Faculty of Economics, University of Niš, 13 October 2016

International Scientific Conference

THE PRIORITY DIRECTIONS OF NATIONAL ECONOMY DEVELOPMENT

OFFICIAL CURRENCY AND ALTERNATIVE CURRENCIES

Velimir Lukić[*]

Aleksandar Živković[•]

Abstract: *The right of issuing currency that was to be used as a legal tender in economy has been assumed by governments as of the establishment of first central banks. However, a modern world with its advances in technology threatens to erode this monopoly and paves the way to the occurrence of what is known as digital currency issued by private entities. This paper analyzes contemporary economic and legal implications of digital currencies focusing on the most successful case among them - Bitcoin. It is argued that overall impact of digital currencies should be carefully considered. The mechanics standing behind these currencies can be easily reused in terms of fueling development in the circulation of official currencies and transition to the cashless society. On the back side, new currencies raise challenges that should be actively managed in order to prevent misbehavior. In sum, these currencies will likely make prominent impact in monetary sphere, although they are far less likely to rule out official currencies.*

Keywords*: money, monetary system, digital currency, Bitcoin*

1. Introduction

The current state of monetary system might be rather convincingly deemed as one, transitory phase specific to its evolution path. As we learned from a long history of money, it evolves in many respects, and although we are well accustomed to modern fiat money it has passed no more than ninety years since its introduction. At a time it was inconceivable for our predecessors to imagine regularly circulating paper money not backed with a pile of precious metals and exchangeable into it, yet they witnessed suspension of convertibility and got used to this change.

Another feature of current monetary system is a monopoly in the provision of money to the economy. The right of issuing official currency that was to be used as a legal tender in economy has been assumed by governments as of the establishment of first central

[*] Faculty of Economics, University of Belgrade, Serbia, ✉velimir@ekof.bg.ac.rs.

[•] Faculty of Economics, University of Belgrade, Serbia, ✉aca@ekof.bg.ac.rs.

UDC 336.74

banks. In the sense, there has been a phase in evolution of monetary system when paper money firstly appeared in which private entities, like goldsmiths and private banks, started issuing special notes that facilitated circulation of money in the economy. This invention is comparable with contemporary means of electronic payments in terms of derived benefits. Current developments characterized with advances in technology threaten to erode government monopoly established and pave the way to the occurrence of what is known as digital currency issued by private entities. These developments raise a lot of issues that are discussed in more detail in the remainder of the paper.

2. Reconsideration of traditional functions of money

If money was to be defined, it would be common to do it in terms of its functions. Any national currency is expected to serve as a medium of exchange, a store of value and a unit of account, whereas the first function is mostly regarded as a defining one. To carry out this function money must have a number of characteristics. It must be widely accepted in exchange for goods and services. It should be circulating easily, meaning its smooth and efficient transfer among transaction agents. It must be convenient for carrying out transactions of small value, which requires its divisibility into smaller units. Besides, it must be hard to counterfeit it, if possible at all.

There have been observed in the past occasional trials of issuing new currency, in parallel with national currency, by small local communities with the aim of stimulating local economy. In Europe, the case of Wörgl town in Austria, dating back from 1930s, reflects a pioneering endeavor in this regard. Michael Unterguggenberge, a major of Wörgl, confronted with a miserable town budget decided to issue stamp scrip in order to finance its local project and help economic recovery of the town. His "monetary project" was overwhelmingly deemed as a success. Other towns in Austria had been very interested in replicating his "project", while he also succeeded to attract international attention. The project was spurred by immense global economic problems in the respective period.

The very same idea revived later in the USA. Examples of what is referred as to community currencies are numerous. The currency called Ithaca Hours appeared at the beginning of 1990s in Ithaca, New York. Due to bad economic conditions many people could use some money in Ithaca, so Paul Glover helped them do so. He created a new currency and distributed it across people willing to accept it in exchange for goods and services who effectively took part in whole scheme. Initially, the value of one Ithaca Hour was set at 10 US dollars. The number of scheme members has been growing through the years and currently stands at above 2500, out of which around 500 businesses, according to a bimonthly directory HOUR town where all persons and businesses that accept Ithaca Hours are listed. In fact, real number of Ithaca Hours users is rather bigger than this posted number since there is possibility that someone accepts it, although he/she is not listed in a directory. In that sense, a directory is more of a manifest of people who are passionately backing the idea of local currency in Ithaca, providing their labor, skills and tools as a foundation of Hours' value. The identical scheme was followed in other US areas such as Madison, Wisconsin, Burlington and Massachusetts.

Above examples point to the widespread understanding that at the core of the money function as a means of payment rests its overall acceptance by the people. If people have enough faith and trust in some token, it can successfully qualify for the status of

money because they stand ready to accept it. When faith and trust diminish, a token is not any more convenient for the use as money. This reasoning motivated both Unterguggenberge and Glover to launch a new currency. But the story is unlikely to stop only with them.

What is common in these two cases is that new currencies circulated together with official ones. In that sense they operated more as complementary currencies, rather than a rivaling currency to a national currency. Additionally, they were not aimed at covering vast geographic area, but only limited local community. As for two other functions of money, new currencies did not have ambition to seize them from official currency. While the role of a medium of exchange is a clear target due to its implications for economic activity, remaining two roles do not provide anything comparable. Since any assets, both real and financial, can act as a store of value, new currencies are virtually marginal addition to this vast pool of assets with minor chances to verify as dominant. A role of unit of account has too remained reserved in community currencies ecosystem for an official currency. All prices even with merchants involved in local currency network continued to be posted in official currency. The conversion from price expressed in official currency to the one in a local currency was to be carried out when transaction was likely to occur and settled in local currency.

Grover (2006) asserted that there were as many as 2500 local currency systems operating around the world. He came with a finding that local currency did stimulate the local economic activity and production for local consumption that enabled preservation of a diverse skill base in local area.

However, in recent times emerged new, digital currencies that were nothing alike already mentioned local currency systems. These new systems are differently arranged and much more ambitiously projected, and inter alia they call into question their own peaceful cohabitation with official currency.

3. Emergence of a digital currency

At the turn of 21st century some commentators have argued that electronic money would fundamentally change the nature of monetary system and weaken the power of central banks. Some of its manifestations like electronic wallet or purse do not represent a radical change. In essence, when someone loads upfront some amount of money onto a plastic card and spends it in various shops when purchasing goods or services, it merely mimics earlier payment methods. At the end, this may only be a more efficient way of transferring ownership of bank deposits from one person to another. Consequently, the society might need less cash, but it still manipulates with well known bank deposits since cash prepaid onto any card is in effect a bank deposit. In general, whenever someone sends order to its bank to transfer funds to some recipient, including an internet message, no new principles are involved and modern technology then serves as a new conduit for authorizing payments.

Nevertheless, it is possible to imagine a special case in which new technology leads to a radical change in a monetary sphere. If new types of institutions or modalities of interaction among transacting parties arose, such that encompass issuing of some kind of tokens that become generally accepted in payments, than this would constitute a new reality

in which these new forms of money could provide a substitute for existing currency. The emergence of digital currencies matches this special case.

Digital currency is perceived as a type of money lacking any kind of physical properties whose existence is represented in a form of computer file. The appearance of digital currencies is closely linked to the advent of Internet and e-commerce. For a digital currency to be credible two problems must be resolved. The issue of controlling the creation of a digital currency is of primary importance, while consideration of its counterfeiting comes at a second place. The general aim is to prevent uncontrolled expansion of money which severely brings down its real value and purchasing power, if not close to nothing in the prolonged period of excessive rise in money supply.

The issue of money creation is clearly resolved when national currencies are in question. The government authority stands behind these currencies and institution of central bank is appointed as the solely issuer of the money. The money gets into the economy usually by the means of central bank buying some kind of financial assets, mostly securities. This is true when it comes to central banks of leading world economies who basically purchase government securities on the open market. For less developed countries this takes place in the form of purchases of foreign currencies, like US dollar, euro, yen; and accumulation of official foreign reserves instead of the stock of government securities. This money is referred to as high-powered money and the central bank has full control over its creation. It is used as a basis for bank deposits creation that account for the biggest part of money supply in the economy. Even in a period of gold standard, when the gold served as money, it was easy to understand how money gets into national economy. Three modes of entry are possible. It can either be extracted and refined in gold mines, or redirected from non-monetary to monetary uses, or imported from other countries.

The government is also held responsible to counter attempts to counterfeit national currency. It correspondingly takes care that banknotes and coins in circulation are valid and of good quality, and also difficult to reproduce. It enforces strict regulation on counterfeiters. In addition, in pursuing this task government relies on bank system. When valid paper money is deposited in commercial banks, banking system becomes responsible for its transfer among economic agents when payments are due, while credit card companies may also play a prominent role. Deposits therefore account for money which is evidenced by an account at a bank and is its liability. In that sense, deposits are represented in individual bank's information systems as bits, and any bank is expected to certify every transaction by which funds that are legally owned by one person are transferred to some other person. Banking system as a whole acts as a relevant authority that provides assurance to all parties that their outgoing and incoming payments are secure and safe.

With digital currencies it is up to their developers to decide how much of a money to issue and in what manner. Digital currency units exist only as bits. They are essentially unique string of zeroes and ones stored in encrypted computer file, delinked from any material form. As such they are easy to create and reproduce, which contradicts to wanted property of a "good" currency. This is usually referred to as double-spending problem of digital currency. If someone copies bits that represent digital currency he possesses, which is the easiest way to do counterfeiting, he may spend the same digital currency units more than once. The costs of counterfeiting are virtually zero. An intuitive way to address this problem would be to set up a central authority. Its task should be to verify all transactions and keeps a reliable record of them. This kind of central authority has more in common

with central securities depository and clearing house than with both central and commercial banks. The main reason is that currency is not a liability of this authority. As with all institutions similarly designed, its success crucially depends on trust parties involved have in it.

However, some digital currencies have found out novel manner to tackle creation and double-spending problems. Bitcoin is the first digital currency effectively successful in addressing these problems.

ECB (2012) developed a money matrix that summarizes phenomenon of money in today`s world, attaching a special field to what it named as a virtual currency. It is digital currency that fits the best to this notion. Figure 1 replicates this matrix.

Figure 1: A money matrix

<table>
<tr><td rowspan="3">Legal status</td><td>Unregulated</td><td>Certain types of local currencies</td><td>Virtual currency</td></tr>
<tr><td rowspan="2">Regulated</td><td rowspan="2">Banknotes and coins</td><td>E-money</td></tr>
<tr><td>Commercial bank money (deposits)</td></tr>
<tr><td colspan="2"></td><td>Physical</td><td>Digital</td></tr>
<tr><td colspan="2"></td><td colspan="2">Money format</td></tr>
</table>

Source: ECB (2012)

Virtual currency is characterized as digital and unregulated currency. According to ECB, virtual currency schemes may be classified in three groups. A closed virtual currency schemes have no link with the real economy, so the virtual money can only be spent on virtual goods and services. A virtual currency schemes with unidirectional flow allow purchasing of virtual currency with real money at a specific exchange rate, but inverse transaction is not allowed, so purchasing of real money with virtual money is not envisaged. Compensating this is that virtual money can be spent on virtual goods and services, but real goods and services as well. Third type of scheme is the most advanced. In a virtual currency schemes with bidirectional flow users can buy virtual currency with real currency, and afterwards exchange back virtual for a real currency. This convertibility property is accompanied with freely allowed purchase of both virtual and real goods and services.

The next section deals with the concept of the today`s most broadly accepted digital currency – Bitcoin.

4. The Economics of Bitcoin

The emergence of Bitcoin has a theoretical foundation in a paper written by Satoshi Nakamoto (2008). Although, the content of paper can be easily verified, the same does not hold for the creator. Its identity is not revealed and there are strong reasons to

believe that it is a pseudonym not of one person but rather a group of anonymous developers. However, the paper of just nine pages gained planetary popularity since it, in a clear and concise way, described a mechanics of bitcoin's functioning.

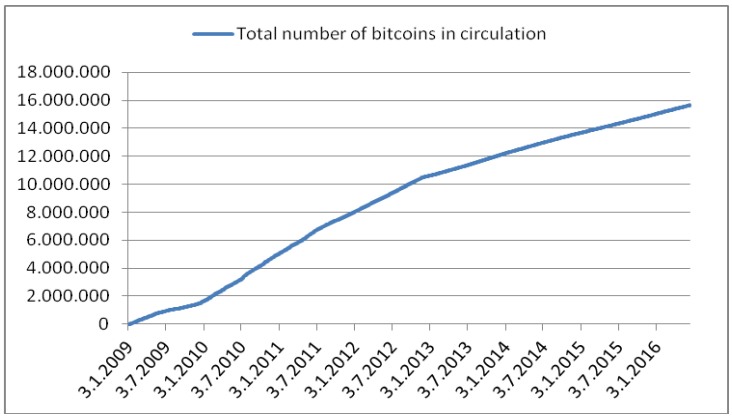
According to the paper, driving motivation of founder was to provide an electronic payment system based on cryptography proof instead of trust, so that any two willing parties were allowed to transact directly with each other without the need for a trusted third party. The system by its design reduces transaction costs. Bitcoin relies on a peer-to-peer networking and cryptography. It is a decentralized structure in which does not exist central clearing house for transactions, or any other kind of financial institution involved. It operates on a worldwide level. It is available for purchases of vast group of goods and services, and there is an online frequently updated database where all sellers that accept bitcoin in exchange for their goods and services are listed. The database has been continuously expanding, witnessing growing popularity of bitcoin.

For a new bitcoin to be created and get into circulation, interested nodes (miners) in network need to engage in a process known as mining. This process is crucial for system operation since its main output is validation of transactions agreed among parties involved. In effect, miners are seeking for a solution of a complex mathematical problem. When they arrive to a solution it is thought of as they discovered, or mined, a new block that is added to a block chain. A valid block consists of a number of transactions that have been recently announced throughout the network by parties involved. In mining real resources are expended – CPU computational power, electricity and time, and accordingly miners are compensated through the issuance of new bitcoins. Böhme et al. (2015) assert that annual costs of power consumption driven by mining are approximately 178 million $, using an average US residential electricity prices. As a consequence, one might think of the value of resources employed as an objective market value of bitcoins produced. In this sense there is analogy between gold mining and bitcoin mining, and also contradiction since bitcoin does not have intrinsic value like gold once it is extracted.

The speed of creation of new bitcoins is predetermined. In the start, each miner was rewarded with 50 bitcoins for every block added to block chain. However, the size of the reward is halved after every 210 000 blocks mined, and as of now it stands at 25 bitcoins. If we know that every ten minutes the new block is discovered, because system varies relevant parameters of mathematical problem so that with the increase in the size of network and computing power time needed for mining the new block does not change, than after every four years halving of reward will take place. With the projected pace of new block creation and accompanied miners' reward the total bitcoin supply is expected to approach but never exceed 21 million. It is expected to occur around 2040. Figure 2 displays current outstanding amount of bitcoins.

By its structural design, bitcoin provides scarcity feature which is a prerequisite for any money to maintain a value. But unlike official currencies, where central bank preserves flexibility in issuing new money, its total supply is finite. As with any scarce good, when supply approaches overall limit closely the value of bitcoin can be expected to rise. Scarcity and predictability of increase in bitcoin supply make up distinctive features of this digital currency. However, while combating the danger of inflation this design gives rise to a deflation, which is a misfortune of present moment in the world economy, linked with forces of recession in many advanced economies, especially those in Europe.

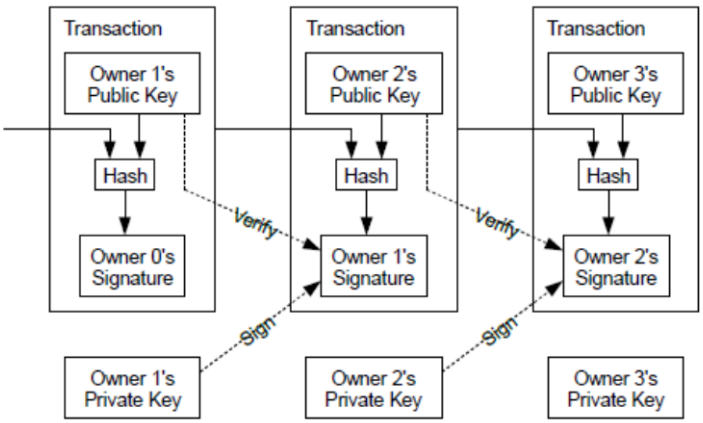
Figure 2: Bitcoins in circulation



Source: www.blockchain.info

Nakamoto (2008) defines an electronic coin as a chain of digital signatures. This view determines the technical aspects of regular bitcoin transaction. Any interested person can join bitcoin network by downloading free software. He accounts for a node in a peer-to-peer network and obtains a "wallet". What a wallet serves for is not storing bitcoins, which is a conventional understanding of a wallet, but rather enables a user to pursue transactions by managing his public and private keys and keep track of a bitcoin`s balance. As with standard public-private key cryptography implementation, one can encrypt message with a public key, which is widely known, and send it to someone else who is equipped to descramble it with a private key he possesses. In effect, when payee sends a payer his public key it is like sending someone a padlock with which to lock a package that is to be sent to him while keeping the key of a padlock in order to unlock it when package arrives. Figure 3 illustrates details of a regular bitcoin transaction.

Figure 3: Sequence of a bitcoin transactions



Source: Nakamoto (2008)

A pattern of bitcoin transactions in Figure 3 emphasizes that what has been followed is actually a path of a single bitcoin. If Owner 0 at the outset owns a bitcoin and agrees to make a payment to Owner 1, he needs his public key. Public key is an "address" by which a user is recognized on the network, or differently put it is his account number. Also, ownership of any bitcoin mined is effectively attached to some address. Owner 0 combines public key of Owner 1 and a hash of previous transactions and adds its signature (private key). The signature is used for encryption. This message is then sent to Owner 1. Messages encrypted with a private key may be unencrypted with corresponding public key proving the authenticity of a sender. When Owner 1 decided to make another payment with very the same bitcoin, he would ask Owner 2 to deliver him his public key and the same mechanism as in phase 1 would follow. As a result, for every single bitcoin complete history of all changes in its ownership, since it was mined, is available. Furthermore, one could argue than bitcoin is just a recorded set of related transactions.

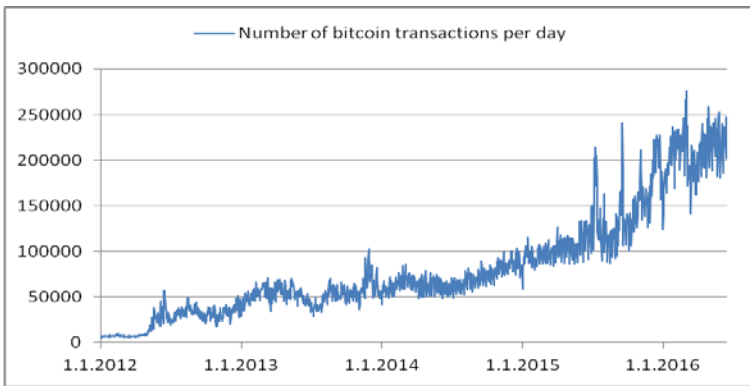
A problem of double spending pops up here. Theoretically, any owner of a particular bitcoin could combine hash of earlier transactions with public key of selected users and add its signature making message that confirms his payment look completely relevant and legitimate. In effect, the owner spends the same bitcoin more than once. The way a bitcoin system moves around this problem is through providing a universal ledger of all bitcoin transactions. Thanks to it, Owner 2 has means to verify that Owner 1 received bitcoin in question from Owner 0 and that there are no prior transactions in which Owner 1 spent the same bitcoin. In bitcoin`s terminology a universal ledger is called the block chain. So if Owner 1 tries to double spend its bitcoin by signing additional transactions, bitcoin system rejects these transactions as invalid because only the first transaction in time counts. Nakamoto (2008) pointed out that the only way to confirm the absence of a transaction was to be aware of all transactions.

In order to implement principle of public knowledge of all transactions every statement about bitcoin transfer between two participants (message) must be published in the network. The transaction is not final by the virtue of public announcement. It appears final only when it is included in the block chain as the part of its last increment. In sum, the block chain is a public good without which a whole bitcoin system would cease to exist. The block chain is a product of accumulated mining effort. It is continuously operational and updated thanks to miners. Providing increment to the block chain is costly, as we already mentioned, and implies delivery of "proof of work" by the successful miners. Proof of work is a solution of a complex mathematical problem. Velde (2013) illustrated it as a search for n such that the resulting hash function $f(x,y,n)$ is less than a set value α, where x is a block chain, y is the proposed added block (increment) and n is some additional number. Since n is impossible to guess, miners need to use a lot of computing power before coming to a solution, whereas the lower the value of α, the harder is to find a solution. At the end, the proof of work must be verified by majority of nodes in the network. An increment contains information on all observed transactions that have taken place since the last increment was successfully incorporated in the block chain. A verification of a new increment triggers working on a next increment containing new pending transactions. It is important that the entire network of nodes agrees on the total historical ordering on all blocks in the block chain.

The analysis above confirms that bitcoin protocol addressed effectively two challenging issues for digital currencies – creation of currency and double- spending.

As a final thought, a pure user`s perspective of bitcoin usage will be outlined. In general, following benefits for the payer may be discerned: anonymity, low transaction costs, global coverage, and relatively short settlement time. The payee (merchant) finds low cost of acceptance (including starting fee) and no possibility of chargeback as main advantages. Online merchants specialized in computer software and hardware dominate over others. Figure 4 depicts a demand for the bitcoin in terms of daily number of transactions. In just four years, number of bitcoin transactions per day went up from low 5000 to over 200 000. Still, there is little evidence of structure of these transactions.

Figure 4: Number of bitcoin transactions per day



Source: www.blockchain.info

Yermack (2013) argues that bitcoin appeals to two distinct clienteles – technology enthusiasts and a special group with pseudo-Liberterian political beliefs who favour bitcoin due to lack of any connection with government. A group of commentators take a view that bitcoin is the most appealing to those involved in illegal activities. Those commentators emphasize a case of the Silk Road, anonymous market place for illegal drugs, which accepted only bitcoins for payments. Speculators certainly account for an important group of bitcoin holders. Grinberg (2011) argues that a growing ecosystem surrounds Bitcoin consisting of exchanges, transaction services providers, market information providers, escrow providers, joint mining operation and others.

5. Conclusion

Overall, the impact of digital currencies should be carefully considered. The principles and mechanics underlying these currencies can be easily reused in terms of fueling development in the circulation of official currencies and transition to the cashless society. It is not unthinkable situation in which even existing financial institutions decide to launch their own digital currency. On the back side, new currencies raise challenges that should be actively managed in order to prevent misbehavior. In sum, these currencies will likely make prominent impact in monetary sphere, although they are far less likely to rule out official currencies.

References

1. Böhme, R., Christin N., Edelman, B., Moore, T. (2015) Bitcoin: Economics, Technology and Governance. *Journal of Economic Perspective*s, Vol (29): 213-238.
2. Dwyer, G. (2015) The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, Vol (17): 81-91.
3. European Central Bank (2012), *Virtual Currency Schemes*, Frankfurt: European Central Bank.
4. Gans, J., Halaburd, H. (2013) Some Economics of Private Digital Currency, Rotman School of Management Working Paper No. 2297296: 1-28.
5. Grinberg, R. (2011) Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science and Technology Law Journal*, Vol (4): 160-207.
6. Grover, D. (2006) Would local currencies make a good local economic development policy tool? *Environment and Planning C: Government and Policy*, Vol (24), 719-737.
7. Harvey, C.(2014) Bitcoin Myths and Facts, Duke University – Fuqua School of Business Working Paper: 1-9.
8. Kristoufek, L. (2015) What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis. *PLoS ONE*, 10(4): 1-15.
9. Luther, W., White, L. (2014), Can Bitcoin Become a Major Currency, George Mason University, Working paper in Economics, No. 14-17: 1-7.
10. Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System, Unpublished paper available at http://bitcoin.org/bitcoin.pdf.
11. Plassaras, N. (2013) Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF. *Chicago Journal of International Law*, Vol (14): 377-407.
12. Velde, F. (2013) Bitcoin: A Primer. *Chicago Fed Letter*, No. 317: 1-4.
13. Yermack, D. (2013) Is Bitcoin a Real Currency? An Economic Appraisal, NBER Working Paper No. 19747: 1-22.

ZVANIČNE NACIONALNE VALUTE I NJIHOVE ALTERNATIVE

Apstrakt: Osnivanjem prvih centralnih banaka države su postavile temelje suverenog upravljanja monetarnim sistemom u nacionalnim okvirima. Uvedene su nacionalne valute kojima je pravno obezbeđen status jedinog zakonskog sredstva plaćanja i prometa. U današnje vreme, nedodirljivost ovog monopola je uzdrmana mogućnostima savremenih tehnologija i pojavom digitalnih valuta. Ovaj rad se bavi analizom njihovih opštih ekonomskih i društvenih implikacija sa fokusiranjem na slučaj najuspešnije među njima – Bitcoin-a. U radu se ističe da paralelno sa nepovoljnim uticajima ovih valuta, koji nisu mali, mogu da se izdvoje i pozitivni. Vodeći među njima je doprinos budućem razvoju novca, obzirom da se koncept i mehanizam funkcionisanja privatnih digitalnih valuta mogu jednako dobro usvojiti i primeniti i u svetu konvencionalnih valuta i postojećeg finansijskog sistema. Zbog svega toga digitalne valute će veoma verovatno imati zapažen uticaj na monetarni sistem, ali je verovatnoća da će biti u stanju da prevaziđu zvanične valute po snazi uticaja srazmerno mala.

Ključne reči: novac, monetarni sistem, digitalna valuta, Bitcoin