



UvA-DARE (Digital Academic Repository)

Bitcoin: not a currency-like informational commodity

Bergstra, J.A.

Publication date

2014

Document Version

Final published version

[Link to publication](#)

Citation for published version (APA):

Bergstra, J. A. (2014). *Bitcoin: not a currency-like informational commodity*. (TCS Electronic Report series; No. 1411). University of Amsterdam, Theory of Computer Science. <https://ivi.fnwi.uva.nl/tcs/pub/tcsreports/TCS1411.pdf>

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.



University of Amsterdam
Theory of Computer Science

Bitcoin: not a currency-like informational
commodity

J.A. Bergstra

J.A. Bergstra

section Theory of Computer Science
Faculty of Science
University of Amsterdam

Science Park 904
1098 XH Amsterdam
the Netherlands

tel. +31 20 525.7591
e-mail: J.A.Bergstra@uva.nl

Bitcoin: not a currency-like informational commodity

Jan Aldert Bergstra
Informatics Institute, University of Amsterdam
email: j.a.bergstra@uva.nl

October 1, 2014

Abstract

Six assertions concerning the status of Bitcoin are formulated and defended: (i) Bitcoin is not and will not become a currency-like informational commodity, (ii) currency-like informational commodities that aren't currencies must be frauds, (iii) specific BTC amounts may become monetized and thus may be turned into financial assets, (iv) currently no BTC amounts are monetized in any currency area and therefore none are financial assets, (v) by means of bureaucratic steps only some BTC volumes can be turned in to an informational currency within a given currency area, modified client software is not required for that step, (vi) if a specific amount of BTC qualifies as currency, it also qualifies as money, (vii) moneyness of Bitcoin, or rather of a specific occurrence of an amount of BTC, should be questioned only after one has agreed positively on its status as a financial asset, and negatively on its status as an amount of currency.

Factions in the Bitcoin promoting movement are viewed from a perspective of organizational multi-threading. Different factions of the Bitcoin movement may wish to see status issues about Bitcoin settled in different ways. Overall consistency in these matters should not be expected from the union of factions in the Bitcoin movement.¹

Keywords and phrases: Bitcoin, informational money, informational commodity, money-like, currency-like, organizational multi-threading

1 Introduction

A vast number of papers and blogs have been written about questions related to the status of Bitcoin in terms of the classical financial jargon: is it money, is it a currency, is it a financial asset, is it a commodity, and so on. New papers on that subject appear on a daily basis.

¹Presented at the Bitcoin meet up of September 30 2014 in Amsterdam.

None of these questions are easy, and few of the existing papers seem to be conclusive concerning the point the author intends to make. It seems that one may only progress if assumptions about the meaning of financial terms (except Bitcoin) are made explicit. I will speak of background terminology when referring to the financial jargon that existed before money-like informational commodities such as Bitcoin arrived on the scene.

Authors who disagree on the meaning of background terminology are likely to disagree about the status of Bitcoin as well. I will try to contribute to the discussion first of all being explicit about my assumptions concerning the background terminology. Obviously my assumptions to that extent can be criticized and who opposes one or more of these assumptions concerning the meaning of the background terminology is likely to disagree with some of my assertions regarding Bitcoin. In that case a disagreement about aspects of Bitcoin has causes outside Bitcoin.

I will take as a point of departure the classification of Bitcoin from [13] (which we saw convincingly confirmed in [15]) suggesting that Bitcoin (or rather specific amounts of BTC) constitute(s) (instances of) a money-like informational commodity (MLIC). MLIC is considered a base type for Bitcoin.

2 Assumptions concerning background terminology

My assumptions on background terminology are these:

1. “Money” is primarily a philosophical notion. Even if some law-maker states that some commodity, be it informational or not, constitutes money, that may fact be irrelevant, and for that reason it may be largely ignored, at least from a philosophical viewpoint.
2. The scholarly works on economics provide necessary, or at least widely accepted, criteria for moneyness but seem not to provide sufficient criteria for moneyness. Economics does not pretend to be responsible for defining the concept of money so to say. (I made an attempt to define money as well as virtual money in [1].)
3. Currency on the other hand is not a primarily philosophical notion, currency-ness of a commodity is a matter of that commodity (inclusive its handling system and conventions) having been accepted as currency by a national bank of some well-recognized national or supranational entity (below called currency area, also called currency region). Currency within a currency area

is under control of the central bank of that currency area, which may in various ways be under control of the political structures dominating the currency area. Classically, that is before the advent of informational currencies, currency areas are geographic entities composed of one or more countries.

4. Within a currency area there are local currencies, usually only a single one. Foreign currencies are currencies of other currency areas.
5. If within a currency area the central bank changes the currency and replace it for another currency, instances of the old currency do not constitute currency anymore, but may still qualify as money.
6. The family of existing currency areas evolves in time. Splitting of countries/nationalities into different nationalities may lead to new national identities that create new currencies, while combinations of national identities may combine their currency areas. Nowadays currency areas composed of coherent combinations of nationalities, still mostly consisting of a single nation. The Eurozone is an example of a currency area that consists of a significant (and still growing) number of nations. Different currency areas maintain different currencies.
7. An amount of any currency is by definition considered to be currency-like as well. (Thus an informational commodity being currency-like will not exclude it being a currency.)
8. An informational currency is an informational money that qualifies as a currency. One may distinguish local and foreign informational currency. Some informational monies may fail to be informational currencies. At the time of writing of this paper no informational currencies are in existence to the best of my knowledge.
9. Currency-likeness is close to being a contradictory concept. Though fraud may lead to specimen of commodity that are so similar to specimen of an existing currency that one may claim commodity-likeness for it. Commodities that are currency-like but that don't qualify as currency for that reason must be manifestations of fraud. Here it is assumed that the similarity with instances of an existing currency do not arise by accident, in spite of the theoretical possibility of such an almost miraculous event.
10. Even if some specific amount of a money-like informational commodity (MLIC) is considered currency in some national system that does not imply that each amount of that MLIC is currency in that same currency area.

11. An amount of some commodity will be classified as currency if in some currency area it qualifies as currency. It is plausible, in the sense of being assumed by default, that a “positive” classification in some currency area implies the same equally positive classification in other currency areas (which of course may not recognize it as “own currency” but rather as a foreign currency).
12. Constituting a financial asset is not primarily a philosophical notion. Financial asset is a technical phrase used in the world of international banking. Its meaning is codified by organizations such as the IMF.
13. A remarkable property of the notion of a financial asset is that a particular specimen of some commodity may or may not be a financial asset depending on the particular history of that specimen. For instance a gold bar that has been monetized (placed on the balance sheet of a central bank against some value expressed in that bank’s own currency) qualifies as a financial asset, but after it has been sold (by the same national bank) to some private party (against a price that may be different from its original valuation in the balance sheet) that very same gold bar is merely a valuable commodity but not a financial asset anymore.² If the national bank once more buys that particular gold bar it becomes monetized once more and its status is that of a financial asset again and so on.
14. All amounts of currency (local or foreign) are financial assets as well.
15. Although the phenomenon of charging, receiving, promising, and paying interest has been a familiar feature of most currencies the presence of the feature of (non-zero) interest (with the mentioned four actions) as such is not a necessary condition for a commodity constituting either a currency or a money. In [2] as a sequel to [8, 9] I have discussed Bitcoin in relation with Islamic Finance (IF), an important argument being that in the setting of Bitcoin the feature of interest is less plausible. Although in IF interests play no role, to the extent of being prohibited, there seems to be no dispute concerning the moneyness of local currencies of currency areas that have adopted the principles of IF.

²The same holds for banknotes and coins. These need to be monetized before (that is in order to) make the transition from commodity to currency and can make the inverse transition by being demonetized.

3 Remarks on Moneyiness and Currencyiness of Bitcoin

Below I will list a number of observations on Bitcoin most of which are directly based on the above assumptions.

3.1 Currency-like informational commodities are either currencies or frauds; this applies to Bitcoin as well

An instance of a currency-like informational commodity must be a fraud because currencyiness be it local or foreign is a matter of formalized acceptance/adoption as such by some central Bank. That in principle can be checked by asking each of those in specific cases.

In particular Bitcoin is unlike ever to constitute a currency-like informational commodity unless it already qualifies as a currency. As long as in general BTC amounts don't qualify as currency (w.r.t. to some national system), specific amounts and contexts where those amounts are handled that are currency-like must be labeled problematic.

3.2 By default Bitcoin isn't a currency-like informational commodity

By asserting that Bitcoin (that is specific amounts of BTC) don't constitute a currency-like informational commodity one may express a default assessment. In a specific (that is non-default) case the setting in which someone encounters a specific amount of BTC may have been engineered in a misleading manner such as to convey the impression that an amount of (legalized) currency is at stake. The title of the paper should thus be read as: "by default a specific amount of Bitcoin is not specimen of a currency-like informational commodity, while in exceptional circumstances (which are ruled out by default) it might be a currency-like entity".

3.3 Specific amounts of Bitcoin may be monetized

I will use N as the name parameter of a currency area, below denoted with CA_N . N will be used as a parameter for related entities such as the central bank and the "own" currency of the area.

The central bank CB_N of currency area CA_N may (at least in theory, that is as a thought experiment) buy a specific amount of Bitcoin and put that on its balance sheet. The result of this action by CB_N will be that this particular

amount of BTC has been monetized (and for that reason by definition has become a financial asset) while at the same time other amounts of BTC still are non-monetized and don't count as financial assets.

As soon as that amount (or a part of it) of BTC is back in the hands of a private entity (or any entity which is not a central bank of any currency area) it would not be monetized anymore and would not constitute a financial asset.

Comparable to the case of gold bars it appears that for an amount of BTC its status of constituting a financial asset is merely a transient property of the history (and of the current ownership) of that amount.³

3.4 The interest mechanism is indecisive for either currency or money of Bitcoin

Whether one classifies an amount of Bitcoin as money, as currency, or as a financial asset, its capacity of generating interest is independent of that assessment. In [4] it has been argued that it is implausible to link Bitcoin with interest payment and that argument is central to [2]. The argument put forward by some that once Bitcoin has been recognized as money its holdings will generate interest is flawed unless one understands and agrees that interest can be zero or negative just as well. Negative interest on Bitcoin seems to be an irrational feature, however.

3.5 Chunks of Bitcoin can be turned into currency by any central bank: Bitcoin as a currency

Bitcoin has the remarkable flexibility of being used as money (with currency status) against a value expressed in the currency of a currency area. An argument for this assertion runs as follows. If the central bank CB_N of a currency area say CA_N with currency C_N buys or mines an amount A of BTC (which may happen in several stages) that specific amount may be monetized by being included in the balance sheet of that central bank for a nominal value say v_n which is deliberately chosen to be far above its current exchange rate against the local currency. Here the exchange rate of Bitcoin expresses the price of BTC in terms of C_N , with BTC merely considered an informational commodity.

I will speak of a chunk of BTC to denote all subsequent descendants of a

³It seems that while for a money-like commodity becoming a money is connected with becoming accepted by the public at large in a statistical manner, becoming a financial asset is precisely determined by its being acquired by a national bank (that is the central bank of a currency area).

particular amount or set of amounts. A simple inspection of the blockchain allows to validate that an amount is part of a given chunk, this check can be applied at all times after the chunk has been named (identified) by way of a defining transaction. The parameters of the chunk may be made public without incurring an infringement of anyone's rights.

The chunk of BTC consisting of all and only BTC amounts that are descendants of the amounts that CB_N has ever acquired and has placed in its bookkeeping against a nominal value of $v_n C_N/BTC$ are redeemable at par (by CB_N) against $C_N \cdot v_n$ per BTC (in the chunk!). CB_N can allow banks in its currency area to freely use precisely these amounts of BTC (and fractions of it). At some stage the current exchange rate may exceed v_n .

Now what may happen to this "Bitcoin as a currency" is what has happened with traditional metallic coins so often in the history of money: the commodity value of a specific brand of coins exceeds its nominal value and for that reason the coins are taken out of circulation by the public. After melting the coins and recovering the constituting metals these can be sold at a profit.

This course of events used to be a significant problem for coin based monetary systems but in the context of BTC it should not be a big worry. This state of affairs is not a big problem for CB_N as it can sell (and demonetize) its BTC remaining holdings with profit and it is under no obligation to redeem that part of the chunk which is in the hands of the public (though monetized) against more than the nominal value (though it may wish to do so in order to motivate the public to deliver these BTC's back).

I conclude that chunks of Bitcoin may not even become financial assets by being monetized but may in excess of that become legal tender money within a given currency area without the need of making any significant change of the software. It follows that in the sense of being legal tender money that property is a contingent property of specific amounts (chunks) of BTC. It may change in time, and it may change without needing fundamental changes in the financial system. It should be noticed that a chunk of BTC which has been made legal tender money this way is still protected against C_N 's much feared home grown inflation (of its own currency) because of the underlying Bitcoin mechanism, at least as long as a "free" market for BTCs is allowed or in existence.

3.6 Bitcoin can do without a market

Bitcoin as such does not require any free market of BTC's on which these find an economically defensible equilibrium price in terms of existing currencies. The

Bitcoin P2P system merely allows that mechanism, but using the Bitcoin transaction technology in other ways (for instance as a technical replacement of an existing currency) may constitute a valid use of it as well in terms of using the software and its mechanisms for what it was meant (how can we know?) to support. I conclude that Bitcoin's blockchain based transaction technology avoiding single points of failure can meaningfully applied in the absence of a free market just as well.

4 Propositions concerning the moneyness of Bitcoin

From a principled point of view it seems that the following propositions (claims) can be maintained.

1. Moneyness of Bitcoin is to a larger extent a matter of the Bitcoin system as a whole than currency. In other words, while, as was argued above, at some instant of time some particular amount of BTC may be currency and another amount of BTC may not be currency at the same time, it seems that if some amount of BTC qualifies as money then every other amount is money-like to such an extent that it qualifies as money as well.
2. In many currency areas the issue whether an amount of BTC constitutes money is still open and is a subject that is investigated by means of legal processes; in different currency areas different conclusions may be drawn on the same questions.
3. The often repeated suggestion that Bitcoin fails to serve as a store of value (and for that reason fails as a money) because of its volatility against the most popular existing currencies says nothing about Bitcoin and merely says something about its use.
4. It seems that those who intend to settle the moneyness question for Bitcoin in court either positively or negatively do so for political reasons mainly. Those reasons include politics of money, and policies favoring specific business interests.
5. Moneyness is not a black and white issue, it depends on circumstances and usage if an amount of BTC may or must be considered as an amount of money. It also depends on one's philosophy of money.
6. It seems useful first to deal with the classification of (particular chunks or amounts of) Bitcoin in terms of notions that the financial world has

provided with more rigid (and uncontroversial) definitions than money.

7. There is no such thing as “it being in the interest of Bitcoin” that it is viewed as money. If asserting moneyness for Bitcoin lowers the value of (a specific amount of) BTC doing so is probably not to the advantage of the current holder of that amount and conversely.
8. However, at first sight it seems to run counter to “the spirit of Bitcoin” (admittedly a fairly risky notion) to regard it as money and its incarnations as currency. To see this consider the following thought experiment.

Suppose that authorities within a currency area by force acquire (seize) possession (control, i.e. exclusive possession of secret keys) of (a part of) A 's BTC holdings (say k BTC) at say time t worth $v_{C_N}(k, t)$ in the local currency (at time t). Now suppose that the same authorities prefer to return “that amount” at time $t + r$ then viewing the amount as currency its value must be measured in that same currency and so an amount of currency (not necessarily physically identical to what was seized) needs to be returned perhaps corrected for interests and perhaps augmented with some compensation for damages incurred by the victim of the seizure (in this case A).

However, it seems to be in the spirit of Bitcoin (that is in conformance with the expectation of Bitcoin holders) that k BTC's are returned to A , and preferably exactly the same BTC's. (Being returned BTC's with a provable criminal history may not be in A 's interest.)

In particular if the rate of BTC against C_N has increased A is still entitled to being returned the same amount k BTC rather than less under the assumption that an equal value (modulo interest and compensation) as measured in local currency C_N must be returned to A by the authorities.⁴

9. Speaking of Bitcoin as a money does not turn it into a money. I hold that saying that Bitcoin is a money does not cause it to be one. As a philosophical issue moneyness must be determined on a more solid basis than the statistics of speech acts.

⁴I don't really believe this argument against the moneyness of Bitcoin as it depends on a conventional theory of ownership of BTC's which I don't support. In [4, 5] the notion of an EXIM (Exclusively Informational Money) has been developed. If one views Bitcoin as an EXIM (or an EXIM-like informational money) ownership cannot be decoupled from control (that is exclusive possession of the relevant secret key or keys) and BTC's cannot be “acquired” (seized) by force by any authority and even cannot be stolen by any agent. The notion of theft depends on ownership being decoupled from possession (the holding relation) with ownership persisting through illegal changes of possession. All titles of ownership go with control.

10. The role of moneyness of Bitcoin in the development of formalisms about it is with some attention. For instance let $MV_N^{btw}(A)$ denote the value of that fraction of an amount A with a size of k BTC that is counted as money (within currency area CA_N) expressed in units of the currency C_N of currency area CA_N .

Determination of $MV_N^{btw}(k)$ if moneyness of A has not yet been settled within CA_A constitutes an issue that is comparable to determination of the value of $1/0$ in cases where the questions about division by zero are somehow still open. There may be a similar spectrum of options, to name some I (i) $MV_N^{btw}(k) = 0$ corresponds to calculating in an (involution) meadow (see [3]), (ii) taking an error value corresponds to the design decisions that underly common meads from [11]), and (iii) choosing any other rational number as the value of $MV_N^{btw}(k) = 0$ corresponds with the design decisions that underly non-involutive meadows (see [10]).

5 Bitcoin promotion movement and legal status mining

One may consider Bitcoin or the Bitcoin ecosystem as a movement of individuals and groups who share or expect to share some common values perhaps “polluted” by individuals and groups whose intention is not at all in conformance with these values. Within the Bitcoin movement at large many factions exist each promoting their own view on the subject in various ways. Working bottom up I distinguish the following levels: personal level, group level, organizational level, factional level (w.r.t. a movement), movement level, and societal level. At the personal level, group level, organizational level, and factional level there is ample room for conscious and deliberate action and planned activity. At movement level as well as at the societal level there is not enough potential for coordination to think in these terms.

Coordinated action about Bitcoin, that is with ambitions beyond the mere use of the system, mainly takes place at a factional level where suitable packages of ideologies and viewpoints can be turned into goals and objectives of distributed threads of activity that can be effectuated by members of the faction. Different threads are running concurrently within a faction and a strategic interleaving⁵ policy determines which thread is allocated the best part of critical resources at any moment of time. For some threads it may be quite unpredictable if the

⁵See [6, 7] for the notion of strategic interleaving (an alternative to the much more familiar notion of arbitrary interleaving). I hold that threads, multi-threading and strategic interleaving are concepts that can be transferred from computer science to their realm of human agency in a fruitful manner.

goals set for that thread will or can be achieved, for other threads that may not be a problem.

It seems to make perfect sense for a faction to strive for a different legal status in different currency areas for various chunks of Bitcoin that it may be in control of or may expect to be in control of in due time. Why not work towards Bitcoin being (i) entirely illegal in Switzerland, (ii) unregulated in Liechtenstein, (iii) highly regulated in Ukraine, (iv) merely tolerated in China, (v) actively promoted in South Africa, (vi) some chunks of BTC being monetized into financial assets in the UK, (vii) some chunks of BTC being monetized and turned into redeemable specimen of currency in the Canada, and (viii) a chunk constituting the entire volume of national currency in Panama. This is just an artificial (random) example of the combinatorial explosion of legal status distributions that a Bitcoin promoting faction may strive for.

The capability to serve as a rationale for the spreading of intricate legal puzzles with unpredictable outcome in different legislations (or rule systems of currency areas) may be considered a viral potential of Bitcoin.

5.1 Legal mining about a (kind of) Second Life (without life)

Perhaps the richer the variety of legal conditions (scenarios) that Bitcoin can and has been accommodated to, the stronger its role will become on the long run. It appears that a combinatorial explosion of different packages of goals and ambitions can be designed for serving as the basis of the multithread activity of different factions.

Bitcoin “as such” does not imply or require any logic or consistency about these matters. Bitcoin might also be viewed as a distributed computer game, a kind of Second Life, but a game without life (Bitcoin as the “Nakamoto Dollar” in a distributed multiplayer game called Bitcoin). Then a diversity of legal status throughout the various currency areas might positively contribute to participant’s game experience.

Some factions may intend to maximize the amount of legal dispute concerning Bitcoin throughout the world other factions may prefer to minimize that distraction from the real work. Besides using an amazing amount of energy for mining purposes Bitcoin may become an amazingly time and energy consuming theme for legal work in all currency areas. There seems to be some form of legal mining going on: spending legal energy and creativity in order to advance the legal position of certain chunks of Bitcoin to a faction’s perceived advantage. These legal battles are may be considered a sign of life for Bitcoin rather than

a source of worry.

5.2 Strategic interleaving policy determination

Given this complex and varied scene one may wonder how a strategic interleaving policy for a faction can be determined given its arrangement of threads and goals for each thread. Are different factions competing with one another in court just as miners compete by means of hardware and software, or are all up against the same world wide regulatory pressure opposing adversaries (such as central banks and financial authorities) reflecting roughly the same interests. Bitcoin seems to become more interesting if legal battles are between factions than if all factions fight the same enemy with marginally different methods and positions. This conclusion seems to be almost irrational: it may be in the advantage of Bitcoin (that is positively correlate with its expected or observed time of survival) if factions work towards legal objectives which are fiercely disputed by other factions. In other words, in terms of legal objectives related to Bitcoin there may be no such thing as “the sprit of Bitcoin” about which most factions agree, or should agree.

The ability for a Bitcoin promoting faction to systematically carry on with the interleaved effectuation of a vector of threads may become vital for its survival. This ability probably counts even more in the absence of a convincing theory underpinning that the package of objectives which together are underlying each of these threads makes sense in terms of higher level objectives of the faction’s leaders.

One aspect where different factions may disagree is the price of BTC against a bundle of official currencies. Can they still agree on the concept of an optimal price of a Bitcoin even if they disagree concerning there own interests regarding that price. These considerations may lead to the following view about the optimal market value of Bitcoin. What would be an equilibrium price given the idea that the essential battle is going on between different Bitcoin oriented factions. Then the notion of an equilibrium price to which all factions might subscribe may be that price which maximizes the expected lifetime of Bitcoin as a vital distributed P2P system. Needless to say that at any given moment of time it is very difficult to analyze if BTC is overvalued or undervalued in terms of this criterion.

5.3 The moneyness issue for Bitcoin unsolvable?

Assuming that expected Bitcoin survival time is maximized if the legal procedural cost around it is maximized as well one may conclude that it is in the interest of Bitcoin (in terms of optimization of its expected life-time), if the question of its moneyness remains unsettled and philosophically open as long as possible. Disparate judgements on that question in different currency areas might be applauded by Bitcoin proponents. Even in philosophical terms Bitcoin may not have to gain much by moving from merely being “Bitcoin” (which might be something new) to being money, which may turn out to be an outdated concept.

6 Concluding remarks

None of the above is definitive, all of it is intrinsically speculative. Moreover as time goes by the meaning of the background terminology is bound to evolve. I expect this evolution to be such that informal monies will be incorporated smoothly into the financial system in such a manner that moneyness questions will sound outdated only a few years from now.

This paper is not meant as an introduction of Bitcoin, far more references and discussion would be needed, and only serves for the communication of my views and underlying research results. The references to work on meadows ([3, 10, 11]) are perhaps somewhat farfetched. Nevertheless I strongly support the view that open moneyness questions should not be considered to stand in the way of the development of advanced formalism and notations. Moreover, I assume that a novel generation of Bitcoin could be based on the full range of rational numbers rather than a finite subset of it in which case meadows would constitute my datatype of choice for its description (see [12]).

In [4, 5, 13, 15] one finds many references to Bitcoin literature, and notably the Wikipedia page on Bitcoin currently features a vast number of relevant references on Bitcoin.

References

- [1] Jan A. Bergstra. Formaleuros, formalbitcoins, and virtual monies. arxiv.org/abs/1008.0616v2 [cs.CY] (2013).
- [2] Jan A. Bergstra. Bitcoin and Islamic Finance (version 3). University of Amsterdam, Informatics Institute, Section Theory of Computer Science, Report TCS1406v3 available

- on <http://www.science.uva.nl/research/prog/publications.html#reports>, (May 2014).
- [3] Jan A. Bergstra, Inge Bethke, and Alban Ponse. Cancellation meadows: a generic basis theorem and some applications. *The Computer Journal*, 56(1): 3–14, doi:10.1093/comjnl/bsx147 (2013).
 - [4] Jan A. Bergstra and Karl de Leeuw. Bitcoin and Beyond: Exclusively Informational Money. [arXiv:1304.4758v2](https://arxiv.org/abs/1304.4758v2) [cs.CY] (2013).
 - [5] Jan A. Bergstra and Karl de Leeuw. Questions related to Bitcoin and other Informational Money. [arXiv:1305.5956v2](https://arxiv.org/abs/1305.5956v2) [cs.CY] (2013).
 - [6] J.A. Bergstra and C.A. Middelburg. Thread algebra with multi-level strategies. *Fundamenta Informaticae* 71(2/3), pp. 153–182 (2006).
 - [7] J.A. Bergstra and C.A. Middelburg. Thread algebra for strategic interleaving. *Formal Aspects of Computing*, 19 (4) pp. 445–474, (2007).
 - [8] J.A. Bergstra and C.A. Middelburg. Preliminaries to an investigation of reduced product set finance. *JKAU: Islamic Economics*, 24(1):175–210 (2011).
 - [9] J.A. Bergstra and C.A. Middelburg. Interest prohibition and financial product innovation. *In: Finance Islamique: Regard(s) sur une Finance Alternative, Mazars Hadj Ali*, 274–284 (2012).
 - [10] J.A. Bergstra and C.A. Middelburg. Division by zero in non-involutive meadows. [arXiv:1406.2092](https://arxiv.org/abs/1406.2092) [cs.CO] (2014).
 - [11] J.A. Bergstra and A. Ponse. Division by zero in common meadows. [arXiv:1406.6878](https://arxiv.org/abs/1406.6878) [math.RA] (2014).
 - [12] J.A. Bergstra and J.V. Tucker. The rational numbers as an abstract data type. *Journal of the ACM*, 54 (2), Article 7 (2007).
 - [13] Jan A. Bergstra and Peter Weijland. Bitcoin: a money-like informational commodity. University of Amsterdam, Informatics Institute, Section Theory of Computer Science, **Report TCS1402** available on <http://www.science.uva.nl/research/prog/publications.html#reports> (Februari 2014).
 - [14] Satoshi Nakamoto. Bitcoin: a peer-to-peer electronic cash system. <http://Bitcoin.org/Bitcoin.pdf> (2008).
 - [15] Tim Swanson. The anatomy of a money-like informational commodity: a study of Bitcoin. <http://www.ofnumbers.com/2014/08/04/published-new-book-the-anatomy-of-a-money-like-informational-commodity-a-study-of-bitcoin/>, (2014).

Electronic Reports Series of section Theory of Computer Science

Within this series the following reports appeared.

- [TCS1409v2] J.A. Bergstra and A. Ponse, *Three Datatype Defining Rewrite Systems for Datatypes of Integers each extending a Datatype of Naturals (version 2)*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1410] J.A. Bergstra and A. Ponse, *Division by Zero in Common Meadows*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1407v3] J.A. Bergstra, *Four Complete Datatype Defining Rewrite Systems for an Abstract Datatype of Natural Numbers (version 3)*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1409] J.A. Bergstra and A. Ponse, *Three Datatype Defining Rewrite Systems for Datatypes of Integers each extending a Datatype of Naturals*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1406v3] J.A. Bergstra, *Bitcoin and Islamic Finance (version 3)*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1407v2] J.A. Bergstra, *Four Complete Datatype Defining Rewrite Systems for an Abstract Datatype of Natural Numbers (version 2)*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1408] J.A. Bergstra, *Bitcoin: Informational Money en het Einde van Gewoon Geld*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1407] J.A. Bergstra, *Four Complete Datatype Defining Rewrite Systems for an Abstract Datatype of Natural Numbers*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1406v2] J.A. Bergstra, *Bitcoin and Islamic Finance (version 2)*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1406] J.A. Bergstra, *Bitcoin and Islamic Finance*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1405] J.A. Bergstra, *Rekenen in een Conservatieve Schrapwet Weide*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1404] J.A. Bergstra, *Division by Zero and Abstract Data Types*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1403] J.A. Bergstra, I. Bethke, and A. Ponse, *Equations for Formally Real Meadows*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1402] J.A. Bergstra and W.P. Weijland, *Bitcoin, a Money-like Informational Commodity*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1401] J.A. Bergstra, *Bitcoin, een "money-like informational commodity"*, section Theory of Computer Science - University of Amsterdam, 2014.
- [TCS1301] B. Dierkens, *The Refined Function-Behaviour-Structure Framework*, section Theory of Computer Science - University of Amsterdam, 2013.
- [TCS1202] B. Dierkens, *From Functions to Object-Oriented Abstraction*, section Theory of Computer Science - University of Amsterdam, 2012.
- [TCS1201] B. Dierkens, *Concurrent Models for Object Execution*, section Theory of Computer Science - University of Amsterdam, 2012.

- [TCS1102] B. Diertens, *Communicating Concurrent Functions*, section Theory of Computer Science - University of Amsterdam, 2011.
- [TCS1101] B. Diertens, *Concurrent Models for Function Execution*, section Theory of Computer Science - University of Amsterdam, 2011.
- [TCS1001] B. Diertens, *On Object-Orientation*, section Theory of Computer Science - University of Amsterdam, 2010.

Within former series (PRG) the following reports appeared.

- [PRG0914] J.A. Bergstra and C.A. Middelburg, *Autosolvability of Halting Problem Instances for Instruction Sequences*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0913] J.A. Bergstra and C.A. Middelburg, *Functional Units for Natural Numbers*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0912] J.A. Bergstra and C.A. Middelburg, *Instruction Sequence Processing Operators*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0911] J.A. Bergstra and C.A. Middelburg, *Partial Komori Fields and Imperative Komori Fields*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0910] J.A. Bergstra and C.A. Middelburg, *Indirect Jumps Improve Instruction Sequence Performance*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0909] J.A. Bergstra and C.A. Middelburg, *Arithmetical Meadows*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0908] B. Diertens, *Software Engineering with Process Algebra: Modelling Client / Server Architectures*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0907] J.A. Bergstra and C.A. Middelburg, *Inversive Meadows and Divisive Meadows*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0906] J.A. Bergstra and C.A. Middelburg, *Instruction Sequence Notations with Probabilistic Instructions*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0905] J.A. Bergstra and C.A. Middelburg, *A Protocol for Instruction Stream Processing*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0904] J.A. Bergstra and C.A. Middelburg, *A Process Calculus with Finitary Comprehended Terms*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0903] J.A. Bergstra and C.A. Middelburg, *Transmission Protocols for Instruction Streams*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0902] J.A. Bergstra and C.A. Middelburg, *Meadow Enriched ACP Process Algebras*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0901] J.A. Bergstra and C.A. Middelburg, *Timed Tuplix Calculus and the Wesseling and van den Berg Equation*, Programming Research Group - University of Amsterdam, 2009.
- [PRG0814] J.A. Bergstra and C.A. Middelburg, *Instruction Sequences for the Production of Processes*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0813] J.A. Bergstra and C.A. Middelburg, *On the Expressiveness of Single-Pass Instruction Sequences*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0812] J.A. Bergstra and C.A. Middelburg, *Instruction Sequences and Non-uniform Complexity Theory*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0811] D. Staudt, *A Case Study in Software Engineering with PSF: A Domotics Application*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0810] J.A. Bergstra and C.A. Middelburg, *Thread Algebra for Poly-Threading*, Programming Research Group - University of Amsterdam, 2008.

- [PRG0809] J.A. Bergstra and C.A. Middelburg, *Data Linkage Dynamics with Shedding*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0808] B. Diertens, *A Process Algebra Software Engineering Environment*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0807] J.A. Bergstra, S. Nolst Trenite, and M.B. van der Zwaag, *Tuplix Calculus Specifications of Financial Transfer Networks*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0806] J.A. Bergstra and C.A. Middelburg, *Data Linkage Algebra, Data Linkage Dynamics, and Priority Rewriting*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0805] J.A. Bergstra, S. Nolst Trenite, and M.B. van der Zwaag, *UvA Budget Allocatie Model*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0804] J.A. Bergstra and C.A. Middelburg, *Thread Algebra for Sequential Poly-Threading*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0803] J.A. Bergstra and C.A. Middelburg, *Thread Extraction for Polyadic Instruction Sequences*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0802] A. Barros and T. Hou, *A Constructive Version of AIP Revisited*, Programming Research Group - University of Amsterdam, 2008.
- [PRG0801] J.A. Bergstra and C.A. Middelburg, *Programming an Interpreter Using Molecular Dynamics*, Programming Research Group - University of Amsterdam, 2008.

The above reports and more are available through the website: ivi.fnwi.uva.nl/tcs/

Electronic Report Series

section Theory of Computer Science
Faculty of Science
University of Amsterdam

Science Park 904
1098 XG Amsterdam
the Netherlands

ivi.fnwi.uva.nl/tcs/