# Digital Currencies: Beyond Bitcoin

Hanna Halaburda
NYU-Stern and Bank of Canada; hhalaburda@gmail.com

**Abstract**
In this article, we review the recent developments in the digital currency landscape. We survey the economic drivers that led to the creation of digital currencies and show that they are a natural step in the evolution of means of payment. We overview two major classes of digital currencies, cryptocurrencies and platform-based digital currencies and discuss how the design of such currencies affects the incentives of their users and ultimately their popularity. Finally, we discuss competition in the digital currency market.

**Keywords**: digital currencies, cryptocurrencies, network effects

Digital currencies have been one of the more intensely debated topics on the intersection of technology and economics over the last few years. In a way, this is not surprising. As we discuss below, digital currencies have the potential of significantly influencing the way we transact and the way our marketplace operates. At the same time, these potentially momentous changes, when seen through the lens of economics, can be understood as natural stages in the evolution of the way we execute economic exchange and the way our marketplace works. Initially the discussion of these developments was limited to the creation of “cash for the digital marketplace,” opening up the possibility of replacing costlier and more cumbersome technologies such as payments via credit cards. Today, the promise of digital currencies seems even greater, with potential applications to the way we organize our payment infrastructure, clear transactions, or even write contracts.

This review will discuss digital currencies in this context. Readers interested in a more in-depth discussion of the topics covered here are welcome to consult ``Beyond Bitcoin’’ by Halaburda and Sarvary (2016)[1] for a fuller, book-length treatment. In the brief review here, we will describe the economic needs that means of payments satisfy, and sketch their evolution from the archaic, to today’s cash, to digital currencies. Of course, while the evolution might in hindsight seem inevitable, we should not trivialize the technological developments that allowed digital currencies to appear. For example, the insights that went into the creation of Bitcoin and the development of “blockchain” solved a longstanding problem in information science and are nothing short of groundbreaking. Bitcoin’s ingenious use of cryptographic tools gave rise to the name of “cryptocurrency,” now shared by hundreds of digital currencies that utilize similar technology. Importantly, we will not limit our attention to Bitcoin – the first fully fledged, and still the dominant cryptocurrency at present. We will discuss the proliferation of the blockchain

[1] H. Halaburda and M. Sarvary (2016). Beyond Bitcoin. Palgrave Macmillan.

technology, the rapid growth in the number of other cryptocurrencies, and – again – the economic needs that these newer creations satisfy. Finally, we will explore less discussed, but also very impactful class of digital currencies: currencies that have been issued by internet platforms such as Facebook or Amazon, that we collectively denote here as “platform currencies.”

This review, by necessity, is only an introduction to these fascinating issues and the limited length of this article does not allow us to give them justice. In particular, we will keep to the minimum the discussion of the technological innovations underlying digital currencies, if only because it has been covered in great detail in a variety of other sources. We will instead focus on the economic underpinning of digital currencies and how economic needs explain their creation, design features, and what they suggest for the future. Even here we will sometimes highlight an issue but refer to a study that may investigate it in more detail.

## 1. Digital currencies as a development in the history of money

To discuss the topic, we need to go back to the origins of money and the reasons why money was introduced and why it replaced barter as the dominant system of exchange.[2] Barter, or the direct exchange of goods or services for other goods or services, critically depends on “double coincidence of wants,” that is, on finding a seller that has something you want, and desires something you are willing to offer. If the exchange makes both parties better off, then trade happens. The key problem with barter is that this “double coincidence of wants” may be rare in practice.[3] Moreover, for some seasonal but perishable goods the coincidence of wants, even if it exists, may not lead to an exchange. For example, surrendering goods and waiting for a few months for the counterparty to reciprocate may expose the first trader to so much risk as to limit or even eliminate the gains to trade.

These frictions were alleviated in hunter-gatherer groups by relying on collective memory of the group.[4] The collective memory served as a ledger, recording each member’s contribution and allowed the group to impose penalties to minimize potential free-riding. This reduced the need for the double coincidence of wants to occur: one may receive a good or a service from other group members as long as that person’s contributions might be useful for the group at

[2] The history of money is a fascinating area of research. The discussion below highlights the key dimensions identified by prior studies, with a more complete discussion available for example in J. Weatherford (1997), The History of Money, Three Rivers Press; N. Ferguson (2008), The Ascent of Money, Penguin Press; or F. Martin (2014), Money: The Unauthorized Biography, Knopf.

[3] W.S. Jevons (1875), Money and the Mechanism of Exchange. London: Macmillan.; Nobuhiro Kiyotaki and Randall Wright (1989), 'On money as a medium of exchange', "Journal of Political Economy" 97, pp. 927–54

[4] J.C. Altman (1987), Hunter-gatherers today. Canberra: Australian Institute of Aboriginal Studies.

another, possibly unspecified time. Using a modern term, we could characterize this situation as extending credit.

The collective memory system worked well in small groups, but it could not sustain larger communities. With more members, it is increasingly difficult to keep track of each person's contribution to and consumption of the group's resources. Moreover, as groups increase, it becomes less likely that the trading partners would know each other, making it more difficult to enforce the "borrower" to repay the favor in the future. (For this reason, collective memory arrangements are also poor at facilitating trade between separate groups.)

In time, collective memory was replaced by the institution of money. One way to think about how money facilitates trade is to imagine a ledger recording each party's contributions. That ledger could be either virtual, held in the memory of the group, or could become material and decentralized through the development of money. Contributing to the needs of others increases the balance of the (de facto) seller of a good or service, with such balance being represented by material objects in the seller's possessions; historically such objects may have been tokens such as shells, but gradually evolved to standardized pieces of metal, still functioning today as coins.

The basic discussion above helps us outline both the economic need that digital currencies satisfy and the major technological impediment that they faced. The need is straightforward: the desire to affect economic transactions in the digital marketplace. Until the introduction of the digital currencies one could transact over the Internet using credit cards, or resort to time consuming and hence also costly process of exchanging the good being bought and a more traditional payment method (e.g., checks). Moreover, using either method could be considered relatively intrusive, revealing to the seller the personal details of the buyer.[5]

While the idea of using a digital equivalent of cash has been long proposed and widely anticipated, there was a basic technological problem that had to be overcome. This problem is counterfeiting. This term, usually used in the context of traditional money, denotes the manufacture of a copy that is similar enough to the original currency that it may be accepted by seller as valid payment for their good and services. Worryingly for any digital currency, such copying is trivial with digital information: one can imagine copying the underlying information bit by bit for a simulacrum that is indistinguishable from the original. Generally, it is seen as a good thing, but occasionally it creates a problem. For example, widespread music and software piracy is a consequence of this low-cost copying possibility. While for music or software it is a problem these industries struggle with but may be able to solve, it is a disaster for money. It opens up the risk that whoever holds a unit of a digital currency may create multiple copies and then spend each of them, possibly with a different seller. Any digital currency needs to solve this "double spending" problem before it can be effectively used in the marketplace.

The potential for creation of perfect copies means that digital currencies need to rely on a form of a ledger, keeping track of each unit of the currency and recording whether a given owner has

[5] There are intermediaries that help ensure the privacy and safety of the personal data of the people transacting, for example, PayPal. We do not discuss them and their role in the digital marketplace in this review.

already spent it or not. (The idea behind such a ledger is essentially the same that we discussed above in the context of communal memory, and the same again in the context of banks, holding the record of funds held in and withdrawn from a given account.) Historically, two different implementations of this idea have arisen. First, one could simply rely on a third party institution to safeguard the ledger and ensure that its entries reflect the transactions and correctly credit and debit accounts of each user of the digital currency. Over the years, a number of such digital currencies have been issued by internet platforms, that is, organizations that link two sides of a marketplace (for example, buyers and sellers). We discuss them in the second part of this review.

The second implementation is technologically more challenging, but is nowadays more popular or at least much better known. One could try to make the ledger distributed, with no one party having the sole control over the ledger and its entries. At first blush, this seems impossible. After all, distributing a ledger across users would make it easier for market participants to manipulate the entries – for example, a buyer may not want to deduct enough from his account in his own copy of the ledger; a seller may be inclined to record a larger sum than he earned. The ledger would then quickly become untrustworthy and the digital currency would stop functioning. This problem was considered difficult or impossible to solve in fully decentralized system, and had been a long standing challenge in cryptography community.[6]

## 2. Bitcoin and incentives in its ecosystem

This changed with the publication of Nakamoto (2008).[7] The pseudonymous author of that paper has proposed a way of solving the "double spending" problem and described an algorithm that achieves that. The solution was based on the idea of blockchain: a ledger that can be freely distributed (i.e., decentralized) and that relies on cryptographic tools to allow all users of the network to verify its consistency and preclude them from making unilateral changes. The blockchain records all transactions involving Bitcoins and allows users to verify where each particular unit of the currency came from and whether a given user has the right to spend it in a transaction. As we mentioned above, the use of cryptographic tools in the Bitcoin algorithm led to the name for Bitcoin and subsequent similarly decentralized digital currencies: cryptocurrencies.

Interestingly, the paper's motivation for this algorithm is based on the economic arguments we discussed above: Nakamoto (2008) recognizes the cost of using traditional means of payment

[6] H. Halaburda and M. Sarvary (2016). Beyond Bitcoin. Palgrave Macmillan.; P. Vigna and M. J. Casey (2015). The Age of Cryptocurrency. St.Martin's Press.; J. Pagliery (2014). Bitcoin and the Future of Money. Triumph Books.

[7] There have been a few earlier implementations, but they suffered from a variety of weakness and were not adopted nearly as widely as Bitcoin. See Halaburda and Sarvary (2016) or Vigna and Casey (2015) for details.

(for example, credit card) over the Internet and argues that they limit the span of the economic transactions that the Internet could potentially allow. For example, the costs of using a credit card could make micropayments impossible, precluding transactions involving items that may be worth very little (e.g., a few cents, or even a fraction of a cent – say, a digital picture, the ability to read a single article hidden behind a paywall, etc.). Moreover, the algorithm allows for transactions that are cleared relatively quickly – not instantaneously, as is sometimes incorrectly believed, but typically within minutes, so a much shorter time frame than that required for, say, sending a check.

One more economic need that Nakamoto (2008) mentioned was the need for privacy – while Bitcoin's viability may not critically depend on that single dimension, it undoubtedly appealed to a number of initial users of that cryptocurrency. The first widespread adoption of Bitcoin happened in the shadow economy – the perceived anonymity and the speed and low cost of transactions appealed to users who were, for example, trading illicit substances over the internet.[8] Over time the cryptocurrency has become adopted more broadly, although in some circles it was still driven by the fact that it operates outside of the government system. For example, it has been used to support the Wikileaks project,[9] and has been appealing in times of crises (e.g. the Cyprus banking crisis,[10] in reaction to Brexit referendum in 2016[11]), or when users may have concerns about or face friction when using their national currency (e.g., Argentina and China).

For some of such users the attraction of Bitcoin is that it operates outside of the banking system and is not subject to oversight and management by a central bank. These characteristics feature prominently in Bitcoin's design. The supply of the currency is governed by an algorithm, so that users know exactly how many Bitcoins are outstanding at a given moment and how the supply will change in the future. The total supply of Bitcoin is capped, with the limit to be reached around 2140, reflecting the idea that once the cryptocurrency is widely adopted, the

[8] For example, the cryptocurrency has been used on the Silk Road website, see for example Andy Greenberg, ``End of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market,'' in Forbes Oct 2, 2013, available at http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/#7faa4810347d (accessed July 3, 2016).

[9] See shop.wikileaks.org/donate (accessed July 3, 2016) and also Jon Matonis, ``WikiLeaks Bypasses Financial Blockade With Bitcoin,'' in Forbes Aug 20, 2012, available at http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin/#36b16f9666c4 (accessed July 3, 2016)

[10] See, for example, Jeff Cox ``Bitcoin Bonanza: Cyprus Crisis Boosts Digital Dollars'' for CNBC News Network on Mar 27, 2013, available at http://www.cnbc.com/id/100597242 (accessed July 3, 2016)

[11] See, for example, Ari Levy ``Bitcoin gains validity as digital gold after Brexit vote'' for CNBC News Network on Jun 27, 2016, available at http://www.cnbc.com/2016/06/27/bitcoin-gains-validity-as-digital-gold-after-brexit-vote.html (accessed July 3, 2016)

total supply will be fixed to preclude inflation or any "meddling" with the currency, say quantitative easing.[12]

While the design of Bitcoin addressed some economic needs outlined in Nakamoto (2008), it also created a set of incentives in the Bitcoin's ecosystem that eventually became a weakness for the cryptocurrency. These incentives relate to mining, or how the Bitcoin algorithm governs changes to its blockchain.

To ensure the blockchain's immutability, when new transactions are added to the blockchain they need to be accompanied by proof-of-work. In essence, proof-of-work is a solution to a puzzle posted by the system that can be quickly verified (confirming it is indeed a solution) but requires substantial computational power to find. Network participants who try to solve this puzzle are called miners, and they are rewarded with newly minted bitcoins for their activity. Their existence is critical to the Bitcoin network, but also imposes an externality on the system.

First, mining requires substantial energy; the needs are large enough for miners to consider moving to countries where energy is relatively cheaper, for example to Iceland or China. The energy outlay keeps the Bitcoin system going, but leads to the question of whether other cryptocurrencies may be more energy-efficient than Bitcoin.

Second, mining is a competitive activity, with the winner-take-all dynamics: the miner who first solves a given puzzle earns the entire payment for the puzzle (the newly issued bitcoins[13]), with other miners receiving nothing regardless of how much work they may have done. This has led to an arms race in the mining community. Since even a slight improvement may affect the miner's chances of winning the race, successful miners need to constantly invest in their mining systems, nowadays built from dedicated hardware designed for mining Bitcoin. The race may not only be socially wasteful, but it also distorts the composition of the mining industry, increasingly tilting the balance towards elite miners who have the best mining equipment. One way for miners to respond is to join forces and set up collectives called "mining pools" that cooperate on the solution to the puzzle and share potential rewards among its members. The consequence of these developments is the loss of de-centralization and the risk that eventually a single miner (or, more likely, a single mining pool) may become powerful enough to threaten the integrity of blockchain and put the existence of the network into question.[14] Moreover, to the extent that the potential upgrades to the Bitcoin algorithm must be accepted by the

[12] To the extent that the intent of this design feature is to make Bitcoin independent of any central authority, that goal is accomplished. It is less likely that the fixed supply would make prices better behaved and more predictable to market participants: for example, there is a concern that the fixed supply will cause a deflationary pressure on the cryptocurrency. (See Halaburda and Sarvary, 2016)

[13] We follow the accepted convention where the word ``bitcoin'' is capitalized if used in the context of Bitcoin system or protocol, and it is not capitalized if used in the context of currency unit.

[14] This possibility, known as the "51% attack," requires the super-miner to control more than half of the computing power of the Bitcoin network.

majority of the network before they are deemed valid, the presence of super-miners might change the dynamics of how such decisions are taken.

Third, some elements of Bitcoin's design may be counterproductive to its general adoption and its use as an everyday currency. For example, volatility in the price of Bitcoin (that is, the rate of exchange between bitcoins and traditional currencies) has been so large that some people doubt Bitcoin's validity a currency. While much of the volatility may be driven by speculation, it may also be a consequence of the fixed supply of the cryptocurrency, limiting the ability to offset changes in demand by correspondingly changing the supply.

Some of these difficulties are purely technological (e.g., energy consumption) while others are more economic (e.g., the incentives induced by the tournament structure of the competition between miners). Interestingly, the same two types of problems arise with traditional currencies. For example, on the economics argument side, central bank policies may harm the viability of a currency and perhaps even induce consumers to switch to a foreign currency instead.[15] Similarly, technological challenges may make a traditional currency easier to counterfeit or simply too expensive to produce. One illustration of this may be the decision of the US Mint in 1982 to replace copper with zinc when producing 1 cent coins in an effort to reduce the cost of production (e.g., Weatherford, 1997). The cost of electricity needed to produce Bitcoin can be seen in the same context.

## 3. Cryptocurrencies other than Bitcoin

As Bitcoin gained popularity, its weaknesses were becoming increasingly apparent. At the same time, being open source, the algorithm behind Bitcoin has been incorporated into new cryptocurrencies that attempted to fix its drawbacks. [16] New coins (altcoins) mushroomed, with about 700 cryptocurrencies being traded one for another (or for traditional currencies) via online exchanges. Presumably, many more cryptocurrencies have been created, although some may have never won enough popularity to lead to meaningful trade. Such proliferation is in fact fairly typical in innovative markets, especially technology. Once there is a product that successfully solves an outstanding problem, new competitors come in – some that aim at improving over the first-mover, and some that are just mere copies or almost copies.

Here we will focus on a few altcoins that changed the design of Bitcoin to address an outstanding issue.[17] One of the early competitors to Bitcoin was Litecoin, created in October

[15] For example, the US dollar has replaced the Zimbabwean dollar as a preferred means of exchange; see "In dollars they trust," the Economist, April 27, 2013.

[16] At the same time, a number of cryptocurrencies have been created with at most cosmetic changes to the Bitcoin's algorithm. Such copycat "me too" altcoins provide no real difference from Bitcoin and while some might win passing popularity, they are perhaps unlikely to meaningfully reshape the cryptocurrency ecosystem.

[17] Please consult Halaburda and Sarvary (2016) for a more in-depth treatment.

2011 by Charles Lee. This altcoin attempted to simplify the cryptographic tools used in Bitcoin and lessen the computation burden miners faced when adding new information to the blockchain. Reducing the complexity of the mining puzzle was thought to alleviate the arms race problem outlined in the previous section. Indeed, initially the requirements and the energy needs to successfully mine litecoins were much lower, returning the possibility for everyday PC users to participate in mining. However, at a deeper level, the problem was not fully addressed and was only postponed for a while. The incentives miners faced were the same as with Bitcoin, with the tournament structure of the mining competition unchanged. As Litecoin's popularity grew, miners again began to invest in ever more powerful mining rigs that in time were designed specifically for the purpose of mining litecoins.

Litecoin was also designed in response to another perceived weakness of Bitcoin: the limited supply of the cryptocurrency. Specifically, it increased the total supply for Bitcoin's 21 million to 84 million. Unfortunately, it is unlikely that simply increasing the number of coins in existence could offset the deflationary pressures inherent in the supply being limited.

Other altcoins, Peercoin and Novacoin, established in 2012 and 2013, respectively, offered a better solution to the problem of mining. Instead of relying on proof-of-work and its resulting tournament structure, they also rely on proof-of-stake mining, which rewarded miners in proportion to their stake in the currency. Instead of depending solely on the competition among the miners, their algorithm randomly selects a miner present in the network to mine the next block in the blockchain, with the probability of being selected increasing in each miner's coin holdings. While the miner still needs to solve a computational puzzle, that puzzle can be meaningfully easier (i.e., require less computational resources) than its Bitcoin equivalent.[18] In addition, both Peercoin and Novacoin also allow their supply to increase at a steady rate, a departure from the fixed supply in the cases of Bitcoin or Litecoin.

Besides altcoins attempting to improve on the above features, there have also been innovations that offer more anonymity than Bitcoin. As we discussed, Bitcoin's blockchain makes the holdings of and transactions in bitcoin public information, even though it may be very difficult to map such holdings and transactions to real-world users. Some altcoins, for example Darkcoin (currently circulating under the name of Dash), do away with this feature, separating transactions from the source of the coins.

## 3.1 Cryptocurrency competition

[18] Both Peercoin and Novacoin initially rely on a combination of proof-of-work and proof-of-stake, only gradually moving to the exclusive use of proof-of-stake mining.

The number of cryptocurrencies in existence leads to the obvious question: could they all survive, and should we expect one cryptocurrency to eventually dominate? Similar questions arise in the context of traditional currencies as well, but the sheer number of the cryptocurrencies and the fact that they were designed to improve on their predecessors suggests that the competition may be much fiercer in this space. In many markets such higher-quality entrants may have a good chance of winning market share, or even taking over the market from a lower-quality first-mover. However, it is not clear that this is the case in the cryptocurrency market, because it is a market with network effects.

Network effects (e.g., Katz and Shapiro, 1985) arise when a good or a service becomes more attractive as the numbers of its users increases. The classic example is the telephone network: a telephone is useless if you own the only one, but its value rapidly increases as there are more phones in the network. This idea translates directly into currencies in general, and cryptocurrencies in particular. Initially, the creator of a cryptocurrency is the only party that recognizes and accepts that cryptocurrency, which makes it difficult to persuade others to adopt it. However, as more and more users appear, the cryptocurrency becomes more attractive (essentially, one has more potential counterparties to trade with: for example, the number of potential bilateral exchanges increases exponentially with the number of users in a network). This property may lead to "winner takes all" dynamics: a cryptocurrency is more useful when more people adopt it, then we maximize the benefit when everybody uses the same cryptocurrency. This suggests that an entrant into the cryptocurrency market may face substantial difficulties if its network is smaller than that of the incumbent. Of course, a large difference in quality (real or perceived) between the entrant and the incumbent may offset the discrepancy in the strength of the network effects. Whether this happens with new cryptocurrencies is an empirical question.

In a recent paper, Gandal and Halaburda (2016)[19] analyze exchange rates between cryptocurrencies for signs of competition between them and potential indicators of which currencies may be winning. Not surprisingly, the Bitcoin, the oldest and the most established cryptocurrency, has entered the competition with stronger network effects, leading some to predict doom for any upstart cryptocurrency that followed the incumbent. Interestingly, this is not exactly what we see in the data. Over the sample studied in Gandal and Halaburda (2016), 2013-2014, one can detect periods in which Bitcoin was indeed gaining at the expense of other cryptocurrencies, but also periods in which altcoins were improving at the Bitcoin's expense.

Earlier on in the sample, various cryptocurrencies studied in the sample move together, with good news for Bitcoin translating into good news also for other cryptocurrencies such as Litecoin, Peercoin, etc. This pattern is consistent with the general increase in the interest in cryptocurrencies, driving their prices up. One way to interpret this pattern is to think about cryptocurrencies as financial assets, the prices of which reflect the future value of the cryptocurrency.  Even if investors may infer that only a single cryptocurrency will eventually dominate, it is not known in advance which one will do so. Consequently, the price of each

[19] N. Gandal and H.Halaburda (2016), ``Can we predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market,'' Games 2016, 7, 16

cryptocurrency may reflect investors’ views on the value of that cryptocurrency (whichever it may be) and the probability that each specific cryptocurrency (Bitcoin, Litecoin, etc.) is the one.

However, the later part of the sample, after April 2014, constitutes a period of clear competition between Bitcoin and altcoins. Good news for Bitcoin translated into bad news for the other cryptocurrencies, consistent with winner-take-all dynamics. Towards the end of the sample, as well as of the time of writing, Bitcoin remained the dominant cryptocurrency. Interestingly, this means that the altcoins that arguably improved on the design have not succeeded in gaining substantial market share. For example, Peercoin and Novacoin, two altcoins that improved on Bitcoin by introducing proof-of-stake, remain relatively unknown. Litecoin has become somewhat popular, (at least, more than other altcoins), even though the quality improvement over Bitcoin was smaller than of Peercoin and Novacoin. The likely reason is the earlier-mover advantage and the ability to build a larger network before another entrant appears. At present it seems that the popularity of each cryptocurrency reflects its age rather than quality, with those cryptocurrencies that were introduced earlier being more popular than their younger brethren.

## 4. Platform-based digital currencies

As we mentioned in the introduction, cryptocurrencies are not the only form of digital currencies. Some digital currencies are centralized, that is, are controlled by an institution that keeps track of who holds how much of the currency and that records all transactions. Because such institutions are typically Internet platforms, we denote these digital currencies platform-based.

While it may seem like a distant memory at this stage, platform-based currencies attracted a lot of attention in the early 2010s. A number of commentators had similar concerns about platform-based currencies to those later raised for cryptocurrencies. For example, Matthew Yglesias (2012)[20] suggested that Facebook Credits, the digital currency introduced by Facebook, may take on state-issued currencies; others voiced the same concern when Amazon introduced Amazon Coins in 2013. Because Facebook and Amazon are large, international platforms that have a large customer base, it was predicted that their private digital currencies could challenge central banks’ monopoly on issuing money.

Subsequent developments showed that these fears did not materialize. Moreover, no new entrant has appeared that would compete with traditional currencies. The platform-based

[20] Yglesias, M. (2012), “Social Cash: Could Facebook Credits ever compete with dollars and euros?” *Slate,* February 29, 2012 (http://www.slate.com/articles/business/cashless_society/2012/02/facebook_credits_how_the_social_network_s_currency_could_compete_with_dollars_and_euros_.html).

currency that arguably came the closest was Q-Coin, issued by the Chinese social platform Tencent. In the early 2000s Q-Coin had rapidly gained popularity in China and eventually started being used as a substitute for the state issued currency, the yuan.[21] This was a testament to both the popularity of this digital currency and a (likely) unintended consequence of its design, allowing it to be freely transferrable outside of the social network. While this was not an intended feature, Tencent had not taken measures against such use until prompted by state regulators. Around mid-2000s the Chinese central bank, the People's Bank of China, started expressing its concerns about Q-Coin's role as a means of payment outside the Tencent social network.[22] Over time, regulation was introduced to preclude this use of Q-Coin, although it is likely that the digital currency continues to be used in the informal economy (see Halaburda and Sarvary, 2016).

Q-Cent notwithstanding, many platform-based digital currencies are designed in a way that effectively precludes their use as everyday currency, as discussed in Fung and Halaburda (2014).[23] Two prominent features of their design are limits to transferability across users and exchangeability for traditional currencies. Many platforms make it impossible for users to transfer the digital currency outside of the platform. For example, World of Warcarft Gold (WoW Gold) cannot be bought or exchanged into national currencies and can only be earned through completing in-game activities.[24] Even within the platform, it may be onerous or just impossible to transfer the currency from one user to another, as was the case with Amazon Coins discussed below.

Such restrictions should not be surprising. Digital currencies such as Amazon Coins are issued by platforms whose business goals do not include provision of well-functioning currencies to the market. Since such platforms have full control over the design of their currencies, it can be expected that they will make it consistent with and supporting their business model, which may invalidate the use of the digital currency as money (e.g., see Gans and Halaburda, 2015).[25] For example, Amazon Coins were designed to stimulate interest in apps written for Kindle Fire and incentivize developers to create new apps for that tablet. The idea was to endow users with Coins (for example, by gifting Coins to customers who bought Kindle Fire; users could also buy Coins directly from Amazon) and allow them to spend the Coins to purchases apps for their

[21] Q-Coin was not linked to or backed by the yuan, and could not be exchanged for the state currency, at least not formally.

[22] See the Govermnent of China news release at http://english.mofcom.gov.cn/aarticle/newsrelease/commonnews/200906/20090606364208.html

[23] B. Fung and H.Halaburda (2014), ``Understanding Platform-Based Digital Currencies,'' Bank of Canada Review, Spring 2014, pp. 12—20

[24]In-depth analysis of currency systems in on-line games can be found in V. Lehdonvirta and E. Castronova (2014). Virtual Economies. The MIT Press.

[25] J.Gans and H.Halaburda (2015), ``Some Economics of Private Digital Currencies,'' in ``Economic Analysis of the Digital Economy, A. Goldfarb, S. Greenstein and C. Tucker (eds), The University of Chicago Press

tablets. The Coins would be earned by app developers, who in turn could bring them to Amazon to exchange them for national currencies, say US dollars. The design features of Amazon Coins become intuitive when we analyze them in this context.

For Amazon Coins to achieve these goals, it was important to limit their exchangeability back to US dollars exclusively to developers. Allowing all users to exchange Coins into dollars would be counterproductive: purchases of Kindle Fire could immediately exchange their Coins and spend them for whatever they wished (not only apps approved by Amazon), reducing the role of Coins to a de facto discount on their purchase. Similarly, it was important to limit to transferability across users. If the Coins were transferrable, one could imagine a situation in which people exchange them for traditional currency, or even directly for goods and services, outside of the Amazon platform. Again, one could see this as consistent with the Amazon's business model. The restriction forces more people to buy apps then they would otherwise, arguably increasing the size of that market and making it more attractive to developers (which again underlines the role of network effects).[26]

Overall, platform-based currencies are designed to support the business model of the issuing platform. This inherently makes it likely that they will be endowed with characteristics that are at odds with their widespread adoption as everyday currency. Consequently, platform-based currencies are unlikely to be a challenge for the national currencies or to affect meaningfully the overall payment landscape.

## 5. Conclusions

In this review we have discussed the new but dynamically changing area of digital currencies. We focused on the economic needs that such currencies satisfy and discussed their role in the marketplace. This framework allows us to understand digital currencies better and to make more informed forecasts about their future.

One area worth highlighting is the continued evolution of digital currencies and the technology that underlies them. We saw how weaknesses in the Bitcoin's algorithm (some real, some perhaps only perceived) drove innovation and competition in the realm of cryptocurrencies. However, the innovation is much broader. The blockchain technology has been utilized in contexts that are increasingly far from currencies. For example, consider the token known as Ripple, which at first blush looks like a cryptocurrency but is use exclusively within the Ripple payment and settlement system. That is, Ripple is not used as a digital currency per se but instead underlies a payment protocol that may be used, for example, to remit and exchange traditional currencies, potentially at a much lower costs than that charged by incumbent

[26] As digital currencies proliferate, there may be those that allow for transferability and exchangeability. At the time of writing, perhaps the best example of a platform-based currency that has this feature is the Linden dollar, used in the online world of Second Life. However, in spite of these attributes, Linden dollars are not thought to be widely used outside that platform.

payment services providers. Another exciting innovation is Ethereum, which uses similar technology to allow for the writing of smart contracts. Such a contract could, for example, make payment conditional on an observable action or quality of a good or service sold, allow parents to give their kids pocket money while at the same time limiting what their children could spend it on, etc. The evolution is ongoing, will undoubtedly bring many spectacular ups and downs,[27] and will be an exciting area to follow in the future.

[27] For example, see the recent smart contract cyberattack on the Decentralized Autonomous Organization (DAO), covered in "Theft is property," the Economist, June 25th, 2016.