve that problem, which we have classified into three exchange system: direct system, indirect system and semi-direct system.

### *2.2. Systems of Commodity Exchange*

#### *2.2.1. Direct System*

The direct exchange system refers to transactions in which no third object is used, between the involved parties. This exchange system uses only barter system, which indicates system by which one commodity is exchanged for another without use medium. Barter refers to direct exchange of goods and services [4]. Realized in primitive societies, barter is possible when market is limited and needs too. Participants must have reciprocally desired goods and require double coincidence of wants. This is why Jevons says barter, is not only the exchange of goods against goods, but rather the exchange of reciprocally desired goods, so barter requires double coincidence of wants [5]. This exchange system has certain limits that Siddiqui enumerate in five points: lack of double coincidence, lack of divisibility, lack of measure of value, problem of store of value and lack of standard of future payments [4]. The barter remains anon-equilibrium system, in view of its limits above. Thus, the barter system gave way to the indirect system.

#### *2.2.2. Indirect System*

Indirect system indicates exchange model which media or third object is use, between parties. Commonly, indirect commodity exchange system is monetary system. Siddiqui defines money as medium of exchange, measure of value, store of value and transfer of value. The features of money are: forms (classification), functions and roles [4]. These characteristics have been developed in history in parallel with the development of man and the need to adapt money to the constraints of modernism each time. The indirect exchange system remains today the exchange system best suited to market exchanges. The success of the indirect exchange system through the money economy was not enough to definitively overcome barter and is not without reproach. The criticisms leveled at the money render its practice in certain markets intosemi-direct exchange system called the Local Exchange Trading System. We will come back to money especially in detail in sub-section 2.3.

#### *2.2.3. Semi-direct System*

For us, semi-direct exchange system refers to an exchange system which is not direct or indirect. There is one model in this system called Local Exchange Trading System. It's an exchange system which abolishes money and interest, born around 1980 from the criticism of monetary system. It refers to non-profit exchange network where all kinds of goods and services can be traded without money. LETS indicates a group of people who in an associative form and on a local basis, exchange services and goods through a transaction register. Micheal Linton [6] redefined the exchange problem, for which the quantity of goods and services is not lacking in general, but the availability of means of access or payment. He then proposed a solution as a monetary supplement which solves the problems of mobility, scarcity of money and exclusivity of the central bank. It is a local currency which everyone has the right to produce. This model emphasizes on member participation, conviviality, transparency, connection and demonetization. The exchange unit is a means of satisfying the needs of the individual or being more important than the asset, the bond over the good and the gift over the merchant exchange.

Jérôme Blanc and Cyrille Ferraton [7] show that the LETS exchange model is not without criticism. The authors classify the critic of LETS into two categories: internal and external

critics. The reciprocity of exchanges in LETS destroys the market principles of exchanges. Since the exchanges in the LETS are carried out within a group which is closed to other economic agents who wish to have access to the goods and service. There is a risk of self-dissolution and isolation. Indeed, strong binary trust between participants threatens the group, to the point that participants may end up favoring bilateral transactions with the possibility of the risk of group collapse. The absence of interference by other external actors can lead to group isolation. LETS are inappropriate for the current legal framework, because they do not give the possibility of levying fiscal and social rights like any commercial activity. This model is an unfair competition for trade professionals.

### *2.3. Currency*

#### *2.3.1. Literature Review of Currency*

There are various definitions of money. For Jean-Yves Capul and Olivier Garner, Money indicates all the means of payment available to economic agents for settling their transactions [8]. For A. S. Siddiqui, Money refers to medium of exchange, measure of value, store of value and transfer of value. For us, money designates a transaction tool characterized by uniqueness of account, store of value and means of exchange. Siddiqui teaches us about its classification, functions and importance. Siddiqui distinguish five classifications of money: full-bodied, representative full-bodied money, credit money, fiat money and high-powered money, as we can see in table 1.

***Table 1.*** *Classification of money.*

| Classification of money | Description | Example |
|---|---|---|
| full-bodied | Value as a commodity for non-monetary purposes is as great | Gold coins |
| representative full-bodied | Represents in circulation an amount of money with a commodity value equal to the value of money | Paper money |
| credit money | Value is greater than the commodity value of the money's material | Cheques |
| Fiat | Which circulated in the country by the other or fiat of the government | CFA Franc |
| High-powered | Monetary base of the country | Currency |

Money realizes many functions categorized in: primary functions, secondary functions and contingent functions. The primary functions concern medium of exchange and measure of value. Secondary functions are store of value, standard of deferred payments, and transfer of value. Additionally, contingent functions are related to modern economic, and regroups: basis of credit, liquidity, maximum use of resource, guarantor of solvency, distribution of national income. Generally, importance of money is to performed economic activities [4].

Number of authors criticizes the currency among which B. Lietear, for who our monetary system has a number of hidden counter productive effects, which as long remains a blind spot to us. Monopolistic use of currencies is well-suited for certain purposes and not for others. In fact, conventional money facilitates particular types of flows, while supports of types of flows within communities are not adequate. There is a monoculture of national currencies controlled by a few financial institutions that centralize decision. Finally, national currencies promote embolism [3]. To these criticisms are added many others to the example of the credit system, the financial crises, debt and monetary governance which justifies the move to cryptocurrencies.

#### *2.3.2. Literature Review of CFA Franc Currency*

The CFA Franc refers to the monetary unit which is legal tender in CFA zone. The 1929 crisis had, among other consequences, the dislocation of international monetary and commercial space, the rise of protectionism and the chain of devaluations. These facts led to the withdrawal of power from the settlers over their empires. The London conference of 1933 will therefore favor the birth of the monetary zones following the failure of the latter, in response to these withdrawals. We then witness the building of an imperial economic zone, protected from competition against the background of complementarity of colonial and metropolitan productions: the "sterling zone". In addition, the Second World War also had the effect of establishing exchange regulations, and the centralization of the dividend reserves applied to the colonies for the benefit of the metropolis. It is under these conditions that the franc zone was born with the objective of isolating the colonial empire from the international market in order to create a preferential zone in the aftermath of the 1929 crisis. The decree of September 9, 1939 established the zone franc for a common exchange legislation for all the French colonies. The CFA franc zone brings together 26 territorial entities, including fifteen African countries divided into two monetary zones, the countries of West Africa and those of Central Africa. The CFA Franc was born on December 26, 1945 by France with its membership in the International Monetary Fund. France then distinguishes the French Franc from the Franc of the French Colonies of Africa and France from the French Colonies of the Pacific.

We can summarize the specifics of this monetary area in three points: the franc monetary area, monetary union and monetary cooperation.

The franc zone: it is an area that is not really so, because the entities in this area hardly share a common geographic space. These different zones are: The countries of the franc zone of Central Africa, the countries of the franc zone of West Africa, the countries from the franc zone of the Overseas Departments and Overseas Territories, the principality of Monaco and Mayotte.

Monetary union: The existence of franc subzones implies a monetary union whichuses acommon currency.

Monetary cooperation: The monetary cooperation agreement between the countries of the zone and France is based on four principles: unlimited convertibility guaranteed

by the French Treasury, fixed CFA parity, free transferability and the centralization of foreign exchange reserves at the French Treasury [9].

### *2.4. Cryptocurrency*

#### *2.4.1. Overview of Bitcoin*

Bitcoin currency indicates an account value (Bitcoin address) comprising public and private keys used to receive or spend this value through a transaction. Bitcoin indicates various ways: protocol, currency, platform which are combine to facilitate the creation of digital currency. This overview of Bitcoin will lead us to present the key concepts of this technology/cryptocurrency [10].

i. Addresses and Transactions

A Bitcoin address is a string of characters that is communicated to people who wish to send funds. It corresponds to the recipient of a payment and begins with 1 or 3 followed by an alphanumeric string comprising between 26 and 35 characters. Can also be represented by a QR code, a Bitcoin address is determined from cryptographic hashes.

A transaction represents a Bitcoin transfer operation including one or more inputs and one or more outputs. It authorizes the credit of the account of the recipient of the transaction or address. Their realization requires the electronic signature of the owner of the Bitcoin account, which allows him to spend his money. The transfer is done by associating a key which secures the transaction that only the recipient can spend. There are three types of transactions: simple, aggregated and distributed. The simple associates a transfer with a single input, the aggregated associates several inputs with an output; and distributed combine one input with several outputs. The construction of a transaction is done by selection of input and creation of output. These two operations are carried out through a wallet, which is a dedicated application. Once signed, the transaction propagates to network participants who will be responsible for adding it in a block, the block in the blockchain through mining [11].

ii. Block and Blockchain

A block is a data structure that groups transactions. Its structure consists of a header, and the list of transactions. The block header is contained in 80 bytes comprising three sets of metadata: the first is the reference of the previous block, the second the difficulty of the block, the timestamp and the nonce; and the third the root of the transactions of the block.

A blockchain is a data structure linking the blocks one after the other in an orderly fashion. It can be stored in a file or in a database. The tree structure of a blockchain is through the chaining mechanism consisting in referencing the previous block by a field called previous hash. The diffusion of blocks in the Bitcoin network often causes the problem of the fork, which is the simultaneous discovery of a block by miners who take charge of it. After processing the block, different substrings are created. One solution to this problem is to choose the longest chain. The linking of the blocks in a blockchain is done through mining which is an operation of verification and validation of the transactions of the block and adds it if successful in the blockchain [10].

iii. Mining and Consensus

Mining indicates a process which validates transactions and adds them to the blockchain by providing security to the system with the consensus. In Bitcoin, mining is done through the PoW algorithm, which subjects miners to competition. How does it work? The miners compete to find a number lower than the system's difficulty target. The process ensures that the miner spends his computing resource by finding a difficulty that is a math puzzle problem. The objective being to occupy the resources which could harm the systems.

Consensus indicates agreement process between distrusting nodes on the final state of data. His mechanism provides decentralization of control through mining and ensures steps that nodes execute to agree on a proposed value [11]. It imposes a vote expressing the acceptance of valid blocks and the rejection of invalid ones. This is done by running a majority decision algorithm, in a distributed network which elects the node responsible for adding the block to the blockchain. There are several types of consensus, including: Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegate Proof-of-Stake (DPoS), Proof-of-Authority (PoA), Proof-of-Weight (PoWeight), Byzantine Fault Tolerance (BFT).

#### *2.4.2. Limits of Cryptocurrency*

Bitcoin is far from perfect, it has certain limits that are worth presenting among which: criminality, accidental loss of money. The anonymity and confidentiality supposed to secure Bitcoin are also rather flawed, because malicious people exploit these properties of Bitcoin for criminal purposes. These properties allow them for example, to circumvent the control put in place against money laundering and the financing of terrorism, or proceeded to scam internet users by offering them shitcoins. Accidental loss of cryptocurrency can occur in the handling of cryptocurrency. In fact, being stored in memory and associated with a key, cryptocurrency can be lost permanently either by the loss of medium in which it is stored, or the forgetting of its address. Instability and high volatility, a consumption of energy are also other limited observed.

### *2.5. Related Works*

An overview of the development of the national cryptocurrency allows us to identify the following works by the authors: Ali Mukhtar et al. and Adam Abdullah et al. These works converge on the problem of developing a cryptocurrency with the specificity is for the use is as national currency. From this angle, these works are related to ours which not only meets the objective of developing a cryptocurrency, but also a national cryptocurrency.

Ali M et al. [12] offers an alternative to the local currency of Iraq through the cryptocurrency solution. To do this, he uses an approach to develop a Token which he names

IQDtoken, developed through the ethereum development platform. authors provide an overall implementation of the system through a block diagram for the system development process, and illustrate la structure project by directories and files of the proposed system. Using well-listed tools, they develop two smart contracts: one for the IQDtoken token and the other IQDtokensale for the token's ICO whose interfaces are illustrated in results. This study shows the interest of researchers for the development of national cryptocurrencies, but also presents an approach to the development of a cryptocurrency by developing a token in the ethereum platform.

Adam Abdullah et al.[13] as for them, proposes in their work a framework of development of a national cryptocurrency. This framework is a model that combines the traditional monetary system with the cryptocurrency system by seeking to integrate a monetary authority into the cryptocurrency system. The approach discussed is an adaptation/customization of the open source code algorithm copied from a cryptocurrency (ethereum, Bitcoin SegWit or Hyperledger Fabric). It should be noted that this article has perspectives on banking and finance that have been associated with technology. Thus, the development approach is not really discussed, but the simulation environment is well described.

in summary, this work adress with and propose cryptocurrency development solutions, for which two approaches are identified: by development of a token and by development from a copied open source code. We will in this paper, following our objectives to explore possible approachs of development of cryptocurrency while taking into account these two identified approaches.

# 3. Methodology

### *3.1. Search Approach of Cryptocurrency Development*

#### *3.1.1. Token Approach*

A token indicates commonly a coin, but since the invention of cryptocurrency, it also refers toa sub-currency dependent on a cryptocurrency. It was introducing by Vitalik Buterin the creator of Ethereum cryptocurrency. What Token doestechnically? A Token is a smart contract application running in the Ethereum EVM, representing a sub-cryptocurrency. The Token approach is a method proposed by Fabian Vogelsteller and Vitalik Buterin in 2015 through the EIP 20 standard: ERC-20 Token Standard. This standard is a protocol that offers an API, with an interface whose contract allows the development of a sub-currency with interoperability in the Ethereum blockchain. The interface offers six functions and two events that allow you to develop a sub-currency that can be interchanged with other sub-currencies. Below is the ERC-20 API contract.

```
contract ERC20Interface {
function totalSupply();
function balanceOf (address tokenOwner);
function allowance(address tokenOwner, address spender);
function transfer(address to, uint tokens);
function approve(address spender, uint tokens);
function transferFrom(address from, address to, uint tokens);
event Transfer(address indexed from, address indexed to, uint tokens);
event Approval(address indexed tokenOwner, address indexed
spender, uint tokens);
}
```

The principle of the method consists in setting up a database offering a single operation. This operation consists of crediting from the units of an account A, an account B; with the condition that A has sufficient balance to credit B. The steps of the method are as follows:

Step 1: ERC-20 API interface development;

Step 2: Token test in the Testnet network;

Step 3: Development of the contract front-end;

Step 4: Deployment of the token in the Mainnet network [14].

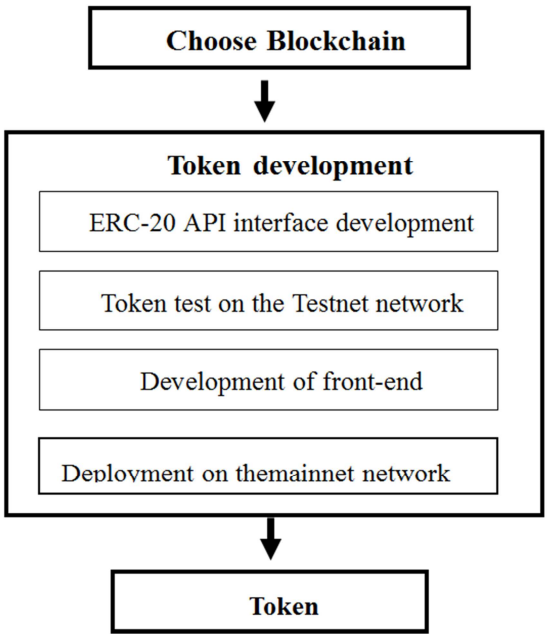


***Figure 1.*** *Token approach of development.*

#### *3.1.2. Hard fork Approach*

The fork is the result when a Blockchain diverge into two branches. It occurs in two ways: either through soft fork or by hard fork. Both produce somewhat similar results, but the difference is that the soft fork is backward compatible and the hard fork is not. Backward compatible means that, nodesoperating under the old rules will still recognize blocks produced under the new rules as valid. What is happening exactly? In the beginning, we have one cryptocurrency that has its Blockchain and its rules. Sometimes, these rules are not unanimous with nodes, and they want to update them; while others prefer them as well. At the end, when nodes adopt different rules, they produce a hard forkwhich creates two Blockchains [15]. Hard fork indicates a radical change in the Blockchain that makes all the previous blocks or

transactions invalid. This change therefore gives an opportunity to create a cryptocurrency with the resulting blockchain. The development of a cryptocurrency by hard fork is done in 7 steps:

Step 1: Choice of Blockchain;
Step 2: Building community;
Step 3: Proposal of elements to modify;
Step 4: Development of news updates;
Step 5: Vote on the date of fork;
Step 6: Apply Fork;
Step 7: Creation of a new cryptocurrency.

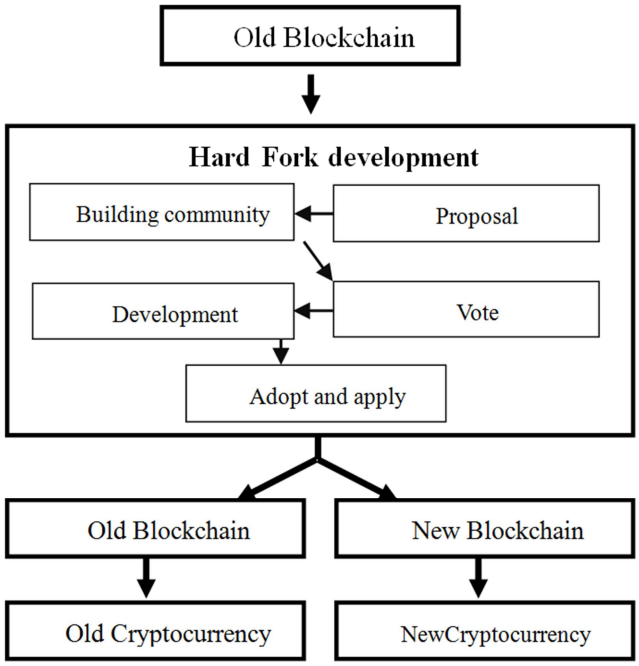


***Figure 2.*** *Hard fork approach of development.*

### *3.1.3. Source Code Fork*

Linus Nyman defined the fork, as any instance in which the code of a program is copied, modified, and reused to start or develop another program. He even adds that, a project that is based on another project but whose code has been entirely rewritten can also be considered a fork [16].

This brings us to categorize the fork: fork of code source and fork of software. The method of developing cryptocurrency by fork of open source code is done by copying (fork) the mother source code of a cryptocurrency and customizing it. Figure 3 below illustrates the development of a cryptocurrency by fork of the source code. It all starts with choosing the cryptocurrency you want to clone. This requires that the source code be open source, which will be customized to obtain a new cryptocurrency. The development of a cryptocurrency by fork of the source code is possible according to the following steps:

Step 1: Choice of the cryptocurrency;
Step 2: Copy of the source code;
Step 3: Conception;
Step 4: Customization.

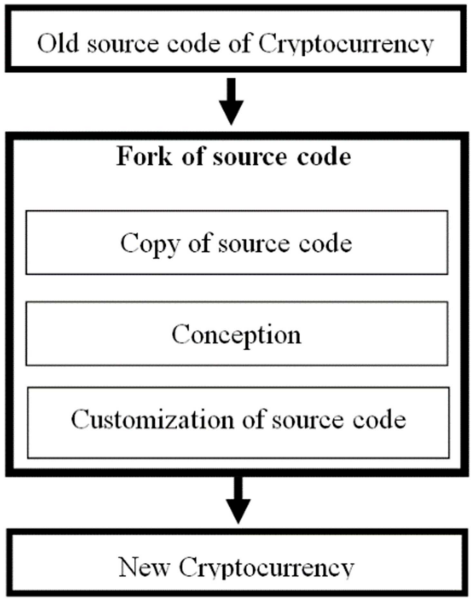


***Figure 3.*** *Fork of source code approach.*

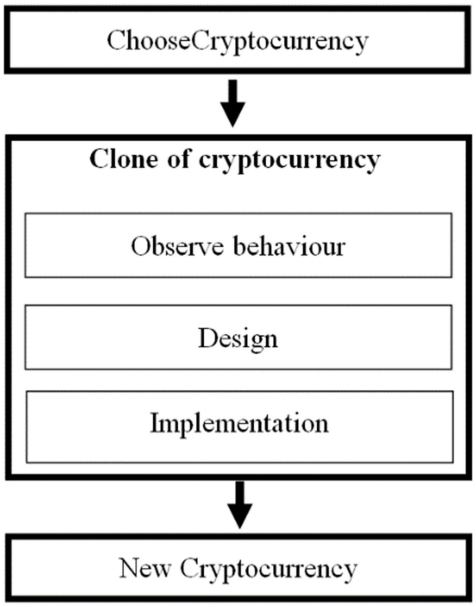


***Figure 4.*** *Soft of software approach.*

### *3.1.4. Software Fork approach*

Fork of software indicates project or software that is based on another project orsoftware and whose code has been entirely rewritten. Itis a code source that simulates anothersoftware through the functionalities or the observation of the behavior of software thatis copied [16]. In this work, the fork of the software refers to the fork of the cryptocurrency whose code has been completely rewritten, in particular Bitcoin. Taken from this angle, the development of a cryptocurrency can be done by this approach, since many existing cryptocurrencies simulate Bitcoin. Their implementation is not always a copy of the Bitcoin code. To do this, the following steps are necessary for the development of a cryptocurrency by this approach.

Step 1: Choice of the cryptocurrency;

Step 2: Observe behaviour;
Step 3: Design;
Step 4: Implement.

### *3.2. Comparison of Approach*

#### *3.2.1. Comparison*

We have identified four development approaches of cryptocurrency: by token development, Hard fork, source code fork and software fork. We will now proceed to compare theseapproaches and choose one of them, that we proposed within the context of this study. This comparison is made in terms of: Cost of project, time of development, dependence on a blockchain platform and solution to exit from the CFA Franc.

i. Cost

Development cost allows us to classify the development approaches in terms of development cost. Without however listing the necessary resources, it is a question of making an idea which informs the developer of the expected development approach compared to another.

ii. Time of development

This element of comparison allows us to compare the time required for the development of a cryptocurrency for each approach. Development time is a very important factor in a process, because, the cost of software also depends on it.

iii. Dependence on blockchain platform

Here, it is comparison of the dependence of development approach on a blockchain platform. For us, this factor makes sense in terms of sovereign solution, since currency is an element of sovereignty, a national cryptocurrency cannot be hosted in a blockchain that is not ours.

iv. Frees to CFA Franc

Does the product resulting from this approach liberate from the CFA Franc, is the question answered by this element of comparison? Indeed, the ambition of this study is to develop not only a cryptocurrency, but a national cryptocurrency able to removeCameroon from the CFA Franc.

The table below presents the result of comparison of cryptocurrency development approach.

***Table 2.*** *Comparison of approaches.*

| Approach | Cost | Time | Blockchain | Frees to CFA Franc |
|---|---|---|---|---|
| Token | Low | Shot | Existing | Yes |
| Hard fork | Fewer | Shot | Existing | Yes |
| Fork Source code | Average | Average | Own | Yes |
| Fork Software | important | Long | Own | Yes |

The analysis of this table allows us to observe that: development by token and by hard fork isinteresting in terms of cost and development time; while the other approaches are interesting in terms of non-dependence of blockchain platform.

#### *3.2.2. Choice of Approach*

We must develop a cryptocurrency which guarantees the exit from the CFA franc and which restores the monetary sovereignty of Cameroon. From the above comparison, all four approaches free Cameroon from the CFA franc. Some depend on a blockchain platform and others do not. However, as we are looking for total independence both on the currency and on the blockchain platform, we exclude the token and hard fork approaches. On the other hand, the development by fork of the source code and the development by fork software are the two approaches which offer the possibility of leaving the CFA franc without dependingon a blockchain platform. Of these, we retain the fork approach of the software for the triple interest: the solution offers a currency that frees Cameroon from the CFA Franc, offers independence from the blockchain platform and finally allows us to have a proprietary solution. In addition, this approach will allow us to domesticate cryptocurrency technology.

### *3.3. Implementation of Cryptocurrency Project*

#### *3.3.1. Building Communities*

Building communities is necessary for the implementation of a cryptocurrency development project; it starts with building communities of developers, miners and future users. Often, this happens through the writing of the white paper which provides a number of indications about communities.

#### *3.3.2. Development of Cryptocurrency*

This is where the cryptocurrency development process is implemented. The development of cryptocurrencies is often carried by developers grouped in community for the occasion.

#### *3.3.3. Set up Exchange Platforms or Coinbase*

At the end of the development, the cryptocurrency is placed in the exchange platforms. The search of exchange platforms allows the introduction of cryptocurrency in the cryptocurrencies market. These cryptocurrencies exchanges points are also a place to buy cryptocurrency. It is therefore a question of accomplishing a cryptocurrency project of any known exchange platform. These platforms will facilitate obtaining/purchasing of cryptocurrency by future users.

#### *3.3.4. Release*

The release of cryptocurrency is also done through a community of cryptocurrency users. Internet users wishing to own the future cryptocurrency can purchase isin advance via an ICO. As part of a sovereign national cryptocurrency, we need to work for its global acceptance.

### *3.4. Development of Cryptocurrency*

The prototype method is a development method centered on a sample or a model, which during the development process

will undergo extension and improvements gradually to produce the final product expected over time. The prototype is justified by its flexibility to change and the addition of improvised functionalities. There are several variants: the rapid prototype, the experimental prototype and the evolutionary prototype. The evolutionary prototype illustrated in Figure 5 below, is the one that grabs our attention in this study.

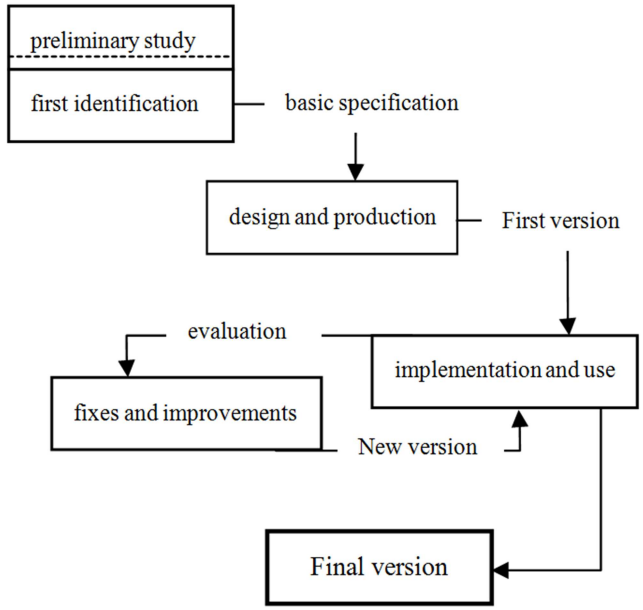


***Figure 5.*** *Evolutionary prototype [17].*

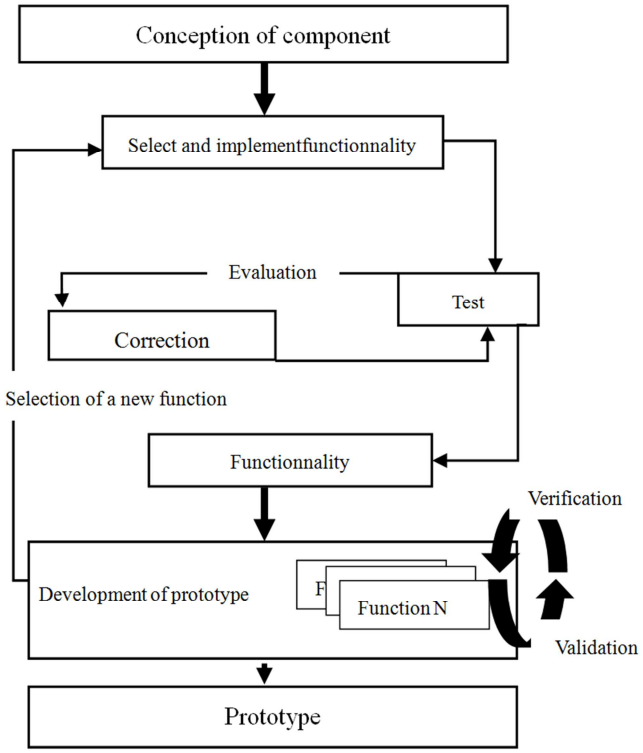


***Figure 6.*** *Custom evolutionary prototype.*

To simplify the understanding of the system we should start by solving a sub-problem and the solutions to the other sub-problems will be added to the initial solution. It is through the above evolutionary prototype method that we propose to develop a cryptocurrency. But, we have customized it for this. Thus, the cryptocurrency will be developed functionality after functionality taken from a component of the system. One of the drawbacks of the prototype method is the lack of visibility. It is for this reason thatwe have associated toit the iterative and incremental method. An iterative process refers to a development process guided by repeated cycles of operations. Iteration development operations bring the prototype closer to the final product in our case. That requires a breakdown of the activities carried out by cycle and which produce in a cycle an increment which in turn will be integrated into the prototype/product.

The effectiveness of this method is based on defining a fixed time for iterations. The version of a product by incrementing the previous version is either an improvement / refinement of the product, i.e. the addition of functionality. The incremental approach has as specificity that the product must always be functional for a given increment. In our study, the iterative and incremental method will reinforce the prototype approach as shown in figure 6.

# 4. Results and Discussions

### *4.1. Environment and Condition*

The experiment is based on Intel(R) Cord(TM)i5-2520M CPU @ 2.5OGHz (4CPU), 4GB RAM, 64bit, X64 system. We use as operating system Windows Professional 64bit. We used the Go (Golang) programming language to develop the prototype, and the IDE LiteIDE X35.2 to write the code. The test environment is a local computer for which we use the port numbers to differentiate the nodes of the network. Each instance is a node designated through an environment variable, named NODE_ID. We use multiple nodes on a single machinerequiring at least three nodes:

The central node

This is the node to which all other nodes will connect, and it is the node that will send the data between the other nodes.

A miner node

This node will store new transactions in mempool and when there’re enough of transactions, it’ll mine a new block.

A wallet node

This node will be used to send coins between wallets.

The usage scenario is the following:

The central node creates a blockchain;

Wallet node connects to it and downloads the blockchain;

Miner node connects to the central node and downloads the blockchain;

The wallet node creates a transaction;

The miner nodes receive the transaction and keeps it in its memory pool;

When there are enough transactions in the memory pool, the miner starts mining a new block;

When a new block is mined, it is sent to the central node;

The wallet node synchronizes with the central node;

User of the wallet node checks that their payment was successful.

### *4.2. Results of Simulation*

*Set NODE_ID:*

*We launch tree terminals window and set environment variable, so we have: first terminal NODE_ID=5000, second NODE_ID=5001 and third NODE_ID=5002.*

*NODE 5000*

*Create a wallet and new blockchain*

>NkapCoin.exe createblockchain –address CENTRAL_NODE

*At the creation, the blockchain contain a single genesis block that need to save for another node.*

>copy NkapChain_5000.db NkapChain_genesis.db

*NODE 5001*

*Generate some addresses.*

>NkapCoin.exe createwallet

*We will name the addresses generated by Wallet_1, Wallet_2 and Wallet_3.*

*NODE 5000*

*We return to the central node and send some coins to the wallet addresses:*

>NkapCoin.exe send –from CENTRAL_NODE –to Wallet_1

–amount 10 -mine

>NkapCoin.exe send –from CENTRAL_NODE –to Wallet_2

–amount 10 -mine

-mine *flag request that the node himself mine the transaction directly. For the moment, the miner node is not yet active in the network.*

*Start the node:*

>NkapCoin.exe startnode

*The node must be running until the end of the scenario.*

*NODE 5001*

*Start the node's blockchain with the genesis block saved above:*

>copy NkapChain_genesis.db NkapChain_5001.db

>start node

*As Bitcoin, the node will download all the blocks from the central node. After stop the node and check that all is okay.*

>NkapCoin.exe getbalance –address Wallet_1

==>Balance of Wallet_1:10

>NkapCoin.exe getbalance –address Wallet_2

==>Balance of Wallet_2:10

>NkapCoin.exe getbalance -address CENTRAL_NODE

==>Balance of CENTRAL_NODE:10

*NODE 5002*

*We generate a wallet, initialize the blockchain and start the node as miner node.*

>NkapCoin.exe createwallet

>copy NkapChain_genesis.db NkapChain_5002.db

>NkpaCoin.exe startnode -miner MINER_WALLET

*NODE 5001*

*Now where all are ready, we send some transactions:*

>NkapCoin.exe send -from WALLET_1 -to WALLET_3 -amount 1

>NkapCoin.exe send -from WALLET_2 -to WALLET_4 -amount 1

*We can view on the terminal of the miner node the above transactions.*

*NODE 5002*

*By starting this node, there is an update of the copy of the blockchain by downloading recent transactions. Below, is the starting of the node and checking of transactions.*

>NkapCoin.exe startnode

>NkapCoin.exe getbalance -address WALLET_1

==>Balance of WALLET_: 9

>NkapCoin.exe getbalance -address WALLET_2

==>Balance of WALLET_2: 9

>NkapCoin.exe getbalance -address WALLET_3

==>Balance of WALLET_3: 1

>NkapCoin.exe getbalance -address WALLET_4

==>Balance of WALLET_4: 1

>NkapCoin.exe getbalance -address MINER_WALLET

==>Balance of MINER_WALLET: 10

### *4.3. Discussions*

In this study, the proposed cryptocurrency integrates all the necessary components as illustrated in Figure 7 below. The simulation performed although it is a prototype simulates the basic functionalities of Bitcoin.

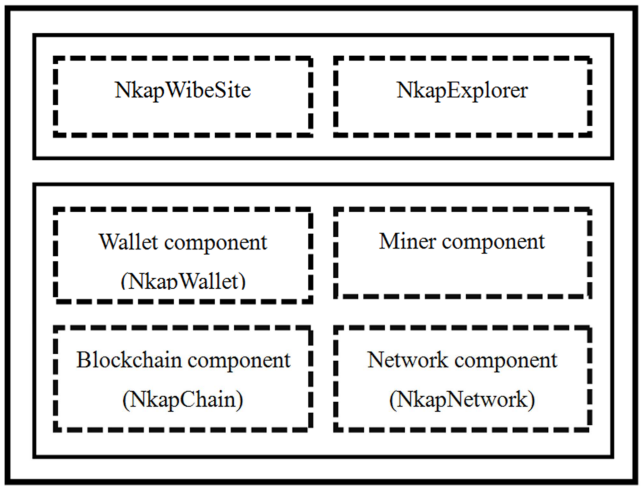


***Figure 7.*** *Architecture of NkapCoin.*

The analysis of this study allowed us to identify the following strong points: First, we conclude that cryptocurrency is the solution to exit Cameroon from the CFA franc. Second, the study presents four different approaches to develop a cryptocurrency. And finally, we simulated the Bitcoin cryptocurrency by a cryptocurrency that we named NkapCoin. However, this study is not exhaustive enough with regard to approaches geared at developing a cryptocurrency, for which we have only made a summary presentation but not detailed. Just like the process of implementing a cryptocurrency, which was also the subject t of a brief presentation. We can also say that although the simulation is an evolutionary prototype, it would have been interesting to render with sling shot rather than text mode. the aforementioned shortcomings are

justified by the fact that this study is preliminary to the project of development of a national cryptocurrency and that in perspectives, it will be enriched. The discussion that we do of the evoked similar work and our research, is mentioned in Table 3. he makes a comparison between related works and our study, in terms of objective, development approach, algorithm, results, limits and criticisms; to the effect to evaluate this work.

***Table 3.*** *Summary of discussion with related works.*

| Works | objective | Approaches of development | Algorithm | Results | limits | reviews |
|---|---|---|---|---|---|---|
| Hussain Ali M. Muayed S. AL-Huseiny | creates a cryptocurrency backed by a national currency | Token development | No algorithm | IQDToken | | the study is limited only to the implementation, it would have been better if it proposed from design to implementation of the token to develop. |
| Adam Abdullah, Rizal Mohd Nor | integrated a monetary authority for a stable cryptocurrency | Clone of open source code (cryptocurencey) | No algorithm provide | cryptocurrency model (framework) with monetary authority | oriented work in banking and finance | repeat the same study specifically on the technological level |
| Our study | explore possible approaches to developing a cryptocurrency for the development of a national cryptocurrency | 1. Token;<br>2. Hard Fork<br>3. Fork of source code<br>4. Fork of software | No improvement, just simulates Bitcoin experimentally through the prototype | prototype of a cryptocurrency that simulates Bitcoin | only one approach is discussed in detail | develop a prototype with coverage of illustrated components of the NkapCoin cryptocurrency |

# 5. Conclusion and Future Work

This study allowed us to observe that the problem of commodity exchange remains topical with different realities by era. Systems of commodity exchanges each time resolve this problem through the direct system, indirect and semi-direct one. In the context of this study, the direct exchange system is the one that hold backour attention through one of its approach: the cryptographic monetary exchange system. One of the major result of this study was to determine that cryptocurrency is an alternative that can get Cameroon out of the CFA Franc. But to the question of how to develop a cryptocurrency, we followed a very specific path to provide an answer. Our method was based on four points: the research of cryptocurrency development approaches, the comparison of these, the stages of implementation of a cryptocurrency development project and the development itself. we have provided four approaches that can be used to develop cryptocurrency. All of them also allow the development of the national cryptocurrency. To this end, these approaches have been compared to the effect of releasing the one that restores monetary sovereignty in Cameroon and above all independent of existing blockchain platforms. it should be noted that these approaches are effective solutions for the development of a national cryptocurrency, which can be applied according to the objectives/specificities sought by the development project. we proposed that the creation of communities, the development of cryptocurrency, the setup of exchange platforms and the release as different stages of a project of development of a cryptocurrency. The prototype named NkapCoin was developed using a fork of software approach, in a process which combines the evolutionary prototype and the iterative and incremental development.

From this work, we can regret that all the above approaches have not been the subject of in-depth study in terms of development and therefore no simulation relating to it for the moment. The process of implementing a cryptocurrency project is not sufficiently developed too. Finally, it would be interesting to complete the prototype developed with its other components: NkapWebSite and NkapExplorer; and its front end and the network part, for deployment in a P2P physical environment. For future work we recommend a detailed discussion of the three approaches presented briefly, and remedied the above-mentioned limits. Taking this work under the aspect of technical assistance to politics, cryptocurrency is still encountering little adoption by states that are dispossessed of an important instrument of power: money. It would therefore be important to study and see how to develop the framework proposed by Adam Abdullah et al. for States wishing to use the instruments of the monetary authority or even stabilize their cryptocurrency.

# References

[1] Beatrice Hibou; The CFA franc seen from Italy, France and Africa; Societes politiques comparees; 47; January/April2019.

[2] Alain Faujas; Exit of the CFA Franc: whattheprojectfrenchlawsays; Jeune Afrique; 21mai 2020; https://www.jeuneafrique.com/985419/economie/sortie-du-franc-cfa-ce-que-dit-le-projet-de-loi-francais/.

[3] Bernard Lietaer; What is the problem with our curren tmoney system? 17 September 2010; http://www.lietaer.com/2010/09/what-is-the-problem-with-our-current-money-system/.

[4] A. S. Siddiqui; Comprehensive Economics XII; Laxmi Publications; 2011.

[5] Ross M. Starr; The Structure of Exchange in Barterand Monetary Economies; The Quarterly Journal of Economics; Vol. 86, No. 2 (May, 1972), pp. 290-302.

[6] M. Simonson; Study of a Cashless Service Exchange System; Digital or Visual Products; 2006.

[7] Jerome Blanc, Cyrille Ferraton; Social currency? Local Exchange Systems (SEL) and solidarity economy; 2005; pp. 83-98.

[8] Jean-Yves Capul and Olivier GARNIER; Dictionary of Economics and Social Sciences; Hatier; third edition; 1996.

[9] Seraphin PraoYao; The CFA franc, acurrency that delays Africa; Bibliotheca; Vol. XII, Issue 3; 2011; pp. 145-162.

[10] Andreas Antonopoulos, Mastering Bitcoin; O'Reilly; Second edition; July 2017.

[11] Imran Bashir; Mastering Blockchain; Packt Publishing; Second edition; March 2018.

[12] Hussain Ali M. et al.; Implementation of national cryptocurrency using ethereum development platform; Periodicals of Engineereing and Natural Sciences; Vol 7, No. 3September2019; pp. 1021-1019.

[13] Adam Abdullah et al.; A Framework of Development of a National Crypto-Currency; International Journal of Economics and Finances; Vol. 10, No. 9; 2018.

[14] Fabian Vogelstellerand Vitalik Buterin; ERC-20 token standard; 2015; https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md.

[15] Nick Webb; A Fork in the Blockchain: Income Tax and the Bitcoin/BitcoinCash Hard Fork; North Carolina Journal of Law & Technology; Janary 2018.

[16] Linus Nyman; Understanding Code Forkingin Open Source Software, An examination of code forking, its effect on open source software, and how it is viewed and practiced by developers; EditaPrimaLtd; 2015.

[17] Anne-Marie Hugues; Different life cycle models; december 2002; https://studylibfr.com/doc/2662740/2.differents-modeles-de-cycles-de-vie/.