University of Amsterdam

Theory of Computer Science

Bitcoin, a Money-like Informational Commodity

J.A. Bergstra
W.P. Weijland

Report TCS1402 February 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

W.P. Weijland

section Theory of Computer Science
Faculty of Science
University of Amsterdam

Science Park 904
1098 XH   Amsterdam
the Netherlands

e-mail: W.P.Weijland@uva.nl

Theory of Computer Science Electronic Report Series

Bitcoin: a Money-like Informational Commodity

Jan A. Bergstra & Peter Weijland

Informatics Institute, University of Amsterdam
Email: j.a.bergstra@uva.nl, w.p.weijland@uva.nl

February 10, 2014

Abstract

The question "what is Bitcoin" allows for many answers depending on the objectives aimed at when providing such answers. The question addressed in this paper is to determine a top-level classification, or type, for Bitcoin. We will classify Bitcoin as a system of type money-like informational commodity (MLIC).

Keywords and phrases: informational money, informational commodity, near-money, cryptocurrency, Bitcoin.

Contents

1 Introduction

For an artifact X we will denote with $\mathrm{BT}(X)$ the class of base types of X. We do not claim that each artifact X has a base type. A base type of X should express a characteristic property or objective for X. We intend to apply our analysis in the case that $X=$ Bitcoin, and we will assume that Bitcoin is an artifact.[1]

We will use a notational distinction between X, a term from some syntax, and $m(X)$, the meaning of X in the world. Most plausibly $m(X)$ is not a term from some syntax. The question "what is $m(\text{Bitcoin})$" is not easy to answer. Informatics provides no answers to such questions because it is initially unclear which aspects of Bitcoin, when viewed as an operational distributed software system with an evolving human user community, must be taken into account.

Base types for X need not be unique. For instance if X is an airplane (say it is of type A for airplane) and at the same time X is a propellor airplane (say it is of type type A_p) then both A and A_p may be considered

to be base types for X (that is members of $\mathrm{BT}(X)$). In this case A_p is a subtype of A. Evidently different base types for X must have a non-empty intersection because $m(X)$ is included in the extension of each base type for X. Extensions of base types of X are partially ordered, but not necessarily totally ordered, by the subset relation for their extensions.

An optimal base type, if it exists, is concise, that is its description is simple, and at the same time it is informative. These two criteria work in opposite directions. Finding an optimal base type for an artifact class[2] may be impossible or unrewarding. For instance looking for a base type for "organization" is probably pointless, because "organization" is best seen as a base type itself.

We will be interested in the case where $X=$ Bitcoin.

1.1 Looking for an ontology of monies

Our contribution aims at a conceptualization of a part of the area of money. A conceptualization may precede formalization in an ontology (for instance making use of the ologs of [40]), and codification of the ontology in dedicated notation such as OWL ([27]). Conventional money, informational money, and money-like commodities, together span a wealth of possibilities for which a sound and stable ontological framework can be developed and combined with existing ontological frameworks such as the enterprise ontology of [41].

1.2 Defining versus typing

When considering a class term Y for some kind of entities with Y still vaguely specified by means of keywords or combinations thereof, the objective may arise to define "being a Y" in

[1] Obviously, the artifact called Bitcoin is a carrier for an activity (process or system) that involves human agents as well, and which for that reason cannot be understood as an artifact.

[2] Instead of artifact class one may prefer to speak of an artifact kind. For a discussion of monies from the perspective of natural kinds and artifact kinds see [9].

a more rigorous fashion. We write $|Y|$ for the extension of Y, that is the class of all of its members. In practice membership of $|Y|$ may be a matter of degree, plausibility, or probability. For instance with $Y=$ "car" (a word serving as a class term), $|Y|$ is the collection of all cars.[3] The extension $|Y|$ of Y may vary in time, we write $|Y|^t$ for the extension of Y at time t.

Now one may wish to consider a particular definition Y_d of Y. We write $|Y_d|$ for the extension of Y_d. Conceivably $|Y_d|$ turns out not to have the same extension as Y (that is to differ from $|Y|$) because striving for precision and conciseness entails simplifications that go hand in hand with minor modifications of the initially assumed extension of Y.

1.2.1 Comparing candidate definitions

Arguably a phase may exist in which different definitions, say Y_{d_1} and Y_{d_2}, of Y are viewed as candidates for being given the status of a preferred definition. Candidate definitions may be compared from different angles: conciseness of description, intelligibility, similarity with definitions for related concepts, compliance with standards, conventions and formats, and the proximity of $|Y_{d_i}|$ with the intended extension $|Y|$.

1.2.2 Defining a single entity

Clearly Y_d provides a criterion that precisely the members of $|Y_d|$ satisfy. If we intend to define a single entity X then we proceed to define the singleton class Y_X such that $|Y_X|$ contains only $m(X)$. Not all entities e have an informative definition. Consider the natural number $e = 257$. In principle we may define e as the unique member of the class defined by "a natural number reachable after 258 steps, counting from below, and starting with zero". This definition is hardly informative, however, and it may be considered circular in an unfortunate way.

When considering Bitcoin we find that we may be looking at a singleton class. Assuming that Bitcoin is the process of use and maintenance of a particular evolution of an implementation of "a given specification of Bitcoin" we find that Bitcoin may not have a definition in the same way as 257 fails to have one.

In [6] one may find some meta-theory of definitions, providing a hierarchy of forms of definitions meant to be of use for defining the concept of money. We feel that a definition of Bitcoin, if it can be given at all, would, just as for the concept of money, requires as a basis the availability of some explicit meta-theory of definition. That meta-theory won't provide a definition of the concept of a definition, however, if uninformative circularity is to be avoided. Unavoidably those who agree on concepts defined by means of "definitions" need to agree on "what is a definition" laid down in less rigorous ways.

1.2.3 Typing

Typing of an entity X as an alternative to defining an entity X proceeds by determining a so-called type T for X. Now the extension $|T|$ of T should constitute a class of sufficiently X-like

[3] We can talk about cars without having made up our mind about the "carness" of a wreck. The latter issue being deferred to the phase of precisely defining cars, preferably guided by having an objective for giving that definition at hand.

entities so that the assertion that X is a T makes much sense as an initial piece of information about X. Different types of the same X may provide further information about it. With a base type of X we will denote a type for X which can be used as a first characterization of "what kind of entity X is".

Providing a type for X may require the introduction of a new type description. That corresponds to the result of finding a definition of a class with a larger extension than the entity X alone.

1.2.4 Describing

We will use description as a term to denote any manner for indicating a class of entities of whatsoever kind. Typically one would start out with a description of X and then proceed towards either proposing a type for X or a definition for X. Obviously in this approach the meta-theory of definition won't apply to descriptions.

1.3 Problem statement

Our question is (i) to argue that BT(Bitcoin) is non-empty, and (ii) to determine an optimal base type (or preferred base type), named OBT(Bitcoin), in BT(Bitcoin). A type B in BT(Bitcoin) can be used to explain what kind of thing Bitcoin is in an initial explanation from first principles of it. We do not claim that on a priori grounds the existence of a satisfactory answer to this question is guaranteed.[4]

1.3.1 Methodological difficulty

The problem of finding an optimal type OBT(X) in BT(X), for some kind X, can only be stated if some description of X has already been found. This suggests the presence of an unfortunate circularity in our problem statement. In fact there is no circularity because we may assume that X is a candidate member of BT(X), it might even be evaluated as being optimal.

Nevertheless we must assume that X has been characterized in a preliminary fashion by means of one or more descriptions that characterize to some extent "what X is", that is a preliminary indication of $|X|$. The difficulty is that the question seems to be stated in terms of its answer. Rather than indicating a circularity, it appears that the mentioned difficulty indicates that the problem of finding an optimal type for an entity is an optimization problem, that may admit a stepwise solution starting with an initial candidate solution.

[4] The original paper on Bitcoin is [35]. We refer to the paragraph "Taking Bitcoin Seriously" of [10] for a statement on the risks of considering Bitcoin from a scholarly perspective. For a technical survey of Bitcoin see e.g. [18]. For some legal information on Bitcoin we refer to [21]. We are not convinced that trying to classify Bitcoin "as a money" requires reconsidering the very concept of money (a viewpoint found in [33]). An exploration of the concept of money may be found in [6], where special emphasis is given to the notion of a money of account of which a virtual money is considered a special case.

1.3.2 Initial kind descriptions

Let IKD(X), the initial kind description of X, be a reasonably clear indication of which Y's are in of the same kind as X. IKD(X) may be quite verbose, it may be too technical still requiring a useful abstraction, it may make use of analogies, it may be a heterogeneous collection of different characterizations al of which are supposed to pertain somehow to those Y's which are supposed to be of the same kind as X. At the same time we allow for the situation that the description is redundant as well as marginally inconsistent. We call an IKD initial because that kind of description is a starting point of the search for an (optimal) element in IKD(X).

In the case of Bitcoin candidates of an IKD abound in the literature. Below we propose an IKD for Bitcoin. Our proposal for IKD(Bitcoin) represents a self-made combination of statements about Bitcoin regularly found on the internet.

1.3.3 IKD(Bitcoin), an initial kind description of Bitcoin

IKD(Bitcoin) reads thus: Bitcoin is a remarkably successful P2P system, mainly consisting of open source clients, which exists since early 2009, having been started up by (at the time of writing) an anonymous programmer or group of programmers. As a tool Bitcoin provides its clients a cryptology based informational money. Amounts in the system are expressed in the unit BTC. The essential feature of Bitcoin is that consists of a P2P network only and at the same time prevents double spending effectively. Bitcoin is also claimed to allow its users a high degree of anonymity. That virtue for the system has been contested by various authors since 2012.

1.3.4 Moneyness and money-likeness

Moneyness is the circumstance that a certain system represents a money (e.g. see [31]). Rather than a binary variable taking values yes and no, moneyness is a matter of degree. With high or significant moneyness we mean that an artifact class could, in principle, be used as a money. The artifact is money-like if its functionality resembles that of a money, though only in part.

We assume that a money-like system or artifact may be further removed from a money than an artifact with a moderate degree of moneyness. Thus we will assume "money-likeness" may be present in some artifact class to some significant degree while moneyness is not.

Claiming that a system or artifact X is money-like requires taking some position concerning the functions of money which X realizes. It is plausible that the money of exchange function is considered indispensable while the money of account function is considered less prominent. Ownership (or possession) of quantities of X must bring with it a bundle of rights resembling that of a quantity of (well-recognized) money. For instance selling one's holding of X at any time to anyone must be a right.

2 Criticizing proposed types for Bitcoin

We will first list some proposals for typing Bitcoin and we will argue why these proposals should be rejected.

2.1 IKD(Bitcoin)

IKD(Bitcoin) does not qualify as an element of BT(Bitcoin) for at least the following reasons:

1. Mentioning double spending attacks should not enter OBT(Bitcoin) though it might be mentioned in some types in BT(Bitcoin). We don't claim that double spending might be permitted, but we merely claim that singling out one of many possible failures is premature when designing an OBT fair any artifact (including Bitcoin).
2. Success is not implied by any optimal base type. Successful artifacts in OBT(Bitcoin) constitute a proper subtype OBT_s(Bitcoin) of OBT(Bitcoin).
3. The year of birth of Bitcoin is an unnecessary detail, which is not an expected entry in any type description in BT(Bitcoin).
4. It being cryptology based is reasonably considered an unnecessary refinement.
5. No mention is made of the status problem: is Bitcoin a money. The suggestion that Bitcoin's status is "money" follows too easily from the phrasing of IKD(Bitcoin).

2.2 Cryptocurrency (CC)

Bitcoin is often called a cryptocurrency (CC). The underlying assumption must be that there is a class of so-called cryptocurrencies to which Bitcoin belongs. We criticize the classification on the following grounds:

1. A cryptocurrency must be a currency.[5] But confirming the status of a "system" as being a currency depends on a plurality of observers some of whom may require that a certain acceptance or usage must have been arrived at by a system before it can be classified as such. Upon its inception Bitcoin did not possess that level of acceptance, and for that reason Bitcoin has not started its existence as a cryptocurrency.
2. Being a cryptocurrency is a status that a system may or may not acquire over time.[6] Assuming that Bitcoin is considered to be a cryptocurrency at some stage then there will

[5] This inference is debatable, but we consider the term cryptocurrency confusing it it does not mean something roughly equivalent to the following: an informational currency, complying with generally accepted requirements for "currencyness" (or equivalently moneyness), for which control (of agents over amounts and corresponding inspections and transactions) has been organized by means of encryption and decryption rather than by means of restricted access policies based on conjectural pseudomonopresence of passwords (see [9]) or on physical access restrictions.

[6] From [4] we quote the question "Does Bitcoin have what it takes to become a serious candidate for a long-lived stable currency, or is it yet another transient fad?" This phrasing suggest that Bitcoin might be considered a candidate currency, and that a currency need not be either long lived or stable.

most likely be variations (alternative designs and systems) of Bitcoin around (perhaps hardly used anymore) which have not been that successful. Such alternative systems should be given the same type, so that Bitcoin might be considered a successful instance of that type. Clearly CC cannot be that type as it contains only systems that have already become successful to a significant extent.

3. Because being a cryptocurrency is the primary success criterion for Bitcoin its classification as a cryptocurrency amounts to a value judgement or a quality assessment rather than as an initial type.[7]

We conclude that as an initial top-level classification for Bitcoin CC is not plausible. That is consistent with the viewpoint that at some stage (and/or in the eyes of some observers) Bitcoin may be or become a system of class CC.

2.3 Digital currency (DC)

The "problem" with digital currency as a member of BT(Bitcoin) is similar to the problem mentioned above with CC. We prefer IM over DC as in general we prefer money over currency as a general term and moreover we consider "digital" to carry an implementation bias which "informational" avoids.

2.4 Informational money (IM)

The difficulty with informational money (IM) as an original class for Bitcoin is precisely the same as for cryptocurrency. Assuming that an informational money is a money, the classification expresses a level of achievement that should not be presupposed.[8]

Our objection to using digital money as an original class for Bitcoin is the same. Stating that Bitcoin can be typed as an informational money need not be understood as an acknowledgement of its status as an unlimited success. Success is a matter of size of circulation and usage. Success is not meant to imply that no alternative is superior.

2.5 Informational near-money (INM)

In [9]) Bitcoin has been classified as an informational near-money. The problem of this classification is that the distance between near-moneys and monies is quite subjective. Near-money says no more than "money-like but perhaps not a money". Classifying Bitcoin as an informational near-money rather than as an informational money solves the problem that its success in terms of realizing "moneyness" is not presupposed, but it is unclear to what extent "near-moneyness" is a criterion of partial success of a so-called near money.

[7] Classifying every book as a bestseller is a similar mistake, and so is classifying every song as a hit.

[8] In [5] the term informaticology (IY) has been explored. In that work Informaticology (IY) is decomposed as: IY = CS + DS + FS = Computer Science + Data Science + Fiction Science. IM has roots in each of these components. The present paper may be classified as a contribution to the exploration of informaticology of informational money.

2.6 Virtual money (VM)

The phrase virtual money shares with informational money and cryptocurrency that it may prematurely oversell Bitcoin as a money (or currency). Besides raising that objection to a classification of Bitcoin as a virtual money, it is hard to make sense of virtuality in this setting as like with virtual memory it would suggest that we are not looking at real money but merely at a virtual look alike of it. In [6] an interpretation of virtual money has been given which takes the unreal aspect into account. Nevertheless, that particular view of virtual money provides no incentive for classifying Bitcoin as such.

2.7 Denationalized money (DM)

A denationalized money is issued by a private party. Although issuing of Bitcoin is very distributed and potentially fully anonymous it is not under control of any state. For that reason it merits the qualification denationalized. DM is less plausible as a type because it implies that the status of a money has been achieved. The criticism regarding DM as a base type for Bitcoin is essentially the same as for CC, DC, and IM.

The Austrian economic school constitutes a source for the viewpoint that monies ought to be denationalized. The Austrian school economist Hayek is often seen as an economist the ideas of whom are materializing with Bitcoin.[9]

2.8 Bitpenny implementation: with Bitpenny a suitable Abstract Money Type

In [10] we have put forward the suggestion that Bitpenny represents an abstract logical specification of the service that one imagines that Bitcoin ideally will provide. For instance Bitpenny achieves by magic that double spending will not occur, while Bitcoin requires sophisticated machinery to implement that property. Bitpenny would represent an Abstract Money Type (AMT). Abstract Money Types have money structures as implementations in the same way as Abstract Data Types have data structures as their implementations. Money structures are as remote from real money as data structures are from real data.

Money structures are processes which evolve in time. Conceivably a money-structure migrates from the status of a near-money to the status of a money and back. Indeed being qualified as a money structure K_m compliant with T_m (an AMT, thus $K_m \in |T_m|$) reflects no social acceptance in a particular state of the structure (as it operates in the real world at some time t) K_m^t of K_m as a money. K_m^t may be merely classified as being money-like.

In the same way K_d being accepted as a data structure compliant with ADT T_d reflects no social acceptance of a particular state K_d^t of K_d as containing data. K_d^t may be merely qualified as a data-like state (of K_d).

Apart from the name Bitpenny which is merely a placeholder for better names, a weakness of this typing of Bitcoin is that Abstract Money Types have yet to be defined and developed.

[9] In [37] Bitcoin is examined from the perspective of compliance with principles of the Austrian school.

In principle, however, this may be a way to go about typing systems like Bitcoin on the long run.

2.9 Attributes and qualifications

If a car is of type CAR then a red car may be viewed as an item in the intersection of types CAR and RED. However, it may be more convincing to consider redness as an attribute (property, or qualification), which applies to entities contained in types or defined by definitions. Some qualities, or claimed qualities, of Bitcoin are best viewed as attributes which do not represent types.

3 Attributes for or properties of Bitcoin

We first list some qualifications for Bitcoin which we consider to be less plausible as type descriptions. When contemplating types for Bitcoin below we do not expect to see these qualifications mentioned. Such qualifications play a role when moving from a type description to narrower type description or to a definition.

3.1 A system for electronic transactions not relying on trust

This is an original qualification from [35].

3.2 P2P system

Bitcoin was designed as a P2P system. Currently users of Bitcoin must trust the collective of miners and the pure P2P status is becoming less obvious.

By stating that Bitcoin is a P2P system not enough information is given about its expected role. (We don't speak of objectives as almost nothing is known (at this stage) about the objectives of Bitcoin's designers.)

Typing Bitcoin as a open source P2P system provides little progress, and it may even be wrong altogether, as there seems to be no requirement that Bitcoin clients are realized as open source programs.

3.3 Reduced product set finance (RPSF)

In [11, 12] we have put forward the notion of an RPSF in order to describe financial systems from which certain features (and corresponding financial products) are banned. One might consider Bitcoin an RPSF because it does not allow for governance by means of management of the monetary base.

Classifying Bitcoin as an RPSF is not plausible at this stage because like money as well as like currency, finance expresses requirements on a system that Bitcoin may not yet meet.

3.4 The first successful digital coin: a landmark in the history of information security

One of us has a vested interest in the history of information security (see [32]) and viewing P2P based money-like systems as a historic necessity of which Bitcoin is a first realistic exemplar may be justified and may on the long run be what will take place. What counts against this approach to Bitcoin typing is that it insufficiently expresses the important aspect that Bitcoin may still have a long and successful future existence and evolution ahead of it (and regarding proposals for its improvement see [4]). In addition not everybody may consider Bitcoin to be a success as a coin, if being a coin counts for anything less than being a currency.[10]

3.5 Converting rejected base type options to attributes

When criticizing IM as a base type for Bitcoin one may uphold that it is an attribute that Bitcoin might be a proto IM, where a pro to X is an entity which is expected (hoped, intended) to evolve sooner or later into an X. Now it is reasonable to have proto CC, proto DC, proto IM, and proto DM as attributes of Bitcoin.

4 Candidate types for BT(Bitcoin)

Given some kind X, which may be an artifact kind, or a natural kind, finding a suitable type in BT(X) requires (i) the preparatory collection of a number of options, that is candidate members, (ii) validating the conclusion that BT(X) is non-empty, and (iii) choosing an optimal element OBT(X) of BT(X).

4.1 Candidate cryptocurrency (CCC)

Candidate cryptocurrency (CCC) may well be a type in BT(Bitcoin), and CCC refers to a larger class than CC, while it is contained in MLICcp as defined below. A disadvantage of CCC as a type is that there is no known procedure for leaving the candidate status. Another problem is that some may think that it can be shown that Bitcoin cannot acquire CC status, from which it would follow that Bitcoin is not a CCC either.

4.2 Cryptocoinage (CCo)

A cryptocoinage (CCo) plausibly refers to the coinage of a larger money-like system. As coinage is unlikely to refer to an entire money including each of its money types, this is not a plausible typing of Bitcoin. The name Bitcoin is suggestive of it being about coins but we fail to see in what sense the quantities of Bitcoin are to be viewed as coins.

[10] As an open source program Bitcoin is successful already, by having many participants tot its P2P system, by capturing the imagination of public media, by driving the emergence of a dedicated hardware industry for mining, and by forcing all major financial institutions to issue policy statements about it.

4.3 Internet based business (IBB)

Possession of BTC quantities may be considered as a proportional share in an new kind of internet startup (now in year 6 of its existence). Mining is the method for issuing and distributing new shares. New shares are issued at a diminishing rate, and the hypothetical objective of the business is to become dominant factor in what is called today the monetary system. Bitcoin shares constitute the money at the same time. If Bitcoin happens to become a dominant factor in the world-wide monetary system the value of a BTC will rise astronomically (though not expressible in the Euro's from the past anymore).

The business model is to become strong on the internet in an underground style. In [9] it has been argued that this view allows an approach to the determination of the value of a BTC. Thinking along this lines the current rate of EUR 600 to a single BTC will correspond with a 20 year survival probability of Bitcoin (as an internet based business) of 10^{-5}.

IBB is a reasonable type for Bitcoin if one intends to explain the economic risks, both upside and downside, of an "investment" in Bitcoin (i.e. buying BTC against EUR). As a business model IBB is really new, which is an attractive aspect of this candidate type. But we believe that the virtue of IBB as a type for Bitcoin is metaphorical rather than intrinsic.

4.4 Investment scheme (IS)

Assuming that the store of value function of Bitcoin outweighs its money of exchange function, one may suggest that it constitutes an investment scheme IS). This view is valid if BTC is bought and sold in exchange for conventional monies only. It seems rather implausible that Bitcoin can survive on this basis, but at the same that very state of affairs cannot be excluded and for that reason we consider "investment scheme" to be a conceivable type for Bitcoin.

An individual user viewing Bitcoin as an investment scheme only is currently considered to be a speculator, because there is no intrinsic argument for BTC to increase its value against conventional monies.[11]

4.5 Multi-player computer game (MPCG)

One may consider Bitcoin to constitute a distributed and multi-player computer game (MPCG). The game is to acquire control over as many BTC as possible. Good gaming is rewarded by other gamers who buy accounts. As a side-track all participants collectively try to make progress concerning attacks on the secure hash function SHA-256.

Viewing Bictoin as an MPCG deviates from a common understanding of its purpose but as a typing it may be useful for some purposes.

[11] The number of outstanding BTC will have some maximum below 21 million in a phase where mining results balance losses of Bitcoin accessibility by users who physically use secret keys to active accounts. From that point onwards losses (of al users together) will outweigh mining (creation). On the very long run, and under the assumption that Bitcoin loss will always have some positive probability each BTC will get lost.

4.6 Informational money-like commodity (IMLC)

Bitcoin provides tradable quantities, with money-like status. On that basis it may be viewed as a (system implementing a) money-like commodity (MLC). Because its exists (or at least it can can exist) in terms of information only Bitcoin is also an informational MLC. We notice that MLC is also a plausible candidate for a type in BT(Bitcoin), but we consider it to be significantly less informative than IMLC. In item 4.7 below we will discuss the way in which Bitcoin might be considered to constitute a commodity.

4.7 Money-like informational commodity (MLIC)

Viewing Bitcoin as a system providing a platform offering the following features:

1. a system for giving agents access, and
2. facilitating the exchange of that access, to
3. informationally given amounts measured in BTC the unit of Bitcoin), through
4. the scarce resource of collections of accessible (to the agents) secret keys, and
5. "a Bitcoin" as a unit of access within this system,

one may grasp how Bitcoin may refer to a commodity, the substance of which consists of information that is independent of any accidental carrier of it, while access to it is scarce.[12]

Thus, in more detail, said commodity amenable to being in the possession of an agent, consists of: conjectural pseudo-monopresent (that is secret) "keyware" (that is collections of keys), the size (commodity measure, commodity weight, commodity volume) of which is determined as the sum of the amounts these secret keys give access to.

After an exchange the same amounts are accessible from other secret keys, equally assumed to enjoy conjectural pseudomono-presence, though in the possession of another agent.

The exchange value of a commodity positively correlates with its size, and with the public trust in the pseudo-monopresence (see [9]) of the (secret) keys from the perspective of the agent currently possessing the keyware.

Playing the role of a money, we will speak of a money-like informational commodity (MLIC).[13]

4.7.1 Ownership and possession of MLIC

A vast legal and philosophical literature explains concepts like property, title to ownership, ownership of property, and possession. We mention [19] as an example of such works. In that paper the coming about of property through the rule of first possession is scrutinized.

[12] Informational commodity is an subclass of information object, a class for which a conceptual analysis can be found in [17].

[13] We notice that viewing information as a commodity has a long history, e.g. see [16]. In [23] explicit mention is made that information as a commodity will have a price, plausibly in excess of the cost of delivery, whereas information in the public domain need not.

We will assume that the commodities underlying an MLIC can be in the possession of agents. Possession of a quantity of the commodity provides an agent with a number of capabilities that are self-explanatory from the perspective of a conventional functionality of money. The extent to which agents can be owners of an item may vary from case to case. By speaking of an MLIC no commitment is made to a particular bundle of rights which is implied by ownership or possession of an item. Technically the same MLIC may exist in different legal regimes.[14]

4.7.2 Preference of MLIC over IMLC

As a type for Bitcoin MLIC is acceptable as well as IMLC, though we prefer MLIC because:

1. Bitcoin cannot be an IMLC without being an informational commodity.
2. The phrase informational commodity is relatively new and without it being accepted IMLC is hard to make sense of.
3. Without insisting that Bitcoin keyware is a substance constituting an informational commodity, the claim that its secret keys give access to a commodity seems to be unconvincing.

The use of the concept of a commodity requires justification. About the question what is a commodity we take a quote from [1], which as we claim applies to Bitcoin keyware:

> To say that something is a commodity is to claim that the norms of the market are appropriate for regulating its production, exchange, and enjoyment. To the extent that moral principles or ethical ideals preclude the application of market norms to a good we may say that the good is not a proper commodity.

4.7.3 Remarks on commodification and informational commodities

Necessarily an MLIC is a kind of commodity. In other words MLIC is a subtype of commodities. Commodities may come about in different ways. Individual commodities are build, produced, generated, or configured, whereas a specific commodity type may come about through a process of commodification. Commodification transforms a type of disparate (though somehow related) entities into a class of entities that can be exchanged on a free market and which are paid for by money.[15]

We suggest that Bitcoin may be considered a result (among many other such results) of commodification (of circulating amounts) starting from digital monies that are still under state control just as conventional monies like EUR and USD. Such monies seem not to meet the definition of a commodity because free market forces are not allowed to regulate their market value.

[14] This independence of circulation technology from legal settings is discussed below in paragraph 6.1.1 on physical coins.

[15] In [42] commodification is defined as: "the process by which objects and activities come to be evaluated primarily in terms of their exchange value in the context of trade in addition to any use-value such commodities might have."

In [22] the phrase informational commodity is used for private information which is owned by an individual. The institution of ownership for that particular kind of commodity is called privacy. As a type of that sort of information we suggest: personal data oriented informational commodity (PDOIC). Privacy indicates that commodities of type BLIC may be owned by an owner with the effect that all forms of access by non-owners are a breach of the rights the owner enjoys in virtue of his ownership. The use of informational commodity is justified in this case because there is a market for such information, even if privacy is about regulating and constraining that market.

4.8 Partial informational money (PIM)/partial cryptocurrency (PCC)

With a partial money we may denote any near-money or money-like commodity which can fulfil some selected subset, (possibly all) of the functions required of a money, and which in addition may fulfil these only partially what is expected for these selected functions. Given an understanding of an informational money (IM) or a cryptocurrency (CC), one may derive from this definition of a partial money what a partial IM (PIM) or a partial CC (PCC) can be.

Both PIM and PCC are plausible types in BT(Bitcoin) and plausible candidates for the role of an OBT(Bitcoin).

5 MLIC, our proposed type OBT(Bitcoin)

The main contribution of our paper is formulating the proposal that MLIC is in BT(Bitcoin) and moreover that MLIC = OBT(Bitcoin).[16]

5.1 Motivation

We see the following arguments in favor of setting OBT(Bitcoin) = MLIC.

1. MLIC is very compact and it specifies a large class of systems from which Bitcoin might emerge as the winner.
2. MLIC seems not to make any false or even contested claims.
3. MLIC is applicable to Bitcoin during all stages of its “life”.
4. MLIC is preferred over PIM and PCC because it is “more consistent” with the eventuality that Bitcoin may not be classified as a money after all in which case its final type would probably be neither PIM nor PCC because arguments for witholding Bitcoin the status of a money would stand in the way.

[16] In `http://en.wikipedia.org/wiki/List_of_cryptocurrencies` for a survey of so-called cryptocurrencies, all of which we propose to classify as MLICs also. See also [39].

5.2 Weaknesses of the type MLIC in its role of OBT(Bitcoin)

Typing Bitcoin as an MLIC, however, leads to many subsequent questions some of which may point to weaknesses of this proposal.

1. Bitcoin is internet based; MLIC fails to indicate that Bitcoin is only useful for those agents who can access the internet freely, to the extent that they can run a specific downloaded client. This restriction may be at odds with property rights on a specific Bitcoin informational commodity to which an agent may be entitled.
2. A potentially problematic aspect of MLIC is the use of commodity as a root concept. Indeed one may claim that amounts are commodity-like at best but are not commodities proper. This objection may be remedied by viewing "money-like commodity" as a semantic unit rather than as referring to a commodity which in addition is money-like. (A similar situation is found with "free will" which according to some philosophers is not pointing to a will (state of willing) that in addition happens to be free.)
3. MLIC fails to express the fact that no backing of value for BTC holdings from outside the system is provided. All value of Bitcoin holdings is to be realized within or by the Bitcoin system, through users who have trust and confidence in the system.

5.3 Counter arguments and risk analysis

Many arguments against the typing of Bitcoin as an MLIC may be brought forward. It seems that legal, economic, monetary, and informaticological perspectives are so disparate that it is inconceivable that a single type proposed for Bitcoin is equally defensible from each of these perspectives.

For instance, while moving from a commodity to a money (and back) may be a matter of evolution from an economic perspective, that may not be the case from a legal perspective. And once Bitcoin like systems become mainstream components of computing infrastructures technical names (like database, laptop, cloud, computer network) may become more prominent that use-related types.

In [36] it is argued that information is intangible and that there is a larger distance between information and its embodiment than with other, more conventional goods. This argument hardly applies to a Bitcoin secret key the possession of which (under the assumption of conjectural pseudo-monopresence) is very much linked to its embodiment. Thus, it must be accepted at least for some informational commodities (e.g. the one's we are contemplating in the context of Bitcoin) a notion of possession, and the corresponding uniqueness of a possessor, make perfect sense.

We consider it implausible that someone would criticize classifying Bitcoin as an MLIC on the grounds that it is to early too award it that status, for instance in the light of deficient regulation (see [30]).

Of course some may consider the classification of Bitcoin as an MLIC as being too cautious, a possibility which brings us to contemplating MLIC maturity levels. Our use of "informational" may be criticized for lacking compliance with a preferred philosophy of information (see [20]).

In [15] a critique of the design of Bitcoin mining is given. Such arguments do not stand in the way if classifying Bitcoin as an MLIC but may constitute objections against assigning it a higher maturity level such as the level IMoE/MfSoV below.

In any case a risk that we see in opting for MLIC in the role of OBT(Bitcoin) is that legal differences between commodity and money turn out to be rather large. Considered from a legal perspective, control over a secret key of a Bitcoin address may prove to be more remote from the possession of a quantity of some commodity than it proves to be from the possession of an amount of money.

5.4 Ramifications of MLIC

Assuming that MLIC serves as a base type for Bitcoin and Bitcoin like systems one is led to the question how large this class of systems might be. For instance one may wonder to what extent cryptographic techniques are necessary for the realization of each conceivable MLIC. We briefly consider two conceivable alternative means of implementation.

5.4.1 Cryptology based MLIC: CBMLIC

Bitcoin and similar systems are essentially based on an extensive and essential use of cryptographic techniques and access control seems to play a secondary role only. The role of cryptography will stay prominent as Bitcoin evolves and the role of access control may increase. For this reason we consider the type CBMLIC (for Cryptology Based MLIC) to be a valid element of BT(Bitcoin). CBMLIC is a refinement of MLIC and we don't prefer it over MLIC as a candidate OBT(Bitcoin) because it is still possible that each MLIC is cryptology based in which case the addition of this aspect to a notation for the type would be futile in hindsight.

5.4.2 Access control based MLIC: ACBMLIC

It can be imagined that an MLIC makes use of password protected data only. That will probably not be an open source P2P system. We suggest that ACBMLIC is coined as a type for which no instances have been proposed at this stage. If ACBMLIC turns out to be empty then by consequence CBMLIC is equal to MLIC.

6 Alternatives for MLIC

Although the future of money is probably informational, it would be too soon to write off non-informational monies or non-informational money-like commodities as being, no more than a thing from the past. When contemplating alternatives to MLIC it becomes important to consider partial monies or rather compartments of monies. On the physical side, to understand the importance of metallic coins as a component of the Euro system it is relatively unimportant that Euro coins have a fixed value in terms of Euro. Small variations can be handled and one may imagine a situation where coins have fluctuating values and a central bank sees to it that these fluctuations are not too big by means of targeted interventions, which are not meant to stabilize coin value under all circumstances and with perfect precision.

6.1 Physical MLC: PMLC

The intuition of money is often connected with coins. At a closer inspection coins are fairly difficult to understand. In [6] an attempt was made to understand "the logic of coins".

6.1.1 Logic of coins

To see the difficulties with understanding a logic of coins one imagines the task to define forgery. What is a false coin? Is it a coin that fails to comply with requirements on its physical constitution, or is it a coin that started its circulation in a fraudulent manner. The difference between both approaches is large. Similarly there is a remarkable distinction between coins and banknotes resulting from these having unique identification numbers: from two identical banknotes at least one must be the product of counterfeit. And if no physical anomalies can be established one is forced to accept a theory of counterfeit that takes the entire circulation of banknotes into account.

A thought experiment relevant for Bitcoin is to imagine a PMLC which constitutes of a certain range of coins only. Of particular importance is to grasp the ramifications of ownership, possession, holding, lending, and stealing. On needs a model where a community of agents makes use of coins. Each coin c can stand in various relations to an agent P: P may own c, P may be in the possession of c (the contrast between ownership and possession has been analyzed originally in detail by Kant, see e.g. [43], and subsequently by many other authors), or P may be a holder of c. At this stage ramifications abound. In [34] four views of property (and ownership) are discussed, each of which may potentially give rise to another view on how coins relate to agents in terms of ownership, possession, and capabilities of these. In [38] one of these views, so-called multi-variable essentialism, has been worked out operationally and in detail by giving six rules of conduct that may be considered constitutive of the concept of owning a property, while none of these rules is considered absolutely necessary in each individual case. Different bundles of rights may be attached to owners, possessors, and holders, of a coin, thus leading to different legal settings for a coin circulation based on the same circulation mechanics. We expect that surveying the different options in the case of metallic coins will shed light on the different possibilities in this respect for an IM. Investigating this matter seems not to have been carried out in the existing literature on coin circulation

In [9] "exclusively informational money" (EXIM) was "coined" for denoting an IM where ownership is reduced to possession. By looking at metallic coin circulation models, legal and philosophical aspects of such "exotic" legal options (for different relevant bundles of rights) can be studied without being detracted by the complexities of distributed computing. In [26] intention is put forward as a prerequisite for possession, and different views are contrasted regarding the perspective (intention) of future ownership being a prerequisite for possession as well. Following this line of thought an EXIM cannot even be defined without making use of a notion of intention, and in addition it may hardly have a place in a world dominantly inhabited by artificial agents.

6.1.2 Advantages of (metallic) coins

Looking at physical coins as a means of exchange which itself constitutes a commodity used exactly for that purpose, the following advantages of metallic coins are noticeable:

1. Use for exchange is possible in a significant range of seemingly adverse circumstances: outdoor, windy weather, wet and dry, low and high temperature, during a power outage.

2. Use for exchange is technically simple.

3. Safeguarding the physical security of coins is comparable (and no more difficult) to maintaining the physical safety of one's body.

4. The possession of coins can be demonstrated to a potential partner before a transaction is performed.

5. Storage is relatively easy and can be performed for a very long time.

We expect that money-like coins will be around for a very long time, in the light of these advantages. That does not necessarily imply that such coins must be pegged to entities/quantities in another money-like system which plays the role of a (real) money. Although these advantages are well-known for metallic coins it is quite possible that new materials allow for the design and mass production of even better coins.

6.2 Computational MLC: CMLC

Computational money unlike informational money has the property that each occurrence of it requires a functioning machine. For instance even if one has a security code memorized that allows access to some chip card containing a money like quantity, only the working chip card once activated via the security code will allow spending the (near) money (or the money-like commodity) that it contains. If that chip card is destroyed the commodity it contains will disappear simultaneously with it.[17]

This differs from the situation of Bitcoin where one may imagine that all blockchain data are printed, that all wallet information is physically stored, that all machines are destroyed and that in a second round every user get a new machine. Subsequently all data written on paper (or on disk) are loaded into the various machines and the entire Bitcoin system is again live. With a computational money or more generally with a computational MLIC a corresponding course of events is unimaginable.

7 MLIC maturity levels

Supposing that an MLIC say XYZcoin progresses from the initial MLIC classification to the stage of an informational money (IM). Now having IM status implies that the moneyness of XYZcoin has been sufficiently generally accepted, the latter depending on one's philosophy

[17] THe Dutch Chipknip is an example of this.

of money. It is practical that XYZcoin's progression through the hierarchy of maturity levels towards the IM stage moves trough stages that admit explicit naming as well.[18] In this Section we will propose a naming scheme for such maturity levels.

7.1 Below IM: CIMoE, IMoE

An informational money of exchange (IMoE) may fail as a money of account (MoA) and it may mail fail to provide a (reliable) store of value (SoV, or MfSoV, money for SoV), it may fail to provide the function of a money of documentation (MoD), that is a tool for the preservation of historic information in excess of mere balance sheet aggregation.[19]

Before IMoE there is the candidate IMoE stage. An MLIC is a CIMoE if the path of development towards the IMoE stage is conceptually clear, though there may be risks that it will not be successful. We consider Bitcoin to have reached maturity level CIMoE. This typing judgement implies that we consider it to provide sufficient defense against double spending attacks (e.g. see [25]).

7.1.1 IMoE/MoD, IMoE/MoD/MoA, IMoE/MoD/MoA/MfSoV

Beyond the IMoE stage we distinguish IMoE/IMoD, where the MLIC serves as an MoE and also as an MoD. A further stage is IMoE/MoD/IMoA, which is a stage where an MLIC serves as an IMoE/MoD and as an MoA at the same time. Still the long term SoV functionality may be considered problematic. If that functionality has been acquired as well we find the maturity level IMoE/MoD/MoA/MfSoV.

Exactly which features can be productively combined in an informational money requires further thought. At this stage many issues about the integration of these features and about system governance, quality control, and risk management must be considered.[20]

7.1.2 CIM

An important intermediate stage close to IM is CIM, candidate IM. A CIM is an MLIC that must have reached IMoE/MoD/MoA/MfSoV maturity. Moreover, XYZcoin has reached CIM level if it has become sufficiently clear how XYZcoin can further develop in terms of usage and support structure so that it would eventually qualify as an IM. Bitcoin has not yet reached CIM status because it is not sufficiently clear that the MfSoV functionality is potentially performed sufficiently well by any Bitcoin-like MLIC, including Bitcoin itself. CIMs compete for IM status and achieving IM maturity is a gradual matter.

[18] In [24] arguments are listed for expecting demise of Bitcoin. Having a maturity level classification scheme at hand, such arguments can be framed positively, acknowledging what has been achieved, rather than negatively.

[19] More functionalities of money can be distinguished, for instance MfVM (money for vending machines, see [3].)

[20] For instance robustness against abuse must be taken into account (see [28]).

7.2 IM

IM status is a very high maturity level. When having reached that status it competes with EUR and USD on par in terms of technology and mechanisms. This stage may be quite distant, it may never arise. And it may be transient as the evolution of an MLIC may also involve a decrease of maturity level.

For an IM some robustness against risks is important. Nevertheless robustness a against risks may be uncertain. The use of elliptic curve cryptography (see ECDSA in [29]) makes it vulnerable to attacks by means of quantum computers, once in existence. We assume that this is not an argument against Bitcoin having a CIM or IM status at some stage because we assume that as an evolving P2P system it has the flexibility to develop towards making use of stronger cryptographic methods when needed. A similar remark would be made in reply to someone who considers SHA-256 (see [13] for a recent specification of that algorithm by means of an instruction sequence) to be a critical weakness of the mining mechanism.

Coins from a conventional money can be handled anonymously. It is unclear to us to what extent the ability to make anonymous use of a money (or of the transfer of specific items of a particular money) must be considered "intrinsic" to a money. And if so, it is unclear to what extent Bitcoin might even achieve CIM status, given the deficiencies concerning its anonymity feature which have been widely documented (e.g. see [2, 14]).

7.2.1 What is an IM?

The quality of being an IM is hard to grasp in a few words. Quite difficult to assess is the quality of an IM as a store of value. We make some remarks about this particular aspect.

- The MfSoV (money for store of value) quality of the Euro depends on one's trust in an open ended political process currently guided from institutions seated in Brussels and in Frankfurt am Main. Suppose one thinks in terms of say 250 years. Is the Euro any better than Bitcoin, who knows?

- Against which disasters, social unrest, earthquakes, inundations, fires, crimes, or other problems, must a SoV function of money protect the holder of an amount? Is transfer to a next generation upon the holder's death an important matter, and if so what requirements must be imposed. As it seems this "problem" is far from having been solved for Bitcoin.

- One may imagine that metallic coins for Euro's are replaced by money-like commodities, so as to undo the Euro (or any other recognized money) from the complexity of coin circulation which introduces such aspects as loss and wear in ways foreign to the informational world. One may also introduce physical coins as a money-like commodity to a Bitcoin style MLIC. Is this form of convergence between monies a reasonable path to contemplate? This matters if one insists that metallic coins (or banknotes) offer their users a package of advantages that cannot be replaced by means of information technology based equipment.

- Is it at all relevant to compare a closed world such as Bitcoin, the evolution of which is supposedly limited to a fairly restricted scope of technical modification and to minimal external influence of a political nature, to a money based on an open ended political process (such the Euro). Is it reasonable to say that the Euro provides an SoV if in fact the EU political process constitutes (or claims to constitute) that SoV? If the "value" of money (say in EUR) is merely a claim on the outcome of a political process, then store of value is rather empty if the ability of the political system to materialize the claims is undermined.

- If Euro's don't do much more than providing a bookkeeping of claims which may or may not loose their value, that is Euro's are mainly a money of account for measuring the value of bonds, then storage of value must take place (if at all) outside the sphere of money. The objection to an IM (supposedly still seen as a CIM) that it fails to provide a store of claims against an important institution (an objection that has been formulated about Bitcoin) may be valid while at the same time there is no support for the objection that it fails to provide a store of value (which has been formulated about Bitcoin as well).

  For making this distinction between storage of claims and storage of values we will put forward two arguments. First of all with a conventional money the institution stores the underlying value in different ways (from storing money proper) thus undermining the argument that a conventional money provides a store of value (and thereby weakening the objection that an IM does not). Secondly the social acceptance and ubiquitous usage of an IM may constitute a "real value" which is stable and may be considered being stored, in a way that a conventional money does not. It is conceivable that precisely because a conventional money constitutes a bookkeeping of claims its own value (as a communicative tool) is minimal once the underlying claims are not counted to contribute to the value

- In different words an IM (which Bitcoin might become) serves as an important part of the communication infrastructure of a community and in that form it stores exactly the combined value of that communication mechanism. Beyond doubt this is a real value and at this stage it is hard to assess how it will compare with the value of assets that underly the stability of conventional monies.

7.3 Beyond IM: RDIM, DIM

Beyond the IM stage we will distinguish two further development stages of an MLIC: RDIM, a relatively dominant IM, which is an IM that plays a dominant role between other IMs (that is relative to the class of MLICs), and a DIM, a dominant IM which is an IM that plays a dominant role in comparison with all other monies.

In [9] EXIM (exclusively informational money) has been put forward as a further important modality of an IM. Perhaps EXIM may be placed between IM and RDIM, depending on how important the "exclusively informational" feature is seen to be.

8 Concluding remarks

We have coined MLIC (informational money-like commodity) as a preferred type indication (base type) for Bitcoin. We have compared this meta-type to several other candidates for a preferred base type for Bitcoin.

In [8] the notion of a conjectural ability has been promoted as a means to assess what a proposed theory might achieve in pragmatic terms. Viewing our typing of Bitcoin as a theory of Bitcoin, one may ask which conjectural abilities an appreciation of this theory may create. The ability that we assume to be created by an appreciation of this (fragment of) theory on Bitcoin is to allow for a systematic discussion of its development through all stages including an initial stage and a possible demise without being constrained by the implications of it being a money or a near-money.

References

[1] Elisabeth S. Anderson. Is women's labor a commodity? *Philosophy and Public Affairs,* 19 (1) pp. 71-92 (1990).

[2] Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating user privacy in Bitcoin. `in: Proc. 2012 ACM Conf. on Computer and Communications Security` (2012).

[3] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten Have a snack, pay with Bitcoins. *13th International Conference of Peer-to-Peer Networks,* (2013).

[4] 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).

[5] Jan A. Bergstra. Informaticology: combining computer science, data science, and fiction science. `arXiv:1210.6636 [cs.SE]` (2012).

[6] Jan A. Bergstra. Formaleuros, formalbitcoins, and virtual monies. `arxiv.org/abs/1008.0616v2 [cs.CY]` (2013).

[7] Jan A. Bergstra and Mark Burgess. A static theory of promises. `arXiv:0810.3294v4 [cs.MA]` (2013).

[8] J.A. Bergstra, G.P.A.J. Delen and S.F.M. van Vlijmen. Outsourcing Competence. `arXiv:1109.6536 [cs.OH]` (2011).

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

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

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

[12] 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).

[13] J. A. Bergstra and C. A. Middelburg. Instruction sequence expressions for the secure hash algorithm SHA-256. `http://arxiv.org/abs/1301.3297 [cs.PL]`, (2013).

[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] Ellen Detlefsen. User costs: information as a social good versus information as a commodity. *Government Publications Review*, 11, pp 385-394, (1984).

[17] Martin Doerr and Yannis Tzitzikas. Information carriers and identification of information objects: an ontological approach. arXiv preprint `arXiv:1201.0385 [cs.DL]`, (2012).

[18] Gerion Entrup. Bitcoin, Der Stärkere gewinnt. *Thesis Leibniz Universität Hannover, Institut für Theoretische Informatik,*
`http://www.thi.uni-hannover.de/fileadmin/forschung/arbeiten/entrup-ba.pdf`
(September 2013).

[19] Richard A. Epstein. Possession as the root of title. *Georgia Law Review.*, 13, 1221-1243 (1979).

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

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

[22] Jarek Gryz. Privacy as informational commodity. *Proc IACAP,* `philpapers.org`, (2013).

[23] John Frow. Information as gift and commodity. *New Left Review,* pp 89-108 (1996).

[24] Brian P. Hanley. The False Premises and Promises of Bitcoin. arXiv preprint `arXiv:1312.2048` (2013).

[25] Matthias Herrmann. Implementation, evaluation, and detection of a double-spend attack on Bitcoin. *MSc Thesis, ETH Zürich* (2012).

[26] O. W. Holmes Jr. Possession. *American Law Review,* 12 pp 688-720 (1877).

[27] Ian Horrocks, Peter F. Patel-Schneider, and Frank Van Harmelen. From SHIQ and RDF to OWL: The making of a web ontology language. *Web semantics: science, services and agents on the World Wide Web*, 1(1) pp 7-26, (2003),

[28] Danny Yuxing Huang. Profit-driven abuses of virtual currencies. `http://sysnet.ucsd.edu/ dhuang/pmwiki/uploads/Main/huang-research-exam.pdf` UCSD, (2013).

[29] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ECDSA). *IJCS*, 1,36–63 (2001).

[30] Nikolei M. Kaplanov. Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Temple University Legal Studies Research Paper* `http://ssrn.com/abstract=2115203` (2012)

[31] Gurcharan. S. Laumas. The degree of moneyness of savings deposits. *The American Economic Review*, 58 (3) part 1, pp 501-503 (1968).

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

[33] 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).

[34] Thomas W. Merrill. Property and the right to exclude. *Nebraska Law Review,* 77 pp 730-755 (1998).

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

[36] Raymond T. Nimmer and Patricia Ann Krauthaus. Information as a commodity: new imperatives of commercial law. *Law and Contemporary Problems*, 55 (3), pp. 103-130 (1992).

[37] Angela Rogojanu and Liana Badea. The issue of competing currencies. Case study–Bitcoin. *Theoretical and Applied Economics,* 21 (1) pp 103-114 (2014).

[38] Frank Snare. The concept of property. *American Philosophical Quarterly,* 9 (2) pp 200-206 (1972).

[39] Ian Steadman. Wary of Bitcoin? A guide to some other cryptocurrencies. `http://www.wired.co.uk/news/archive/2013-05/7/alternative-cryptocurrencies -guide/page/4` (2013).

[40] David I. Spivak and Robert E. Kent. Ologs: a categorical framework for knowledge representation. `arXiv:1102.1889 [cs.LO]` (2011).

[41] Mike Uschold, Martin King, Stuart Moralee, and Yannis Zorgios. The Enterprise Ontology. *The Knowledge Engineering Review,* 13 (1) pp 31-89 (1998).

[42] G. Llewellyn Watson and Jospeh P. Kopachevsky. Interpretations of tourism as a commodity. *Annals of Tourism Research,* 21 (3) pp. 643-660 (1994).

[43] Howard Williams. Kant's concept of property. *The Philosophical Quarterly,* 27 (106) pp 32-40 (1977).

Electronic Reports Series of section Theory of Computer Science

Within this series the following reports appeared.

[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/