EXIM: Exclusively Informational Money

Jan Bergstra, Minstroom Research, Utrecht
janaldertb@gmail.com

20 november 2026

1 Inleiding

In Bergstra & Weijland 2014 [17] hebben we Bitcoin omschreven als een money-like informational commodity. Sindsdien is heel wat geschreven over de vraag hoe en waarom zgn. cryptocurrencies als geld kunnen worden gezien maar ik meen dat de lijn gekozen in [17] nog steeds stand houdt.

In Bergstra & de Leeuw 2013 [10] wordt Bitcoin (BTC) gezien als een EXIM, een exclusively informational money. Dit gezichtspunt is inmiddels onverdedigbaar geworden, en was destijds misschien ook al minder plausibel dan wij toen dachten. De transparantie van de BTC blockchain, een feature that BTCvan meet af aan had, leidt er toe dat er een onderscheid is ontstaan tussen legale en niet-legale, of althans minder legale (Engels: taitned), BTC addressen en bijbehorende BTC volumes. Een gestolen volume kan worden gevolgd van adres naar adres en elke poging om dat volume wit te wassen langs gereguleerde kanalen kan worden getraceerd en desgewenst geblokkeerd. Zo'n blokkade kan al optreden bij een nog onbewezen vermoeden van digitale inbraak (dit volgens recente regelgeving in Zuid Korea). De idee achter een EXIM, namekijk dat beschikking de plaats inneemt van eigendom, kan daarmee voor BTC niet meer in volle algemeenheid worden gehandhaafd omdat de beschikking van een BTC volume verkregen door een formeel aangemelde digitale inbraak, of zelfs maar een vermoede digitale inbraak, in een ernstig beperkte mate van bruikbaarheid reulteert. Hiermee wordt complementair de beschikking over een volume aan BTC op een adres waarvan men de private key kent, mits rechtmatig (d.w.z. conform de op dat moment in een gegeven jursidictie geldige regels en binnen de geldige beperkingen) verkregen, beschermd op een wijze die niet bij een EXIM zou passen.

In Bergstra & Tucker 2026 [15] stellen we dat fraction ambigu is, en leveren we een reeks mogelijke betekenissen van fraction, elk van toepassing binnen elementair rekenen. Geld is vergelijkbaar in die zin dat er een bij geld van een continue schaal van legaliteit sprake kan zijn. Bij digital coins (Bitcoin, Monero/EMR, etc.) is er minstens sprake van twee posities op de schaal: legaal en problematisch (tainted). Daarme wordt b.v. BTC ambigu: bedoelt men gewoon (legaal) BTC of minder legaal (tainted) BTC? Illegale BTC kan men bijvoorbeeld verwerven door een atomic swap uit te voeren van XMR (Monero) naar

© J.A. Bergstra 2026 Licence CC BY-SA 4.0

BTC. Bij zo'n swap kan men opgezadeld worden met tainted BTC en daartegen is dan niet veel te doen omdat zulke transacties niet onder de gebruikelijke regelgeving vallen. De verkregen BTC is dan tainted omdat deze al tainted was, niet zozeer vanwege de aankoop via XMR, hoewel die transactie aan de betrouwbaarheid ook van de betreffende BTCook niet bijdraagt.

In deze tekst heb ik de volgende vier doelen:

(i) een bespreking van eerder werk met Karl de Leeuw en met Peter Weijland,

(ii) aangeven dat het werk met de Leeuw deels achterhaald is,

(iii) aangeven hoe het werk met de Leeuw eventueel weer up to date kan worden gemaakt, en

(iv) in zeer algemene termen aangeven hoe onderwerpen uit de hoe van programma's en algorithmen waar ik in de loop der jaren aan heb gewerkt relevant zouden kunnen zijn voor het bespreken van informational monies.

2 Exclusief informationeel geld (EXIM)

Exclusief informationeel geld, ofwel EXIM (voor exclusively informational money) is informationeel geld (IM) dat nog aan extra eisen voldoet.

Definitie 2.1. *Een EXIM is een informational money (IM) die de eigenschap heeft dat er ten aanzien van volumes in deze IM geen, door een buitenwereld in stand gehouden notie van eigendom (entitlement) bestaat die stricter is dan de facto beschikkingsmacht.*

De notie van een EXIM is zeker niet evident en is voor kritiek vatbaar. Hieronder geef ik nog een herformulering van de gedachte achter EXIM uit [10]. De idee is dat een EXIM een systeem S_{exim} omvat (een informational money, ofwel IM) dat geld en het gebruik en de circulatie daarvan reguleert op zodanige wijze dat alleen (de beschikking over) een qua vorm vaste maar overigens "betekenisloze" (doorgaans met pseudorandomgeneratie, of varianten daarvan, geconstrueerde informatiestructuur (d.w.z. de inhoud daarvan) houderschap/beschikkingsmacht en daarmee eigenaarschap aantoont. Geen enke andere instantie draagt bij aan de garantie van houderschap of eigenaarschap. Er mag ook geen partij zijn die als single point of failure het bestaan van S_{exim} functioneert.

Een bankrekening bij een bank die door alle relevante partijen erkend wordt is bevat geen EXIM omdat eigenaarschap indien nodig met persoonsidentificatie kan worden aangetoond. Een tegoed bij een bank dat men met een unieke code kan opvragen is om een andere reden geen volume van EXIM, namelijk omdat de betreffende bank als single point of failure kan optreden.

Inmiddels is, zoals hierboven gesteld, duidelijk dat Bitcoin ook geen EXIM is. Hiermee vervalt een belangrijke claim uit [10]. De bij een digitale inbraak ontvreemde volumens BTC waarvan de publieke adressen op de zwarte lijsten staan en waarvan transacties op alle denkbare manieren worden nagetrokken en door gereguleerde handelshuizen worden geblokkeerd vormen mogelijk een deel van Bitcoin, zeg $\mathrm{BTC}_{\mathsf{tainted}}$, dat men als een EXIM zou kunnen opvatten.

Maar dan is de definitie van het systeem in kwestie toch erg onduidelijk. In de praktijk zijn veel volumes aan BTC transparant in de blockchain opgenomen zodat vaststellen van eigenaarschap ook zonder het laten zien of gebruiken van een private key (door de vermeende eigenaar) mogelijk is, dit dan met allerlei log files en historische data, waarbij een vast formaat ontbreekt. Daarmee ontstaat hoe dan ook een aanzienlijke afstand van de idee van een EXIM.

Nu is er naast Bitcoin nog veel te beleven in de wereld van informational monies en de vraag dient zich dan aan of alternativen voor Bitcoin wel de status van een EXIM kan worden toegekend. In deze bijdrage bespreek ik argumenten voor en tegen volgende claim.

Claim 2.1. *Monero (XMR) is een EXIM.*

Op dit moment meen ik dat Claim 2.1 aannemelijk is. Qua techniek is Monero nog niet perfect en een zekere mate van tracking van transacties is nog steeds mogelijk, iets wat toekomstige doorontwikkeling toenemend onmogelijk zal maken. Qua techniek is het ontraceerbaar gebruik van Monero ook een uitdaging die mogelijk beter ontwikkeld moet worden. Maar Monero is in elk geval een zodanig goede benadering van een EXIM dat in beginsel de mogelijkheid van zo'n IM als bevestigd kan worden gezien, qua design en ontwerpdoelstelling is Monero een EXIM, qua uitwerking mogelijk nog niet perfect. Dat toont dan aan dat EXIM's bestaan, maar zegt nog niet veel over de levensvatbaarheid van een EXIM. Monero is een zgn. privacy coin en dat betekent in de praktijk dat het traceren van een sequentie van opeenvolgende betalingen vijwel onmogelijk is, maar tegelijk levert die praktijk een reeks van complicaties op die het dagelijks gebruik van Monero, in vergelijking met Bitcoin formidabel compliceren. Monero is een privacy coin in sterke zin, privacy is geen add on feature maar is bij all transacties gegarandeerd. Wil men transparant zijn over het gebruik van Monero dan moet men dat buiten het de utilities van Monero om bereiken, en zelfs dat is niet zo eenvoudig.

Wie met Monero anoniem wil betalen staat desondanks voor een uitdaging. Zo'n betaling kan bij de huidge regelgeving in veel landen en blokken van landen niet meer via een gereguleerde beurs of transactieplatform verlopen. In de plaats daarvan komen zgn. atomic swaps, of de aankoop van tegoedbonnen voor kleine bedragen, en komt men qua techniek toch in handen van tussenpersonen (of intermediaire software agents), die men bij toepassing van zulke swaps wel enigzins moet vertrouwen. Bovendien moet men zorgen dat de eigen identiteit ook niet voor buitenstaanders zichtbaar wordt meegenomen als neveneffect van de gebruikte technologie waarmee men de wallet die de betreffende Monero volumes kan bevatten installeert en gebruikt.

3 Ethische vragen

Nu wel enigszins scherp hebben wat een EXIM is of kan zijn, en met Monero een nieuwe kandidaat voor deze status ook hebben (waarmee met mogelijk wordt

om [10] weer up to date te maken door daarin Bitcoin door Monero te vervangen, dan dient zich direct een veelheid aan vragen aan:

Vragen 3.1. *(i) Het ligt voor de hand dat een EXIM, zeg* IM_{exim} *zich kan lenen voor illegale transacties (of wel transacties in de context van illegale activiteiten vanuit het perspectief van een gegeven jurisdictie). Moeten we alleen al om die reden verwachten dat* IM_{exim} *in iedere jurisdictie als problmatisch wordt gezien.*

(ii) Als het zo zou zijn dat IM_{exim} *in elke jurisdictie als onwenselijk wordt gezien, volgt daar dan uit dat gebruik van* IM_{exim} *ook in meer algemene en absolute zin onwenselijk is?*

(iii) Of mogen we omgekeerd constateren dat juist vanwege de mismatch met iedere individuele jurisdictie, het bestaan van een EXIM ook een rechtvaardiging heeft, namelijk in de het perspectief van persistentie door volstrekt diametrale jurisdicties. Bezien vanuit jurisdictie A is het tenslotte niet zondermeer wenselijk dat in jurisdictie B niet kan wat dar niet mag. Ofwel kan het vanuit jurisdictie A wenselijk zijn dat IM_{exim} *binnen jurisdictie B sommige partijen de mogelijkheid biedt om illegaal (in de zin van B) te betalen?*

(iv) Kortom: is het ethisch gesproken (en daarmee niet vauit enige specifieke jurisdictie bezien) wenselijk of onwenselijk dat IM_{exim} *bestaat en wordt doorontwikkeld.*

(v) Met als afgeleide vraag: is het ethisch gesproken wenselijk of onwenselijk dat Monero bestaat en wordt doorontwikkeld.

Ik zie de antwoorden op de verschillende vragen hierboven als volgt (i): JA, (ii): NEE, (iii): JA, (iv): JA en (v): JA. De argumentatie bij (ii) lijkt op het fenomeen terrorisme: all jurisdicties zijn daartegen. Maar vanuit jurisdictie A kan wat men in jurisdictie B als terrorisme ziet juist "gerechtvaardigde strijd zijjn". De volgende claim volgt dan uit het combineren van deze antwoorden op (ii) en (iii).

Claim 3.1. *(Interjurisdictie paradox) een gedrag, entiteit of handelingsoptie welke in elke afzonderlijke jurisdictie ethisch onwenselijk is, hoeft niet noodzakelijk categorisch (d.w.z. vanuit een standpunt "boven" specifieke jurisdicties) onwenselijk (en daarmee onethisch) te zijn.*

Ik neem hierbij aan dat de verschillen in opvatting tussen onderscheiden jurisdicties zo groot kunnen zijn dat (a) het vanuit jurisdictie A van belang kan zijn dat het binnen jurisdictie B mogelijk blijft om buiten het zicht van de overheid (in B) om transacties te doen en money-like commodity te verplaatsen, en (b) men, om die reden, vanuit A het risico wil lopen dat een EXIM, zeg $\mathrm{IM}_{\mathsf{exim}}$, ook binnen A wordt gebruikt voor doelen die binnen A onwenselijk worden geacht.

Vraag 3.1. *Als een EXIM, zeg* IM_{exim} *in alle jurisdicties een probleem heeft, is deze dan niet meer levensvatbaar?*

Met andere woorden, en dan concreet voor Monero, is de wereldwijde problematiek rond Monero een indicatie dat deze EXIM op omvallen staat, of juist

niet. Dwingt deze wereldwijde politieke druk Monero tot technische versterking die uiteindelijk de levensvatbaarheid gaat vergroten, of juist niet. In het laatste geval kan men nog twee mogelijkheden onderscheiden: gaat de motivatie om de EXIM te versterken aan externe druk ten onder, of is ook met zulke versterking de externe druk op het gebruik van de (vebeterde EXIM) niet te weerstaan.

4 Meer over EXIM's

Er zijn verschillende implicaties van de notie van een EXIM,daarover het volgende:

1. Een EXIM kan geen stablecoin zijn. Want het is niet redelijk om te verwachten dat in een jurisdictie die het gebruik van de EXIM probeert terug te dringen enige partij de conversie naar gewoon geld garandeert (regelgeving zit dan in de weg).

   Vraag 4.1. *Kun je een stablecoin op basis van Monero maken? Misschien wel, maar dat is dan geen EXIM maar een soort tussenproduct dat niet alleen Monero's technologie gebruikt, maar ook de XMR-blochcain als primaire drager van IM-volumes gebruikt.*

   Het ligt niet voor de hand dat zoiets ontstaat want regulering zal het verhinderen, al dan niet in combinate met onaantrekkelijke fiscale behandeling van inwisseling van de EXIM volumes voor eem andere maar traceerbare traceerbare stablecoin. Er wordt op dit vlak veel geprobeerd zie b.v. de toelichting op de ZanoX site (URL, inspected 15-11-2026).

2. We spreken van een EXIM volume: een hoeveelheid van eenheden van een gegeven EXIM; men kan de beschikking hebben over een zeker EXIM volume, dan heeft men noodzakelijk ook de beschikking over lagere EXIM volumes (bij dezelfde EXIM).

3. Essentieel aan de EXIM is dat je aan het volume niet kunt zien waar het vandaan komt.

4. Beschikking in de plaats van bezit. Het is onpraktisch om over bezit van een een EXIM volume te spreken, de betere term is beschikking (Engels control, holding).

5. Het is onredelijk om belasting te heffen over beschikking over een EXIM volume omdat die beschikking en de duur daarvan niet of nauwelijks aantoonbaar is.

6. Het lijkt redelijk om belasting te heffen bij de conversie van EXIM naar een gewoon geld of goederen dan wel diensten waarvan de waarde in "gewoon" geld, of enige non EXIM IM uitdrukbaar is. Dit betreft dan conceptueel een vermogensbelasting die idealiter evenredig is met de duur van de beschikking over het betreffende EXIM volume.

Het wordt dan een additionele eis aan een EXIM dat die duur transparant is, maar dat is bij Monero niet het geval, zodat alleen de formule van een nogal willekeurig vast te stellen belasting bij verkoop overblijft.

7. Gezien de complicaties van belastingheffing over EXIM transacties lijkt het denkbaar om een EXIM een speciale status te geven en EXIM transacties (en beschikking) belastingvrij te doen zijn. Tegelijk wordt het gebruik van de EXIM op vele wijzen tegengewerkt. Gebruikt men een EXIM voor aankoop als consument dan is al sprake van belastingbetaling via mechanismen als BTW.

8. Het is conceptueel onmogelijk dat een EXIM volume wordt gestolen, wat wel kan gebeuren is daar men de beschikking verliest zonder dat daar enig vooreel tegenover staat en complementair dat men de beschikking verkrijgt zonder daarvan verder groot nadeel te ondervinden (b.v. door te betalen in e.o.a. vorm).

   De situatie ligt bij BTC anders, maar hoe anders is nog een vraag:

   Vraag 4.2. *Is er bij Bitcoin sprake van bezit/eigendom naast beschikking. Als alle transacties "wit" zijn geweest en belastingen betaald zijn (maar at is niet te zien), dan is bezit misschien een goede term. Er is sprake van een overgang waarbij de door een digitale inbraak verkregen BTC uitsluitend beschikking betreft en in gunstige gevallen sprake is van bezit, hoewel dat bezit niet met 100% garanties gedekt wordt.*

5 Verbindingen met "programma's en algorithmen"

We bekijken een EXIM, zeg $\mathrm{IM}_{\mathsf{exim}}$. Er is sprake van een community van ontwikkelaars van $\mathrm{IM}_{\mathsf{exim}}$ die stappen zet voor de ontwikkeling van de clients voor opeenvolgende releases van $\mathrm{IM}_{\mathsf{exim}}$. Deze client software komt in twee delen: mining clients en wallet clients. De mining client draagt zorg voor het voortbestaan van het systeem, de wallet clients faciliteren het gebruik van het systeem. Beide kan een deelnemer draaien, zij het dat een miner (knoop die mining client draait) ook een wallet nodig heeft.

De mining clients hanteren een pseudogerepliceerde (alle clients hebben een instantie van de datastructuur, vaak genoemd de $\mathrm{IM}_{\mathsf{exim}}$-blockchain en deze instanties zijn op elk moment bijna gelijk), en op termijn convergeren deze datastructuren (in een passende topologie/metriek) naar dezelfde oneindige (maar nooit bereikte) instantie. Deze instanties beschrijven elk de transactiegeschiedenis van $\mathrm{IM}_{\mathsf{exim}}$ en wel vanaf het begin van dat systeem, met kleine verschillen inzake de beschrijving van de meest recente transacties. Deze convergentie treedt niet met 100% zekerheid op maar is wel heel waarschijnlijk gezien het ontwerp van de verschillende clients. De datastructuur in de limiet, niet noodzakelijk een berekenbare structuur, beschrijft het totaal van de transacties. Dit is een hypothetische notie, want deze limiet wordt nooit bereikt.

5.1 Abstracte datatypen

De IM_{exim}-blockchain is een realisatie van een ADT (abstract datatype), ofwel een isomorfieklasse van een gegven datastructuur, bestaande uit wiskundig te noteren domeinen met een reeks van totale (dwz. overal gedefiniëerde) operaties daarop. Wallets werken niet met de IM_{exim}-blockchain (waarbij een blok een reeks van uitgevoerde dan wel beoogde transacties beschrijft, en de chain deze tot een geheel integreert) maar met veel kleinere instanties van datatstructuren die communicatie over de blockchain mogelijk maken. Er is dus ook sprake van een interactiedatatype dat de verschillende data beschrijft die clients onderling kunnen uitwisselen, iets wat met de gehele blockchain doorgaans niet gebeurt. Er ontstaan bij de informele uitleg ellerlei noties die ook informeel vastlegging vergen:

(i) Een grootboek datatype (vaak genoemd de IM-blockchain voor het grootboek datatype behorende bij informational money IM), met als implementaties dynamische datastructuren, waarvan mining clients (programma's onde beheer van clients) instanties beheren die pseudogerepliceerd zijn, en die in de reeks van transacties met grote kans langzaam convergeren naar eenzelfde oneindige datastructuur. Specificatie van abstracte datatypen (ADT's) was mijn onderwerp van 1977 tot 1983 en inmiddels weer maar dan met een focus op datatypen die men in het elementaire rekenen tegenkomt, zie b.v. [5, 4, 9, 13, 16]. Rekenwerk in en aan een IM kan met en in de common meadow van decimale rationale getallen. Common meadows worden precies beschreven in [14].

(ii) Wallets (wallet clients), in essentie ook een ADT, die gebruikerspecifieke instanties hebben, die een rol spelen bij het gebruik van een IM.

(iii) een IM-interactie datatype, dat de berichten beschrijft waarmee al deze clients via het internet of een communicatie laag op het internet zoals TOR met elkaar communiceren.

Bovengenoemde systemen kunnen ook gezien worden in het licht van de relatief moderne notie van een app: een programma, dat (i) in kopie aanwezig is op een veelheid van hosts (ik noem die kopie op een enkele host een instantie), (ii) een proces realiseert dat gaandeweg data verzamelt die samenhangen met de specifieke instantie, (iii) vaak met een korte en duidelijke naam wordt benoemd die primair staat voor de evaring van de individuele gebruiker met de instanties op een of meer hosts die deze instanties gebruiken, (iv) onderhouden wordt door een team, al dan niet anoniem, dat met enige regelmaat nieuwe releases van het programma verspreidt.

Procesalgebra ([8] levert één van de vele technieken die men kan gebruiken om de interactie te beschrijven tussen de verschillende clients die gelijktijdg binnen een netwerk actief zijn. Maar zulke toepassingen spreken niet vanzelf en zijn gezien de omvang van de relevante programma's alleen mogelijk met gebruik van ondersteunende hupmiddelen zoals mCRL2 (URL).

5.2 Programma, algorithme en algorhyme

De operaties op de verschillende datastructure worden (informeel!) gegeven door algorithmen, die ik conform [3] zie als eindige collecties van algorhymes (ofwel pseudocodes met uitleg/explanation als doel), al dan niet in combinatie met een informele uitleg over de doelen die men met deze algorithmen wil bereiken (de functionele specificaties ervan).

Een algorhyme is een implementaties van een algorithm en is daarmee een programma's in een passende programmanotatie. Ik heb rond 2000 geprobeerd om een betekenis toe te kennen aan het concept computerprogramma. Hierbij was steeds mijn probleem dat concrete programma's in bestaande talen zo technisch en specifiek zijn dat de gedachte er achter nauwelijks meer te formuleren is, en dat dit probleem er wat mij betreft ook in educatieve pseudocodes nog steeds is. De fameuze while programma's zijn een voorbeeld van een begrijpelijke pseudocode maar daarmee is weer de vraag wat nu in essentie ee programma kan zijn, je komt dan uit op: net zoiets als een while programma maar dan misschien ingewikkelder. De programmalagebra PGA uit [12] is bedoeld als een mogelijke oplossing voor zulke vragen. In PGA is er de notie van een programmaobject, dat is mogelijk een oneindige reeks van instructies, en is een programma een tekst waarvan de betekenis wordt gegeven door vertaling naar zo'n programmaobject.

5.3 Globale uitleg van Bitcoin

Vraag 1.2.2 uit [11] betreft het geven van een abstracte technische uitleg van Bitcoin. Die vraag is naar mijn overtuiging nog steeds open. En toepassing van datatypen, procesalgebra en programma algebra of vergelijkbare methoden kan daarbij misschien van nut zijn. Een aanpak in die richting vindt men in [18] en [1] en in de daargenoemde verwwijzingen naar vergelijkbaar werk. Een overeenkomstige vraag speelt bij Monero en bij elke andere IM.

Referenties

[1] Fahad F. Alhabardi et. al. Verification of Bitcoin Script in Agda using Weakest Preconditions for Access Control. arXiv.2203.03054v3 [cs.SC], DOI (2022).

[2] Jan Bergstra. Zijn er natuurlijke getallen? over decimale natuurlijke getallen. Minstroom Research website, URL, (2026).

[3] J.A. Bergstra. Defects and Faults in Algorithms, Programs and Instruction Sequences. Transmathematica), DOI, (2022).

[4] J.A. Bergstra. Adams conditioning and likelihood ratio transfer mediated inference. *Scientific Annals of Computer Science*, 29 (1), 1–58, (2019).

[5] J.A. Bergstra. Arithmetical datatypes, fracterms, and the fraction definition problem. *Transmathematica*, 2020. DOI.

[6] J. A. Bergstra. Errors, Failures, and Faults in the Context of Elementary Arithmetic. *Transmathematica*, 2024. DOI.

[7] J. A. Bergstra. Shapes for naturals, integers and rationals. Submitted to Transmathematica, *Transmathematica*, 2026. (forthcoming).

[8] J. A. Bergstra and J. W. Klop. Process algebra for synchronous communication. *Information & Control*, 60 (1-3), 109-137 (1984).

[9] J. A. Bergstra, I. Bethke, and A. Ponse. Equations for formally real meadows. *Journal of Applied Logic*, 13(2): 1–23, (2015).

[10] Jan A. Bergstra and Karl M. de Leeuw. Bitcoin and Beyond: .Exclusively Informational Monies. arXiv:1304.4758v3 [cs.CY], DOI, (2013).

[11] Jan A. Bergstra and Karl M. de Leeuw. Questions related to Bitcoin and other informational money. arXiv:1305.5956v2 [cs.CY], DOI (2013).

[12] J.A. Bergstra and M. E. Loots. Program ALgebra for Sequential Code. *J. Logica and Algebraic Methods in Programming*, Vol. 51 (2), 125-156 (2002).

[13] J.A. Bergstra and J.V. Tucker. Equational specifications, complete term rewriting systems, and computable and semicomputable algebras. *Journal of the ACM*, Vol. 42 (6), 1194-1230 (1995).

[14] J.A. Bergstra and J.V. Tucker. Rings with common division, common meadows and their equational theories. *Journal of Symbolic Logic*. Published online 2024:1-27. DOI, (2024).

[15] J.A. Bergstra and J.V. Tucker. On Ambiguity: The case of fraction, its meanings and roles. arXiv 2604.04647 URL, (2026).

[16] J.A. Bergstra and J.V. Tucker. The rational numbers as an abstract data type. *Journal of the ACM*, 54 (2), Article 7, (2007).

[17] Jan A. Bergstra and Peter Weijland. Bitcoin and Beyond: Exclusively Informational Monies. or arXiv:1304.4758v3 [cs.CY], DOI, (2013).

[18] Anton Setzer. Modelling Bitcoin in Agda. CoRR, abs/1804.06398, 2018. URL: URL. (2018).