

# Proposal of a Smart City Built on Application of Cryptocurrency

教授：亀田

G2120018: Saud Abdelaziz Alhammadi

## 1. Introduction

Bitcoin became the first cryptocurrency not long after the 2008 global financial crisis. Bitcoin was created in 2008 by a group or individual known as Satoshi Nakamoto, allowing individuals to conduct daily transactions using a digital currency [21]. The currency that is not centralized, Bitcoin operates independently of banks or other financial institutions. Peer-to-peer exchange is possible because transactions can be conducted anonymously. Personal data protection concerns arise if the middleman or go-between (such as a bank) is aware of the buyer and seller's identities. The Bitcoin platform, which does not share personal information, has made coin trading and transactions more convenient and independent. As a result of using this method of trade, some individuals have been able to conduct business undetectably.

Bitcoin was the first digital currency to utilize blockchain technology. A transaction log is created when computers connected to a network contribute to its creation. Because it prevents fraudsters from reusing the currency, this blockchain is one of the most secure systems. In addition, the blockchain protocol uses proof-of-work (POW) to ensure that miners adhere to the structure. The computing power required to mine currencies is called "hashpower," a term that refers to a computational operation called "hashing". Since the 1960s, this system has evolved from a paper-based foundation to a computer-based one [7]. A failure of the information system, such as a security breach that results in theft or a failed transfer instruction, is legally required to compensate the asset owner.

### 1.1. History of Cryptocurrency

When Satoshi Nakamoto first introduced Bitcoin [21], only 50 of them were present. At this early stage, only computer geeks worldwide dismissed the hype. When Mt Gox, a Japanese company, launched its Bitcoin trading platform in 2010, there were twenty Bitcoins available for trading at 4.951 cents each. The merchandise was approximately \$1.00 in value. When this paper was

published, the value of Bitcoin had risen to an all-time high of \$6,777, making it the most valuable currency in history.

Since their inception, cryptocurrencies such as Bitcoin have generated considerable debate over whether they can be considered real money. A currency must first meet the following criteria: Safeguarding an individual's financial assets. Customers can influence the value of their purchasing power to make current and future purchases. Second, to make a payment method, one must possess both the capability and the unit of account, i.e., the price at which a product can be purchased or sold on the open market. Each of these requirements must be met theoretically, but this is not always the case in practice.

### 1.2 Problems of Cryptocurrency in UAE, the World and Previous Work

Since then, many changes have occurred, resulting in the loss of its fundamental meaning and roots in altering current cryptocurrency systems, which have become destabilized due to the numerous changes that have occurred over several years. It is intended that this segment of the course will go into further depth about the design and cryptography of cryptocurrency tokens, as well as the idea of "moneyness" as it relates to cryptocurrencies in general and specifically bitcoin in particular.

#### a) Role of Cryptography in early Cryptocurrencies

Technically, the ability to write and read transaction records can be used to categorize projects according to the permissions granted. A cryptocurrency system can be classified as "public" or "private." There are also "permission" and "permissionless" cryptocurrency systems, among other things. To accomplish this, Peters et al. (2019) developed a popular categorization: Transactions in a public-permissionless system can be read and written by any node. Access to public-permission systems is restricted to nodes that have been granted permission. To summarise, only authorized nodes can access the information within private permissioned systems.

Cyberpunks lack a vision for an infrastructure that is more "private" and "permissioned," as opposed to an infrastructure that is more "public." Privacy coins have emerged as a new trend to compensate for the lack of trust inherent in traditional cryptocurrencies. Take, for example, the cryptocurrencies Zcash and Monero, both of which have a long history. It is impossible to separate them from the permissionless public setup of reading and writing rights that characterizes archetypal cryptocurrencies.

## b) Monetary Characteristics of Early Cryptocurrencies

This has been a major concern for those who believe that cryptocurrencies can be used to create "digital cash" or "currency," and it continues to be so. However, it should be noted that not all development strands are geared toward creating general-purpose monetary tokens. Because they are the first- and second-layer tokens of smart contract platforms, coins such as Ether and Ethereum are referred to as "cryptocurrencies" (e.g. Ethereum). On the other hand, these tokens are primarily intended for activating smart contracts rather than serving as a general payment method for goods and services. However, it is possible to think of smart contract activation as a genuine service accessible through token ownership, thereby "anchoring" tokens into a real economy even though they are in the virtual world, as described above.

On the other hand, even "general purpose" tokens are subject to change. Due to Bitcoin's and its descendants' inherent volatility, the development of "Stablecoins," intended to stabilize Bitcoin's purchasing power, has taken place as a response to the volatility. In some cases, Stablecoins can be found that are "tethered" to fiat currencies, or that is "backed" by assets that have a monetary value in fiat money. As a result of the fact that they are no longer "blank" empty signifiers, it is easier to estimate and communicate their worth. Several frameworks have recently attempted unification and abstraction of stabilization techniques for Stablecoins.

According to Blawie and colleagues, "tokenized funds" are "new forms of electronic money" that may be subject to anti-money laundering, counter-terrorist financing, and other regulatory requirements. This could, at the very least, guarantee "moneyness" in a legal context. Stablecoins, from an economic standpoint, may lead to an increase in the use of cryptocurrencies as money in the future, even if the legal case for doing so is not always clear. However, Stablecoins aren't widely accepted in the retail sector at this time due to their infancy.

### 1.3 Research Goal

My business plan revolves around two primary services;

- Intermediary services

- Liquidation services.

In the former, whenever a client's transaction has a cryptocurrency as a payment method, my company gets involved in smoothing out crypto-related transactions for both parties and takes care of any legal issues that may arise. In the latter, my company sells or converts the cryptocurrencies to cash and then deposits them into designated bank accounts. In case of a person from a country outside of the UAE, the company then takes care of all the legal procedures and paperwork needed to open a bank account in the UAE.

Cryptocurrency functions similarly to any traditional national currency with a few fundamental differences. Current "fiat currency" is created and regulated by a governmental body, all of which now represent debt. Anyone that owns a country's currency holds an "IOU", i.e. I owe you, issued by that respective country. Cryptocurrency does not stand for debt. It strictly represents itself, and its value is determined by someone willing to trade for it. The fact that decentralized cryptocurrency plays an essential role in deciding its currency value. Nobody owns or regulates a cryptocurrency. Its value is not subject to a country's political whims or a central bank's monetary policy. Cryptocurrency operates on a blockchain, the distributed ledger we discussed above.

Understanding blockchain technology will help you understand what cryptocurrency is all about and why this is the key to the power of digital currency. The "block" is composed of chunks of encrypted data. The "chain" is the public database in which the blocks are stored and sequentially related.

### 1.4 Monetary Characteristics of Early Cryptocurrencies

State central banks, state treasuries, and private commercial banks all issue fiat money, guaranteed to be redeemed by the legal system. Credits are initially created, distributed, and then returned to their issuers once their value has been depleted.

We refer to this flexible credit system as "money" because it can expand and contract. The term cryptocurrency implies from the start that tokens are money tokens, which is problematic in this context. The term "performatively" has been abused to argue that crypto tokens "should be money" or to deny the existence of what we currently refer to as "money," escalating the debate.

When comparing crypto-tokens to fiat currency, begin by referring to them as crypto-tokens and then listing their uncontroversial characteristics. In accounting terms, early cryptocurrency tokens are comparable to the mental image of a 'thing' created by typing the number '1'. Our "tokens" or "blank tokens" are identical. In the real world,

examples include clear plastic tokens devoid of inscriptions or rights. Bitcoin tokens are limited in supply, acting as the digital equivalent of a blank physical token. These tokens would be nearly featureless without adding a name and a brand logo. If you possess a private key capable of unlocking an "unspent transaction output," you are the sole entity capable of initiating a transfer. This resemblance to a "bearer instrument" is one of the reasons why some people refer to cryptocurrency as "digital cash" (physical cash being the bearer- instrument form of fiat currency).

Thus, Bitcoin is most frequently used for speculation, that is, purchasing the token with fiat currency and then selling it for fiat currency rather than as a medium of exchange for goods and services. There is considerable speculation about the value of tokens, which contributes to the volatility of the tokens' fiat currency price, which when viewed through the conventional 'functions of money' paradigm preferred by economic textbooks raises concerns about the tokens' "monetaryness." [23]

To summarize, my research goal would include the following:

- Implement smart city functionalities using cryptocurrencies as a building block.
- Understand how cryptocurrencies boost the development of smart cities.
- Understand how cryptocurrencies facilitate smart city application.

## 2. Survey of Cryptocurrency

Due to the success of Bitcoin in 2018, a new term, "cryptocurrency," was coined. This protocol is intended to enable an online community of people connected via peer-to-peer electronic networks to create and exchange digital tokens while also ensuring the transaction's security through cryptography. Satoshi Nakamoto coined the term "cryptocurrency" to describe the project in an online network and a cryptography mailing list. In online and print media chatter, the term "cryptocurrency" was quickly coined to refer to digital currency. During the early stages of Bitcoin, both the protocol and its associated tokens were referred to as Bitcoins. A network participant (referred to as a miner) is responsible for creating new bitcoins by converting the format of a bundle of proposed transactions (along with a single request to issue new ones as a reward) into one that can be attached to a chain of previously hitched bundles. Possibly as a result of this protocol and its immediate descendants, the term "cryptocurrency" was coined.

### 2.1 What is Currency, and Why has it been used in Many Societies?

Cryptocurrencies such as Bitcoin and others are still a novelty in the world of payment systems and technology. While the term "cryptocurrency" is frequently used in domestic and international literature when discussing cryptocurrencies, these concepts have a number of distinct properties that do not fully define them as synonyms. In the broadest sense, "digital currency" refers to money that is electronically stored (digitally). To conduct operations and interact with this type of currency, you must have access to the Internet or another network that supports electronic wallet interaction. Digital currencies have no intrinsic value [1], they simply reflect an issuer's ability to claim money or the right to a claim on the issuer's balance sheet. However, this type of currency is frequently used when making online purchases of goods and services.

The term "cryptocurrency" is used in cryptography to refer to a digital currency. Cryptography can be traced all the way back to over 4,000 years ago. Modern cryptography, which encrypts and decrypts data using a key, is based on mathematics and computer science. Cryptography has evolved into numerous subtypes over the course of its long history: Each network participant must have a public key to verify their identity before data can be decrypted; this is referred to as asymmetric encryption. Both the sender and recipient of encrypted data have access to the same secret key that enables decryption [2].

A process known as hashing can be used to generate a unique code from an array of data. The result is a hash code, also known as a hash function. The only way to recover the original data is to decrypt each hash code. The foundation of cryptocurrency systems is based on a subset of cryptography known as "hashing." A hash is generated for each transaction using the method depicted in Figure 1.

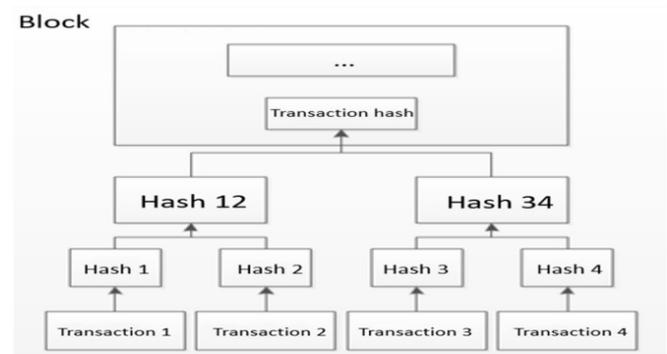


Figure 1. The scheme of obtaining a hash of transactions in cryptocurrency

### 2.2 Survey of Currencies and their Problems of Current Currency System

Money has taken on various forms throughout history. Still, it has always served the same fundamental functions: a medium of exchange, a means of storing value,

and a unit of account. As a result, money has become a necessary tool for social and financial transactions in the modern world. It's nearly impossible to imagine a day without money in any form. While non-cash money is not yet displacing cash, its turnover is growing faster than cash. The graphs below illustrate the year-over-year growth in demand for plastic cards and the volume of plastic card transactions [4]. Non-cash payment methods such as credit cards and debit cards pose a serious threat to digital currencies (Figure 2).

Despite their widespread use, plastic bank cards do not come without inherent risks. According to the Russian Federation's Central Bank, cyber criminals and fraudsters stole 1.3 billion rubles in 2019 from card accounts. This figure is 50% higher than the previous quarter's data. Among the threats to the security of plastic cards are phone and SMS phishing. To gain the customer's trust, the criminal poses as a bank representative and then steals their personal information. Additionally, financial transactions can be conducted directly from your phone. If the phone is stolen, an attacker may use the app to complete transactions [5]. ATM robbery and apprehended. The information about the owner of an ATM can be retrieved by installing special equipment capable of reading the ATM's data.

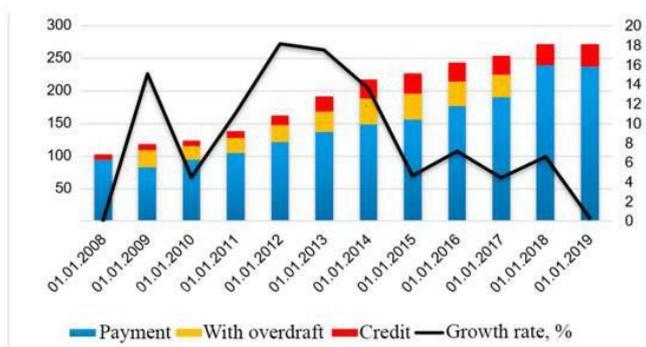


Figure 2. Number of payment cards issued by credit institutions, millions (left scale), percent (right scale)

### 2.3 Open Innovation with Cryptocurrency

Numerous researchers working with cryptocurrency in "Open Innovation" employ deep learning techniques in their selection processes. Autonomous open innovation is the best method to select novel features for sustainable artificial intelligence. This particularly involves:

- Hybrid clustering analysis using an improved krill herd method
- An unsupervised text feature selection technique based on a hybrid particle swarm optimization algorithm with genetic operators for text clustering,
- A feature selection method to improve the document cluster.

Businesses worldwide, including those in Russia, recognize the critical nature of business development and devote significant resources to the Endeavour. Russia's venture capital funds invest their entire current income (net management fees) in various activities, including business development.

### 2.4 Mining and the Blockchain System

Unlike fiat currency, which the government issues, cryptocurrency is created on the blockchain by cryptographic experts. Each new block mined results in the birth of a new cryptocurrency. The blockchain system relies on users, developers, miners, and node administrators to maintain the functionality of distributed ledgers. Miners who employ this method of mining must purchase software and hardware. Numerous Bitcoin mining programs fall into this category. For example, anthracite utilizes three hardware platforms: Avalon, Antminer, and ASICMiner.

To mine additional cryptocurrencies, you'll need a high-performance graphics card capable of running various algorithms. In addition, new miners must open an online wallet and a bank account capable of storing and accepting cryptocurrency as part of the mining process. Blockchain technology will record each transaction within its unit. Each block, as well as the one preceding it, is assigned an identification number. This is known as the "proof of work" protocol. This method enables transactions to be verified and communicated to others.

### 2.5 Discussion regarding Cryptocurrencies

When blockchain technology came to be, it caused an unimaginable disturbance in the financial sector and thus affecting the rest of the business sectors. This sparked the idea of establishing my business which cryptocurrencies are a big part of, as it has great potential in the future.

To summarize the discussion, the problems are as follows:

- Mining cryptocurrency requires expensive equipment, both software and hardware.
- Mining consumes large amounts of power and this can be costly.
- Blockchain causes disturbances in the financial and business sectors.
- Blockchain requires a lot of understanding in the way its used.
- There can be security and privacy concerns as wallets are tied to identities.
- A lot of governance and regulation would be needed to keep up with the blockchain technology.

### 3. Analysis of the Current Situation in the UAE

CoinDesk is the primary source for information on cryptocurrency prices. Due to the early years of Bitcoin's lack of market liquidity and trading, we use data from January 1, 2011, to May 31, 2018. The Ripple and Ethereum data series are available from August 4, 2013, to May 31, 2018. We generate cryptocurrency return data using the cryptocurrency's price as a reference point. Google allows for the download of search data series. Crimson Hexagon tracks the number of downloaded tweets containing "Bitcoin." Blockchain.info provides the number of Bitcoin Wallet users. Calculate Bitcoin's "dividend" ratio by multiplying its current price by the total number of people who have downloaded a Bitcoin wallet. This index is calculated by adding the daily squared log returns from the previous month's cryptocurrency volatility.

#### 3.1 Discussion and Consideration

Since the inception of cryptocurrency, there has been a never-ending stream of detractors who have expressed their reservations about the technology. Following the FBI's closure of the Silk Road marketplace, it became clear that cryptocurrencies were being used in an unlawful manner. Silk Road, a well-known Bitcoin exchange, was forced to close its doors earlier this year. In the past, the Silk Road has been associated with illegal activities such as drug trafficking and human trafficking. Alston claims that coins and blockchain technology were not to blame for the demise of Silk Road, which he believes is incorrect (2017). In the same way that criminals and scammers have taken advantage of any other platform, criminals and scammers have taken advantage of this technology in order to further their own financial gain [11].

Throughout Bitcoin's history, central bank intervention has played a role in both the speculative booms and busts that have occurred, as well as the price declines that have occurred since. Government policies and regulations should be put in place in order to ensure that everyone can benefit from cryptocurrencies while also protecting the interests of major market players. In the absence of a stable market [6], it is impossible to maintain government spending and the central bank's influence over the economy.

### 4. Overview of my Smart City in UAE

Forging or misusing a cryptocurrency is nearly impossible because of the way cryptocurrency is cryptographically protected in the first place. Several cryptocurrencies, such as Bitcoin and Ethereum, are built on the Distributed Ledger technology, which is enforced by a distributed network of computers. Alternatively, cryptocurrency is theoretically immune to government interference or manipulation because it is issued by no

central authority and thus does not have a central authority, as opposed to fiat currency. The term "cryptocurrency" refers to digital or virtual currency that is based on cryptographic systems and is used to conduct online transactions. Because of their existence, it is now possible to conduct secure online transactions without the involvement of a third-party intermediary. Several methods are used to protect these entries, including elliptical curve encryption, public-private key pairs, and hashing functions, among other things.

#### 4.1 Importance of my Smart City in UAE

Quite simply, bitcoin is here to stay and will not be phased out any time soon: transactions are quick and secure, and the system can be maintained without the danger of data being stolen or hacked, as is the case with traditional currencies, as is the case with bitcoin. As it turns out, there is less of an issue than you would have initially thought there was. Furthermore, Bitcoin should not, in the long run, cause inflation to occur.

As an additional point of comparison, there is no way for any central bank to boost the overall amount of money in the system because the total number of bitcoins that may ever be created is capped to approximately 21 million, making it impossible for any central bank to do so.

#### 4.2 Implementation of my Smart City in UAE

Post COVID-19, many cities are opting for sustainable urban solutions. The UAE already has a smart toll collection program called "Salik". This Smart Mobility involves every vehicle inserting a smart sticker on their windshield, and after passing through the Salik toll gate, a fixed amount is deducted. Each sticker is linked to a bank account belonging to the vehicle owner. In a similar fashion, my smart city plan for the UAE would include the following:

- Smart Utilities
- Waste Disposal
- Public Participation

##### Smart Utilities

A smart meter monitors electricity, gas or water consumption levels. At the end of the billing period, the meter computes how much the residents have to pay, and the money is automatically deducted from the associated bank account. This could be seamlessly integrated, as the public is already used to this modality from the Salik programme.

##### Smart Waste Disposal

The municipality in every Emirate would be informed when every container gets full of trash. A smart

water-proof sticker could be inserted inside the trash cans and when the trash levels reaches a certain point, it would alert the municipality to make the collection ready.

## Smart Public Participation

In a place like Dubai and Abu Dhabi, the public voices are heard. The public can share their opinions on legal matters or even fill out surveys for the government via the smart app. This would involve inclusion and transparency from every member of the society. Voting would not be possible in a place like the UAE because it's a kingdom where no voting takes place. Also, the number of expats are greater than that of the locals.

When it comes to working the theory into practical work, there will always be challenges. However, since I already made my research thoroughly, the number of inconveniences was minimized immensely, and the rest of the project was launched without any problems. My business plan centers on two main services: Intermediary services and Liquidation services. Intermediary services in general describes the act of being the link between buyers and sellers and insure a smooth business transaction between the two parties.

## 5. Conclusion

In addition to the fact that the cryptocurrency markets are always improving in terms of their technical and technological systems, the prices of cryptocurrencies fluctuate in tandem with these advancements. The creation of new and old digital currencies and the testing of existing digital currencies are now in progress at the Bitcoin Foundation. Only by using digital currencies outside of a single system can compete in the cryptocurrency market be achieved, which is currently not the case. Stablecoins, alternative currencies (altcoins), and cryptocurrency systems are the three regions in which the growth of cryptocurrencies will be split, according to the experts who have been acknowledged.

A thorough review of the digital currencies under consideration found that EOS, based on the Ethereum blockchain and works on the EOS platform, is the most effective and promising cryptocurrency currently in circulation, according to the study's findings. Also possible is the easy integration of third-party applications into the system is also possible.

In the future, we expect that the theoretical framework offered in this study will be relevant in further investigations into the digital currency of bitcoin. A primary focus of future research will be on new developments in the modelling of combination, including integrating additional components into a single theoretical framework, among other things.

My plan to implement smart city solutions in the UAE has great potential as this country has already adopted smart city urban plans like smart mobility. My plan includes using cryptocurrency to implement smart utilities, smart waste disposal and smart public participation.

## 5.1 My Future Work and Remaining Problems

There is a lot of potential for the future works for a smart city which includes smart communications, smart public administration and services and smart security. In a place like the UAE, these smart city solutions can be implemented once a proper system has been put into place. However, when it comes to the risks and problems of using cryptocurrency and blockchain in a smart city, cybercrimes can become possible. Personal information can be misused.

Bitcoin is certain to have a major impact on the global economy. It is imperative that all economists, researchers, and investors learn more about blockchain technology. It is imperative that we examine cryptocurrency in greater detail to ensure that it is not a one-time occurrence in the market. Despite this, the upcoming difficulties do not alleviate the financial woes of stakeholders. More research is needed to prevent a 51% attack on the mining network.

## References

- [1] IBM Cloud Education, "IBM," 03 June 2020. [Online]. Available: <https://www.ibm.com/cloud/learn/what-is-artificial-intelligence>.
- [2] IBM Cloud Education, 02 September 2020. [Online]. Available: <https://www.ibm.com/cloud/learn/speech-recognition>.
- [3] "Programatium," 2022. [Online]. Available: <https://www.programatium.com/what-is-the-ibm-shoebox/>.
- [4] S. James, "Fosspost.org," 19 February 2022. [Online]. Available: <https://fosspost.org/open-source-speech-recognition/>.
- [5] IBM Cloud Education, 15 July 2020. [Online]. Available: <https://www.ibm.com/uk-en/cloud/learn/machine-learning>.
- [6] K. Didur, 11 July 2018. [Online]. Available: <https://towardsdatascience.com/machine-learning-in-finance-why-what-how-d524a2357b56>.
- [7] D. Shewan, "WordStream," 21 December 2021. [Online]. Available: <https://www.wordstream.com/blog/ws/2017/07/28/machine-learning-applications>.
- [8] K. Damarla, "Extrudesign.com," 18 July 2021. [Online]. Available: <https://extrudesign.com/virtual-assistant-using-python/>.

