University of Amsterdam

Theory of Computer Science

Bitcoin and Islamic Finance (version 2)

J.A. Bergstra

Report TCS1406v2 May 2014

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

Theory of Computer Science Electronic Report Series

Bitcoin and Islamic Finance
(version 2*)

Jan A. Bergstra

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

May 10, 2014

Abstract

It is argued that a Bitcoin-style money-like informational commodity may constitute an effective instrument for the further development of Islamic Finance. The argument involves the following elements: (i) an application of circulation theory to Bitcoin with the objective to establish the implausibility of interest payment in connection with Bitcoin, (ii) viewing a Bitcoin-like system as a money-like exclusively informational commodity with the implication that such a system need not support debt, (iii) the idea that Islamic Finance imposes different requirements compared to conventional financial policies on a money concerning its use as a tool for achieving social and economic objectives, and (iv) identification of two aspects of mining, gambling and lack of trust, that may both be considered problematic from the perspective of compliance with the rules of Islamic Finance and a corresponding proposal to modify the architecture of mining in order to improve compliance with these rules.

Keywords and phrases: informational money, exclusively informational money, money-like informational commodity, IFR compliant finance, Bitcoin.

*This is a revised version of [6]. In this revision the following changes and additions were made (apart from the correction of some typo's): (i) indicating that IP (interest prohibition) follows from the other requirements of IFR (Islamic finance requirements) in many cases, if not in the majority of cases, (ii) making mention of the fact that circulation theory does not prove the impossibility of interest in circumstances of a fixed monetary base, but only bounds the volume of interests that can be paid by the available amount of money, (iii) clarification of the absence of property rights (for agent A) on amounts of Bitcoin in control of agent A when assuming an EXIM status for Bitcoin, (iv) improved arguments concerning the suspicion that mining involves gambling, and that (for that reason) mining would not be IPR compliant (given the current mining technology. The improvements (ii) and (iii) were triggered by questions raised in [23] and item (iv) resulted from a question raised in an email that I received from an anonymous source.

Contents

1 Introduction

Following [13] I will classify Bitcoin as a money-like informational commodity (MLIC). The virtue of this classification is claimed to be that it is technically defensible while it involves no premature commitment to an answer in either direction to the question whether or not Bitcoin is a money. An MLIC may evolve through a life-cycle where it begins as a non-money, then functions as a money, and finally returns to a non-money status. This flexibility of an MLIC with respect to its moneyness is especially important for candidate informational moneys with a more or less rigid and fixed technology. For such informational commodities moneyness correlates with usage and acceptance by a significant and relevant fraction of the public.

The discussion below of the potential connections between Bitcoin and Islamic Finance is not dependent on the actual moneyness of Bitcoin and can be read with the understanding that Bitcoin is an MLIC that might (but need not) evolve into an informational money for which its moneyness is undisputed. The probability that of Bitcoin will become an undisputed informational money in part depends on its perceived usefulness for Islamic Finance.

1.1 About Islamic Finance

Following [7] I will characterize Islamic Finance as any system where all ethically correct financial transactions and agents are supposed to comply with the five rules mentioned below (thus following the exposition of [8] and simplifying the description in [4]).

Instead of speaking of Islamic Finance I prefer to speak of Islamic Finance Requirements which may be met in a financial system to varying degrees. An additional advantage of this way of using the terminology is that a financial system will not be Islamic simply because its governors prefer to label it that way.

1.1.1 Islamic Finance Requirements (IFR)

I will use this set of requirements as a definition of IFR. Instead of Islamic Finance I will prefer to use the phrase IFR compliant finance.

Interest prohibition (IP). Interest on debt must neither be asked and received nor promised and paid.

No misleading. Agents should not mislead their trade partners. Trade partners are entitled to know what they buy. Further trade partners must be able to take their own decisions in freedom.

True entity requirement. Transactions against money must deal with existing goods and services (true entities).

Gambling prohibition (GP). Gambling is forbidden.

Mandatory donation. Agents must donate a reasonable fraction of their income to those in need.

1.1.2 Some remarks on IFR

Much can be said about the origin of these rules and about the effects such rules may have on an economic system for which compliance with those rules is sought. I will only provide a number of scattered remarks that I collected on the basis of a recent effort to read a number of (English, Dutch, French, and German) texts about Islamic Finance.

1. These five principles of Islamic Finance can be viewed as a conceptual option for organizing a financial system independently of its Islamic background. One may wish to

experiment with the same bundle of principles for different reasons. In principle supporting IFR is an option from a non-Islamic perspective just as well.[1] In [4] I have proposed to refer to a financial system compliant with (a somewhat different phrasing of) these rules as a (rules of) Crescent-Star Finance (CSF), thus expressing the potential decoupling from its Islamic background which might promote a wider acceptance outside Islamic circles.

2. I do not hold in any manner that these five principles (of IFR) provide either a better theory of money or a better economic system than so-called conventional or Western principles. What can be argued convincingly, however, is that these principles differ from conventional ones and for that reason alone the implications of IFR merit investigation.

3. The fact that these principles can be understood as being compliant with Islamic views is independent of these principles as such.

4. For each of these principles the following questions arise:

   (a) what does it mean in practice (what is the importance of case history),

   (b) how to deal with borderline cases (in theory),

   (c) how principled should one be in seeking compliance (who takes decisions),

   (d) how about consistency with the other rules (parametrized by one's economic background theory),

   (e) what are implications of the rule as a restriction one one's behavior when one's financial actions are embedded in a financial system that is not compliant with these five rules,

   (f) in the light of which financial and economic background theory must the rule be understood (both in terms of current economic theory and in terms of its historic development),

   (g) is the rule incorporating restrictions for individual persons or rather for entire financial and economic systems,

   (h) in which cases can the rule be ignored or compromised at the level of financial system design.

   These questions arise from a non-Islamic perspective just as well as from an Islamic perspective. Needless to say views on these issues differ through the Islamic world in just the same way as views on economic matters vary in conventional finance and economics.

5. The consistency of Islamic finance is mostly taken for granted, but it is not at all a trivial matter. That issue has been discussed in [10] by pointing out methodological aspects of the matter, however, without arriving at a conclusive result. Cristian (pre-reformation) support for interest prohibition had to give way in the view of its inconsistency, which

[1] I have become intrigued by Islamic finance because of the parallel with computer programming: disallowing options or mechanisms in a program notation need not make that program notation weaker than previous more liberal notations. Is a strengthening of the financial system a conceivable outcome of what seems at first sight to be a drastic reduction of its operational options? (See also [10].)

came about by simulating interest payment as a result of financial engineering by means of a sequential arrangement of ethically accepted (at that time, and in the context of IP) transactions. It is remarkable that scholars of Islamic Finance do not commonly express the need to demonstrate that IPR (or any improved version of it) is consistent, given the fact that a Christian ideology starting out with a comparable commitment to IP failed to sustain that commitment.

6. The intuition of IP is most easily understood in a setting where all income must be earned as an unpredictable profit from sequences of business transactions.

   Assuming that at time t agent A borrows amount x from agent B, and A agrees to pay back $(1+p)\cdot x$ to B at time $t+k$ (e.g. 1 year later). Now one may consider the amount $p\cdot x$ an interest and oppose to the agreement on that basis. But if at time t it is already sure that at time $t+\frac{1}{2}\cdot k$ A will receive an amount $y>(1+p)\cdot x$ from agent C then A thinks in terms of delayed payment to B rather than in terms of interest.

   However, the more plausible interpretation of IP results if one assumes that B has no income guarantees at time t. In that case B "sells" a profit (by promising to pay $(1+p)\cdot x$ to B at time $t+k$) that is unavailable (by simply keeping x in stock in preparation of returning it to A, the income is unlikely to be created by B) at time t and which may just as well turn out to be a loss. That is the surplus $p\cdot x$ over x can only be earned as a profit from business entertained after t and as such its existence is in doubt. That implies that in this case IP follows from the "true entity requirement". B should not entertain a transaction where an entity that does not yet exist (and may never exist in all likelihood) is exchanged for whatever other entity.[2]

7. It is evidently somehow problematic to write about Islam or about Islamic Money from a position outside Islam. In [2] I have given both a justification for and a systematic risk analysis of writing about Islamic matters from a Christian background as well as from an agnostic background.

   With reference to [2] I mention that the manifest importance of Islam for all human beings, irrespective of their religious views, justifies and even requires its analysis from external positions.

8. Again with reference to [2] I mention that Islam is large, varied, and very complex, and that hardly any generalizing assertion about Islam can be justified. My point of view is that Islam should be understood and approach by external observers with a positive attitude. That positive attitude implies an understanding of the fact that the Islam should not, or at least need not, be identified with its extreme forms. Rather the other way around one should feel invited to develop a positive attitude towards Islam, because only then its potential impact can be fully appreciated. I consider an appreciation of the following issues helpful in this context.

   (a) The influence of Islam on Western thought has been significant and its mediating role in transferring Greek Philosophy to the West has been essential.

[2]This argument can be turned around by stating that where regular income guarantees for A prevail, the payment of interest to A may be considered more justifiable.

(b) Although Islam may be considered a political system with some justification, that by itself does not imply that it is either outdated or that it embodies a deficient understanding of the separation between the state and the religious institutions (I refer to [2] for an elaboration of this matter).

(c) As a system of governance what Islam prescribes, suggests, or promotes, bears some similarity to how "Western" science runs itself. There are no democratic elections in science, and that absence is supposedly justified with the argument that "truth", the topic of science, is a matter too important to be left to the erratic outcomes of democratic elections. Instead of Sharia boards, science has editorial boards, program committees, and grant awarding bodies. These groups always have to take principles of scientific integrity and competence in to account. Science allows competing teams (nations, factions) to express different views at the same time and is reluctant to accept the single authority of monolithic international bodies.

9. In [10] an attempt has been made to analyze in detail the technical content of interest prohibition. The following conclusions were drawn:

   (a) Interest prohibition turns a system into a so-called a RPSF (reduced product set finance). With reference to classical principles of program notation design it is concluded that the restrictions of an RPSF need not necessarily render it weaker as a financial system than its unrestricted proxies in the space of financial systems.

   (b) The concept of interest is by no means easy to define, not even in a setting of modern finance, because it ultimately depends on the outcome an analysis of the undisputed cost incurred by a lender when lending money to a borrower.

   (c) The idea that the original Islamic sources contain a theory of money which is sufficiently detailed to allow the specification of interest in a way that is or convincingly transferable to a modern financial system is lacking plausibility.

   From the perspective of an outsider the picture can be simplified by assuming that the concept of interest prohibition came to the forefront of Islamic thought in the context of the adoption of Greek philosophy as an important source for its philosophers. Aristotle opposed interests and so did Judaic ethics for several millennia. Events before and during the reformation moved (Roman Catholic) Christianity into accepting interest payments, though with considerable reluctance only.[3]

10. That a financial system satisfies the rules of IFR does not imply ethical virtue per se. Even if Bitcoin or an appropriate alternative for it provides for a financial system compliant with IFR rules, its adoption may lead to many ethical questions some of which are rather pressing. I refer to [7] for an initial survey of ethical issues in connection with Bitcoin.

[3]Interest prohibition has been quite universal in the past, and one might claim that its removal from prominence primarily signed a change in the conception of money, and not a change in the appreciation of interest payment.

1.2 About interest prohibition and debt avoidance

Much attention in the literature on Islamic Finance is paid to the effects of and the rationale for Interest Prohibition (IP). In [3] I have attempted to describe the roots of IP. As far as I can see the supporters of IF do not claim that money can be borrowed by A from B without any cost for B, and not without risk for B either. Moreover initial transaction costs of a lending transaction are usually permitted by proponents of IP. In [10] the difficulties of precisely specifying what must be considered interest have been scrutinized. This is a difficult topic about which the literature on Islamic Finance seems to be rather uninformative with as a consequence that a payment may be considered forbidden merely because the description "interest" is assigned to that payment by an agent who is unaware of the consequences of that labeling. That agent is likely to be unaware of the necessity to provide a (potentially non-trivial) explanation as to why that payment is (and must be) considered an interest payment.

A common method for implementing IP is the avoidance of debts. Debts and interest go hand in hand. Islamic finance and trade provides many forms of cooperation that allow financing and workload for an activity to be unevenly distributed over a number of parties without the need to create debt positions in any direction. In [10] the well-known (almost classical) observation has been outlined that the transaction costs of such forms of cooperation are in some cases unexpectedly high and may in some cases be considered prohibitive.

I will argue that by viewing Bitcoin (or rather a Bitcoin-like informational money) as a so-called exclusively informational money (EXIM, see [7]) debt (in terms of that informational money) turns into an implausible feature and as a consequence interest (in connection with that informational money) becomes both unnecessary and implausible.

1.3 About Islamic Logic (IL)

At first sight the phrase Islamic Finance seems too be comparable to the phrases Islamic Art and Islamic Logic. This is unconvincing, however, because Islamic Art and Islamic Logic can be identified with art and logic from a specified historic period and geographic region. In contrast Islamic Finance is a recent movement with roots in the early years of of the 20th Century.[4]

In [2] I have made an attempt to redesign Islamic Logic as a modern theme in such a way that, just as Islamic Finance, its use may be specifically useful for achieving Islamic objectives. Redesigning IL along such lines is a risky project because some interpretation of Islamic objectives is unavoidable. Today's practice of Shariah Boards, however, calls for an investigation of common reasoning patterns used by such bodies. The suggestions of [2] are preliminary only and extensive subsequent theoretical and empirical research will be needed to assess their relevance. The resulting approach to Islamic Logic was termed Real Islamic Logic (RIL).[5]

[4] Islamic Art and Islamic Finance have in common the noticeable impact of restrictive rules of conduct. Islamic Logic, however, seems not to embody or to incorporate any restrictive rules of conduct that are supposedly specific to an Islamic context.

[5] Perhaps Current Islamic Logic (CIL) would have been a better phrase than RIL because CIL allows for the existence of a discrepancy between what Shariah Boards actually do (if common patterns can be found) and what they ought to do (if it is not taken for granted that their judgments are in sufficient compliance with

The main conclusion of [2] is that paraconsistent logics ought to play a central role in any RIL. (For a recent survey of paraconsistent logics see [21]). Another conclusion is that RIL makes use of prioritized rules with many different levels of priority (I counted up to 9 such levels which defeats any formal analysis by means of methods known in today's theoretic computer science to mention an area where prioritized reasoning has become quite common). These two features render RIL very different from conventional formal logics, their combination presenting ample novel challenges for the modern logician.

Taking a more modern (instead of historic) approach to Islamic Logic is plausible, because, at least in principle, that kind of logic is needed when one intends to reason about how to apply a IFR compliant Finance to an actual problem in a way which conforms to time and place dependent manifestations of Islamic principles. RIL is primarily a human reasoning style, and RIL needs to be applied when matching the rule based constraints of IFR compliant money to a specific context. The final and admittedly rather speculative conclusion of [2] is that RIL carries a relatively high perspective (in comparison to other informal logics) to defeat attempts for automation and virtualization. This (claimed) robustness against the potential ubiquitous advance of software robots in applied ethics may not be considered an important issue today, but it may become critical in a not so distant future.

2 Bitcoin: a Money-like Informational Commodity (MLIC)

Bitcoin, both in its design and in its development, contributes to the understanding of the concept money. This contribution is visible already from the ongoing debate concerning its moneyness. In [13] the proposal was made to classify Bitcoin in such a way that the question whether or not it constitutes a money need not be settled in advance. By labeling (typing, classifying) Bitcoin as a money-like informational commodity (MLIC) a significant flexibility is obtained. Indeed, viewing Bitcoin as an MLIC is compatible with a life-cycle where it starts and terminates its existence as a non-money, with one or more episodes of ("true") moneyness (rather than mere "money-likeness") in between.

2.1 About Bitcoin and about money

Bitcoin is supposed to originate from the same yet unknown source as [22]. It is common to consider Satoshi Nakamoto as Bitcoin's originator in spite of persistent lack of clarity about the pseudonymous status of this name.

Islamic Principles).

When contemplating RIL, I have made an attempt to reconcile an external perspective (that from a religiously indifferent external observer) and a hypothesized internal perspective (from an observer who tries to feel convinced by core principles of the religious ideology at hand). This thought experiment is highly problematic from a methodological viewpoint, but I hold that only by performing such thought experiments one may gain access to the mechanics of said common reasoning patterns (assuming that such patterns can be reliably determined). Needless to say this thought experiment may have different outcomes for different persons (and even for the same person in different circumstances) and for that reason I do not claim in any manner that the outcome reported in [2] should be predictive for outcomes arrived at by other individuals when attempting to carry out a corresponding thought experiment.

One may consider the development of Bitcoin a step forward in the development of information (see [16]) as a core philosophical concept, or as an exotic chapter in the history of information security (see [19]), or as a system in need of further improvement (see [1, 15]), or as a contribution to the philosophy of money (see [20]), or in any other manner. Its mere existence justifies writing about Bitcoin.

In [5] I have made an attempt to survey the vast and heterogeneous volume of viewpoints on money. I summarize some conclusions from that paper:

1. The main conclusion from [5] which has some bearing on issues around Bitcoin is that I prefer to reserve the phrase virtual money for a concept not remotely similar to Bitcoin. The mere existence in the digital world is not a sufficient criterion for virtuality. Bitcoin seems not to be a virtualized form of any non-virtual money-like commodity. It is far too innovative.

2. Another conclusion of [5] is that in order to write about any any existing money (or near-money) in theoretical terms one needs some formal counterpart to (the units of) that particular money. In particular "Formalbitcoins" enter the picture if one inters to speak or write about hypothetical activities or events involving (equally hypothetical) transaction by means of Bitcoin. Unfortunately the methodology of having a formal substitute for a money as a vehicle for theoretical discussions is not without its own complications.

3. A (unit of) a kind money (for instance EUR, BTC) may serve as a dimension. And just as in physics composed dimensions such as Second/EUR^2 are meaningful.

4. Money as featuring inside an organization may differ subtly from money carrying the same name outside that organization. An individual's understanding of money may depend on his or her role within the organization. Virtual currency is used to refer to an (adapted) perception of money within an organization from the perspective of an employee (or a category of employees).

In [7] Bitcoin is considered an informational money (disregarding the complication that it may initially be lacking moneyness) and an attempt is made to map the space of possible informational monies.

Yet another way to look at Bitcoin, admittedly quite remote from an ordinary monetary perspective, is that it constitutes a step forward in the development of the non-negative rational numbers (rather than natural numbers) towards being the preferred datatype of for the quantification of monies of exchange. [6]

2.2 Exclusively Informational Commodities (EXICs)

The main proposal of [7] is to consider informational money as a concept for which access has priority over legally backed ownership. With exclusively informational money (EXIM)

[6] This viewpoint connects well to my personal long standing interest for the specification and use of the rational numbers as an abstract datatype starting with [12]. Notably the use rational numbers as quantifies come into play only in a context of informational monies.

the proposal of [7] is to denote an informational money for which ownership of a quantity is identical to control (or access) to that quantity. With exclusiveness the absence of any other title than the availability of information is meant. In particular the possibility of existence of legally backed titles of ownership (of EXIM quantities) is refuted.

The counterintuitive implication of the notion of an EXIM is that an amount of an informational money (when viewed as an EXIM) cannot be stolen by definition. Change of control (access) is the only way of transfer for an EXIM quantity and a change of control is only problematic if it was effected as a consequence of unacceptable force imposed on the agent who lost control.

Using the terminology of [13] it is systematic to speak of an exclusively informational commodity (EXIC), and of a money-like exclusively informational commodity (MLEXIC) if one intends not to commit tot the moneyness of an informational commodity while claiming its exclusively informational status.

2.2.1 Interest on Bitcoin: objections from circulation theory

The property of Bitcoin that the amount of monetary units is fixed (or almost fixed) creates a setting where interest can be criticized on the grounds of so-called circulation theory. Circulation theory has a (neo-) Marxist background but its modern shape is rather mathematical in style. Simply told the story is this: suppose all BTC holders hold equal amounts. Now they all lend that amount to other holders in a cyclic fashion. After that step all holders have the same amount but now each of them must pay interest to the previous holder of the amount.

Now the means to pay interest must come from somewhere and using new (that is freshly created) money is demonstrably the only available option. On the basis of such arguments, though more sophisticated, circulation theory demonstrates that interest payment and inflation caused by monetary expansion go hand in hand, which then is construed as a weakness of the underlying financial system. Now circulation theorists have to demonstrate that monetary expansion cannot be accounted for by economic growth in order to predict inflation and so on, but the case of Bitcoin is simpler. The closed circulation of BTC in the Bitcoin environment seems to provide an argument in circulation theory style against the plausibility of interest payments on large debt positions.

It should be stressed that even if the monetary base is constant, circulation theory does not "prove" that some interest may not be paid. Evidently, per unit of time no more than 100% of the money base (say m_b) can be used for the purpose of interest payment, which implies an upperbound ($p^{-1} \cdot m_b$) on the total debt position of all participants (given an interest rate p to be paid for all debt per unit of time).[7]

[7] In conventional finance this (kind of) upperbound may be compromised by a cascading application of the mechanism of fractional reserve banking. Fractional reserve banking may be considered a major mechanism in conventional finance for creating money that may eventually be used for interest payment. In many cases that growth of volume of the amount of money may also be justified by economic growth. That dynamics, with constant prices could be called inflation (an expansion of the economic universe), but instead inflation is used only if the financial universe grows faster than the underlying economic universe, that is the growth of the volume of money cannot be completely justified by a growth of the economy. These considerations become far more complex if changes in the technology of money (such as a gradual transition to the use of informational money) have effects on the speed of circulation of money which are not correlated to dynamics in the size of

2.2.2 Borrowing Bitcoin: impossible for an EXIC (and for an MLEXIC)

An important conclusion drawn in [7] about an informational money with EXIM status is that besides theft also borrowing and debt is meaningless. It is pointless to qualify the transfer of quantity for an EXIM as borrowing because all transfers of access have the same status.

For an EXIM (say M_e) control by agent A of an amount $x \cdot M_e$ does not imply the presence of any legal title to that amount which can survive a loss of control by A over (that particular) amount $x \cdot M_e$. An illegal activity by B which allows B to take control over the amount $x \cdot M_e$, and which does so in such a manner that A looses control over the amount $x \cdot M_e$, can be punished on the basis of forbidden actions that constitute a part of the activity. No form of restitution of $x \cdot M_e$ to A can be part of a corresponding retaliation directed to B. This state of affairs is different from the common case for so-called tangible commodities, but it is well-conceivable for informational commodities.

In [7] care is taken not to classify Bitcoin as an EXIM in order to imply that BTCs cannot be stolen (which might be misconstrued as a viewpoint that stealing Bitcoin should be permitted).[8] Instead a thought experiment is carried out where Bitguilder, a hypothetical technical clone of Bitcoin, is introduced and is thought of as having EXIM status.

Thinking of Bitcoin as a potential money-like exclusively informational commodity (MLEXIC) rather than as an informational money will not change the picture concerning either the (im)plausibility of lending or the (im)plausibility of interest payment. Doing so merely introduces increased resilience against doubts about the moneyness of the informational commodity at hand.

2.2.3 MLEXIC casting of Bitcoin and gradual transition to IFR compliance

If one views Bitcoin as an MLIC (or more precisely as an MLEXIC) then this allows a smooth transition to an IFR compliant system where intermediate development stages allow interest-like payments on Bitcoin denominated debt which are IFR compliant for the trivial reason that (at that stage) Bitcoin is not yet an informational money.

3 Bitcoin style financial technology for Islamic Finance

Having argued that both debt and interest payment are implausible features for an MLEXIC (or EXIM) interpretation of Bitcoin its relevance as a potential tool for Islamic Finance seems to have been demonstrated sufficiently well to justify further research into that connection.

Some remarks on the remaining rules of behavior for IFR compliant finance in connection with Bitcoin (or Bitcoin-like technologies under an EXIM perspective) are in order. If clients don't mislead other clients during transactions the irreversible nature of Bitcoin transfers will not be felt as a handicap. Bitcoin is a technology geared towards realizing donations. After effecting a donation the amount has been fully transferred, no strings attached. Gambling

the economy.

[8] If a (quantity of) an informational commodity can be stolen, doing so is an unlawful act of course, but if stealing it is considered a theoretical impossibility, it can't be unlawful either.

with borrowed money will not happen in a Bitcoin driven context (assuming EXIM status). This limitation is insufficient to eliminate gambling but it significantly reduces opportunities for gambling. The irreversible nature of transactions seems to go well with the true entity requirement. That requirement, however, may constitute a significant impediment for the promotion of Islamic Finance in its own right which needs to be compromised in various ways by introducing flexible views on what constitutes a true entity.

What would require rather immediate attention is the trustworthiness of the mining system as well as its compliance with the five principles mentioned above.

3.1 Problems with mining: stepwise restructuring towards compliance with IF principles

Mining is a problematic aspect of the Bitcoin technology chain: a high eco-footprint, various vulnerabilities against DoS attacks, degrading client participation, nearly insurmountable thresholds for hopeful new miners, and lacking protection of clients against consortium building among miners, to mention some issues.

From the perspective of IFR compliant finance I want to mention two issues: gambling implicit in mining, and transparency of mining. Mining involves a search for a solution to a combinatorial problem. An instance of that problem is automatically generated about each 10 minutes. This search mechanism involves (pseudo-) random generation which is the close to a lottery in a world of deterministic computers. I conclude that mining involves some form of gambling which might be criticized from the perspective of Islamic Finance.[9]

Another matter is that Bitcoin is said to have been designed in such a way that its users need not trust any specific other user. Currently Bitcoin clients (Bitcoin client users) must trust the mining mechanism and the decreasing number of strong miners and independent mining pools sheds doubts on that part of the current implementation of Bitcoin's promised ideology as expressed in [22]. From the perspective of IFR compliant it seems meaningful to modify Bitcoin along the following lines (following [7]):

1. Do away with the ideology of distrust: ask clients to trust the community of miners. This requires a modification of the architecture and governance of mining. Insist, however,

[9] One may compare Bitcoin mining to gold mining (which is considered ethically unproblematic in Islam), thereby assuming that a reasonable result in investment is guaranteed (as a rule, that is normally). That comparison makes some sense, but it holds for most lotteries that a participant will get his/her statistical share when participation is sufficiently long. The question is where planned action ends and gambling begins. In risk analysis some authors state that whenever one can calculate the probability of a problem it is not anymore valid to speak of a risk (of occurrence of that specific problem). Perhaps gambling (insofar as it is to be forbidden in IFR) must also be linked exclusively to cases where a probabilistic analysis is unavailable.

However, there is another way in which one may speak of a gamble implied by Bitcoin mining and that relates to the choice of a search strategy by the miner. A search strategy for a (normal) miner must be so that s/he will not predictably lose against miners with faster equipment. I have the impression that the choice of a search strategy which deviates sufficiently much of the methods used by other miners one may indeed be considered a form of gambling.

In gold mining I would claim that some form of competence, earth science etc. enters the picture, but I agree that a complete argument that Bitcoin mining is not IPR compliant needs to demonstrate some clear conceptual difference with gold mining. My second argument (about strategy choice) my be useful for just that purpose.

that no miner, or even no group of say 10 miners, may become a single point of failure. (This step may be needed for Bitcoin as it stands as well.)

2. Accept a formalized split between miners and ordinary clients.
3. Introduce centralized authority for admission to the mining league.
4. Introduce, say, between 100 and 1000 mining agencies, operating independently of one-another, representing subsets of the relevant population of comparable sizes. Make sure that these agencies do not enter into fraudulent coalitions.
5. Impose innovations that systematically reduce the energy cost (eco-footprint) of mining.
6. Introduce one or more joint Shariah Boards for groups of mining agencies which develop a viewpoint that removes objections against (residues of) gambling as present in current and forthcoming mining technology.

Apart from the gambling aspect of mining I don't see any ethical objections against Bitcoin emerging from the IFR requirements. It may well be that an Islamic perspective on money produces lower expectations concerning the services that the financial system will provide to society as a whole than a conventional (Western) perspective does. For instance the ambition to strive towards full employment may drive the financial-economic management of a currency area into growth of its monetary base which then creates inflation as collateral damage that one subsequently seeks to remedy by means of increased interest rates. When dispensing of the "weapon" of interest rate manipulation the financial/economic management of a currency area may need to look for non-financial interventions for achieving purposes such as a high employment rate.[10]

3.2 Evolution towards an informational money

The evolution of any MLIC (including Bitcoin or a modified version of it) to the status of an informational money (with an emphasis on money) is unpredictable. As its stands this evolution will require many other changes in the case of Bitcoin. If Bitcoin is to coexist with other monies some form of rate-stability must be achieved on the long run and the phenomenon of different monies serving different purposes needs to be well-understood.

On the other hand if Bitcoin must drive out other monies in order to evolve to the status of an (informational) money then important changes are needed concerning the design of the portfolio of societal objectives that are to be dealt with by means of financial policies. Remarkably it seems to be the case that such changes are easier to achieve from the perspective of Islamic Finance than from the perspective of a conventional finance. To see this notice that in the Islamic context fewer degrees of freedom are needed to shape money as a policy instrument in the light of the fact that more policy objectives are to be achieved by other means than by manipulating money streams and financial incentives

[10] In [7] a preliminary survey is given of the ethical problems that may arise if one seeks to use Bitcoin as the sole replacement of the existing financial system, while assuming that problems nowadays tackled though financial policies will be solved in similar manners in a forthcoming Bitcoin era.

3.3 Co-existence with other monies

Following [7] I suggest that Bitoin-like systems may co-exist just like different monies do nowadays. However MLEXICs will not be limited by the geographical boundaries that are so characteristic for today's monies. Instead different MLEXICs may serve different user communities, or different purposes, in such a way that a single agent simultaneously uses different MLEXICs.

4 Concluding remarks

Finally I will have some remarks about financial innovators and I will formulate some speculation on how Bitcoin, or rather Bitcoin-like financial technologies of an EXIM brand may further develop in connection with Islamic Finance.

4.1 Financial innovators: Maududi, Gesell, and Nakamoto

In [7] a connection is made between Maududi who is often credited as an originator of Islamic Finance in its modern form, Gesell, who proposed demurrage, a form of personalized and artificial negative interest, and Nakamoto. These names may be considered central figures in the development of unconventional financial systems and methodologies. Interestingly they entertained vastly different views towards interest payment. In each case the lasting impact of the contribution to the development of money cannot yet be appreciated. Financial innovations take many years and giving a convincing assessment of the impact of Nakamoto's contribution may not be doable within the next 50 years.

4.2 What will happen? What may happen?

There is a significant probability (higher than 99% I would guess) that Bitcoin as it is in existence now will disappear from the scene and that some investors will be disappointed. It is mainly the efforts in mining by those who have accumulated BTC stock without selling in between who may loose real money when that happens. The current rate of BTC (around 425 USD while sliding downwards at the time of writing) takes such risks into account. That rate may perhaps be considered a market estimate of exactly that risk.

Bitcoin-like technology and what was called the Nakamoto-architecture in [7] is a different story altogether. This technology may well stay with us for a long time (see [18] for a recent statement to that extent, and [24] for a recent opposite opinion) and the risk that Bitcoin represents for conventional finance is not primarily residing in the current Bitcoin infrastructure itself but in the proof that has already been delivered that the web is as good and cheap for transferring (informational) money as it is for the distribution of all other informational commodities. Moreover it has now been proven that with the modest means of an open source community a system can be delivered and maintained that seems to be able to compete with the systems of professional banking.

Now it seems to me that either by adopting Bitcoin, and in particular by adopting its perception as an EXIM, while somewhat reorganizing the mining system, or by reengineering the Bitcoin design and its open source software into a newer system with an even better fit to the needs of IFR compliant finance, those who intend to promote IFR compliant financial structures would avail themselves of a remarkably cost effective financial instrument for which interest prohibition comes for free and which reduces incentives for an almost unlimited and ultimately counterproductive accumulation of debt.

References

[1] Simon Barber, Xavier Boyen, Elain Shi, and Ersin Uzun. Bitter to better–how to make Bitcoin a better currency. *In: A.D. Keromytis (ed.): FC 2012*, LNCS 7397, 399–414 (2012).

[2] Jan A. Bergstra. Real Islamic Logic.
`arXiv:1103.4515 [cs.LO]` (2011).

[3] Jan A. Bergstra. Dialectical roots for interest prohibition theory.
`arXiv:1105.2900 [q-fin.GN]` (2011).

[4] Jan A. Bergstra. A Rationale for Crescent-Star Finance.
`http://crescent-star-finance.blogspot.nl` (2011)

[5] Jan A. Bergstra. Formaleuros, formalbitcoins, and virtual monies.
`arXiv:1008.0616v2 [cs.CY]` (2013).

[6] Jan A. Bergstra. Bitcoin and Islamic Finance.
University of Amsterdam, Informatics Institute, Report TCS1406, April 2014, `http://www.science.uva.nl/pub/programming-research/tcsreports/TCS1406.pdf` (2014).

[7] Jan A. Bergstra and Karl de Leeuw. Bitcoin and Beyond: Exclusively Informational Money. `arXiv:1304.4758v2 [cs.CY]` (2013).

[8] Jan A. Bergstra and Karl de Leeuw. Questions related to Bitcoin and other Informational Money. `arXiv:1305.5956v2 [cs.CY]` (2013).

[9] J.A. Bergstra and C.A. Middelburg. An application specific informal logic for interest prohibition theory. `arXiv:1104.0308 [q-fin.GN]` (2011).

[10] J.A. Bergstra and C.A. Middelburg. Preliminaries to an investigation of reduced product set finance. *JKAU: Islamic Economics*, 24(1):175–210 (2011).

[11] 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).

[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. arXiv:1402.4778, (2014).

[14] Jerry Brito and Andrea Castillo. Bitcoin, a Primer for Policymakers. *Mercatus Center, George Mason University,* (2013).

[15] Nicolas T. Courtois, Marek Grajek, and Rahul Naik. The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining. arXiv preprint arXiv:1310.7935, (2013).

[16] Luciano Floridi. Philosophy of Information. *Oxford University Press*, ISBN 978-0-19-923239-0 (2011).

[17] Reuben Grinberg. Bitcoin: an alternative digital currency. *Hastings Sci. and Tech. Law J.*, 159–208 (2012).

[18] Benton E. Gup. What is money? From commodities to virtual currencies/Bitcoin. *The University of Alabama, Tuscaloosa*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409172 (2014).

[19] Karl de Leeuw and Jan Bergstra (eds). The history of information security–A comprehensive handbook. *Elsevier* (2007).

[20] Bill Maurer, Taylor C. Nelms, and Lana Swartz. "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. *Social Semiotics*, DOI:10.1080/10350330.2013.777594 (2013).

[21] C.A. Middelburg. A survey of paraconsistent logics. textttarXiv:1104.4324 [cs.LO] (2011).

[22] Satoshi Nakamoto. Bitcoin: a peer-to-peer electronic cash system. http://Bitcoin.org/Bitcoin.pdf (2008).

[23] Peter Šurda. Personal communication (by email), (April 2014).

[24] Daniel L. Thornton. Are virtual "currencies" likely to succeed? *Economic Research, Federal Reserve Bank of St. Louis*, https://research.stlouisfed.org/publications/es/article/10092 (2014).

Electronic Reports Series of section Theory of Computer Science

Within this series the following reports appeared.

[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. Diertens, *The Refined Function-Behaviour-Structure Framework*, section Theory of Computer Science - University of Amsterdam, 2013.

[TCS1202] B. Diertens, *From Functions to Object-Orientation by Abstraction*, section Theory of Computer Science - University of Amsterdam, 2012.

[TCS1201] B. Diertens, *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 Architecures*, 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: www.science.uva.nl/research/prog/

Electronic Report Series

section Theory of Computer Science
Faculty of Science
University of Amsterdam

Science Park 904
1098 XG Amsterdam
the Netherlands

www.science.uva.nl/research/prog/