The identity, fungibility, and anonymity of money

Author 1 and Author 2[1]

This version 7 June 2018

Abstract: Participants to exchange have identities, as do the goods and services being exchanged. The identity of the medium of exchange is increasingly important as the use of cash becomes less common, and regulated industries require more information about the provenance of the money they receive. Cryptocurrencies, including bitcoin, are themselves subject to tracking, as the distributed ledger on which they are transacted provides a method to track individual transactions back to users. 'Privacy coins' are one attempt by users of cryptocurrencies to develop a currency which is truly private, and completely fungible. Different money technologies provide varied levels of privacy, and cryptocurrencies which utilise technologies such as zero-knowledge proofs offer possibilities for users to choose the level of information they choose to share when they transact.

1. Introduction

Identity is a crucial component of any economic exchange (Berg et al. 2018). The participants in an exchange have identities, the good and services being exchanged have identities, and the medium of exchange they use to affect their exchange has an identity (or identities). This paper looks at the identity of money in its various technological guises, examining fiat cash, cryptocurrencies, and cryptocurrencies with privacy features. We claim that the level of fungibility associated with the type of money used in exchange is closely related to the anonymity it provides; a highly fungible form of currency provides a high level of anonymity to the user, and vice versa.

Fungibility is a characteristic long associated with cash, however human behavioural practices, as well as regulatory impositions, sees the substitution of money becoming increasingly imperfect. While the relative anonymity of cash suggests it is largely interchangeable with other units of the same nominal value, money of all types which interact with regulated industries are increasingly examined for their use in criminal and other illicit activity. This increased examination and regulatory imposition results in circumstances where money believed 'tainted' by criminal enterprise is not accepted by the receiver – regardless of any actual criminality or

[1] Author 1 and Author 2 affiliation

malfeasance. More recent innovations in money technologies, such as the cryptocurrency bitcoin, have characteristics of fungibility and anonymity, but units are not completely interchangeable, nor do they allow for completely anonymous transactions. The development of 'privacy coins', cryptocurrencies which aim to allow users to transact with more complete anonymity, may be some of the first truly fungible currency.

Section 2 examines some of the economics of money identities, including the historical precedent for the general fungibility of physical cash. Section 3 describes how human behaviour and regulation shape the fungibility of money. Section 4 describes the fungibility of various types of cryptocurrencies, and how technology can provide privacy protections for users. Section 5 concludes.

2. The economics of money identities

Understanding the identity of the counterparty to a transaction, that which is traded, as well as the medium of exchange used to settle that transaction is a prerequisite to most exchange. Working in the transaction costs school (à la Coase 1937, 1960, Williamson 1979, 1985) we have developed a transaction cost theory of identity (see Berg et al. 2018). This theory determines that for commercial - and often regulatory – reasons, parties to an exchange can incur significant identity costs during the course of business. Commercially derived identity costs can be exemplified by the need for financial institutions to understand a borrower's willingness and ability to repay according to a loan schedule: these commercial reasons demand that these firms understand a borrower's income, wealth, credit history and other identity attributes. Similarly, regulatory derived identity costs manifest in Know Your Customer (KYC) requirements, which can themselves be significant: these regulatory requirements mandate financial institutions establish the identity of their customers – and monitor their activity on an ongoing basis – often at great expense. We also determine that the existence of firms such as financial institutions can in part be explained through identity cost economising (see Berg et al. 2018).

Berg et al. (2018) examined the identity of counterparties to exchange, as well as the identity of the good or service being exchanged. The identity of the medium of exchange used as part of a transaction was not examined, in part due to the fungibility generally associated with fiat currency. Fiat currency – and particularly banknotes as we shall see – are to a large extent fungible. The fungibility of banknotes – their homogeneity, or the characteristic of being interchangeable with others of equal denomination - was determined through common law in 18th century Scotland (see Reid 2013). In 1749, a court considered the case of two £20 notes which had gone missing in the post, and examined the ownership of one of those notes which had subsequently turned up at a branch of the Royal Bank of Scotland - identified courtesy of the serial number recorded by the sender. The case determined that one who took possession of a banknote in the course of normal and legal exchange was free from the "infirmities of title which affected those from whom it had been acquired" (Reid 2013, 3). In general, this means

that the history of an individual banknote – which we analogise to its identity - is largely irrelevant to a transaction according to this 18th century case law. More contemporary legislative and regulatory requirements have challenged this precedent; global anti-money laundering efforts and efforts by taxation authorities to maintain revenues have seen that the history of fiat currency – its identity - is relevant to legal exchange, hence the precedent of fungibility established in 1749 has been challenged (see Section 3).

We determine that coming to a level of assurance over the identity of the medium of exchange incurs identity costs, as the recipient has a commercial imperative to ensure that he or she can subsequently use that medium of exchange in future transactions, and be confident that the value associated with it can be maintained. Regulatory obligations can also provide an imperative for recipients of all forms of currency to have an understanding of the history of what they receive – where they must take steps to ensure that it has not been associated with criminal activity and so forth.

Merchants have an overriding desire to ensure that they can derive future value from what they receive in commerce; the currency they receive must be able to be used to pay expenses, as well as be drawn down in the form of profits. A transaction using some form of currency consists of an *ex ante* promise that a nominal amount of currency might be realised *ex post* in some future transaction by the merchant or other recipient. This is analogous to fungibility. Merchants and other recipients of currency will take steps to 'screen' the currency and detect counterfeit money, and potentially discover past instances of illicit activity associated with it; this screening aims to reduce the information asymmetry between the two parties, and can be aided by security features that are present on modern bank notes, as well as by examining the publically auditable and distributed ledger which some currencies are transacted on (see Section 4).

3. Fungibility, human behaviour and regulatory action

Fungibility is the property of being essentially interchangeable. Money is frequently described as fungible as in principle one $10 note is perfectly substitutable for another $10 note; rational individuals offered the exchange (costlessly) of one note for another of equal nominal value should be indifferent as to whether to make the exchange. Fungibility is a key assumption behind much economic analysis that seeks to analyse utilities and disutilities. However, sociologists have drawn attention to a variety of human practices that reduce the fungibility of money. For example, using money for gift giving is seen as impersonal, and gift-givers often 'earmark' money by converting it into a gift certificate for a particular store or category of good (Carruthers 2010). Households frequently collect income into 'buckets', depending on its source, dedicated for certain categories of expenditure (Zelizer 1997). Organisations also categorise and earmark funds to pay particular creditors and to finance particular projects. In a university environment grant money is cordoned off for the duration of a project. Governments frequently earmark funds. Behavioural economists have likewise emphasised how economic agents have

mental accounts and use heuristics about income and wealth that reduce fungibility (Sahm, Shapiro, and Slemrod 2010, Thaler 1990).

Leiser and Shemesh (2018, 108) argue that money "implicates a nexus of attitudes, emotions and confused knowledge", attributable to the origins of money and the medium in which it is held. Strategic and behavioural approaches deployed give otherwise fungible money an *identity*. The purposes of that identification can vary. Dividing money at the household level is a strategy for self-control. Regulatory requirements and other conditions placed on income and financial institutions may demand earmarking. Human sociability (in the case of gift cards) also gives money an identity that reduces its fungibility. Converting money into non-money 'scrip' encourages spending – the psychological distance between (for instance) casino chips and 'real' money seems to encourage gamblers to spend more on gambling (Raghubir and Srivastava 2008). Fungibility is not a binary attribute. Even relatively anonymous cash is not perfectly fungible: serial numbers, markings, and other distinct physical features of individual notes give those notes an identity. Commemorative coins are often put into circulation. Earmarked funds kept in one account can be switched with funds kept in another.

Apart from these strategic and behavioural practices, efforts by financial and other authorities also effect the fungibility of money. Since the 1970s global authorities have introduced compliance measures to combat money laundering, as well as counter the funding of terror organisations. The 1970 Bank Secrecy Act in the United States focused on stamping out domestic money laundering, while in the 1980s concern about international drug trafficking led to the creation of the international Financial Action Task Force (FATF) to combat the misuse of the financial system on a global scale. Following the September 11 attacks in 2001, FATF further expanded its remit to provide recommendations to combat terror financing (Stanley and Buckley 2016). A number of FATF recommendations have been incorporated into the Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Stanley and Buckley 2016). This legislation imposes compliance requirements, including for regulated organisations to monitor and keep records of transactions, as well as notify authorities of 'threshold transactions' (Department of Home Affairs n.d.-a). Such legislation creates a regulatory requirement for entities such as financial institutions to report transactions considered suspicious from the perspective of money laundering or terrorism financing.

Such efforts mean that the identity – and by extension the history – of money which is transacted as part of exchange is now part of the regulatory system of those jurisdictions like Australia which maintain Anti-Money Laundering (AML) regimes. For instance, advice given to Australian entities explicitly asks financial institutions to review sources of income in determining whether or not to report a customer to the Australian Transaction Reports and Analysis Centre (AUSTRAC) (Department of Home Affairs n.d.-b). This has even seen financial institutions exit entire markets which they see as too risky, and where they feel they are unable

to adequately evaluate sources of money which their customers wish to transact. For instance, large sections of international payment corridors have been closed due to concerns about complying with AML standards (Durner and Shetret 2015). In addition to AML requirements, efforts to maintain taxation revenue, have seen the fungibility of fiat currency weakened.

The use of physical cash in transactions has been criticised as a means of enabling illegal activities including illegal drug sales, the facilitation of bribery, as well as tax avoidance. Such sentiments have resulted in a challenge to the fungibility of money. Rogoff (2016) argues that there are few legitimate reasons for the use of physical cash, particularly large denomination bills. Governments around the world have taken a similar stance, with the European Commission opening public debate on the use of physical cash as a medium of exchange for reasons which mirror Rogoff (see Passas 2018). Such sentiment has been echoed by the Australian government, where the 2018-19 Federal Budget was used to announce a prohibition on the use of cash for payments to businesses over $10,000 from 1 July 2019 (Commonwealth of Australia 2018). Such a prohibition fundamentally alters the fungibility of cash from the perspective of those who hold it (or wish to receive it); the 10,001st dollar is not equivalent to the 10,000th.

Thus, while fungibility is still associated with cash and indeed money in general, the way in which it is truly interchangeable is reduced by both human behavioural traits as well as regulatory action. Behaviours of 'earmarking', and the collection of income into various 'buckets', means that individuals do not treat their units of liquid wealth as interchangeable and homogenous. Similarly, regulatory action demands regulated industries increasingly understand the provenance of the money they interact with, reducing its fungibility for those industries, as well as their customers.

4. Fungibility as a privacy technology

Cryptocurrencies, including bitcoin, have been described as a tool which may enable illegal activity, as they offer a "venue for individuals to generate, transfer, launder and steal illicit funds with some anonymity" (Federal Bureau of Investigation 2012). A number of studies have examined the role of cryptocurrencies in criminal activities, including in; money laundering and tax evasion (Gruber 2013); child pornography, assassination markets and the international drug trade (Trautman 2013); as well as terror financing (Cockfield 2016). The perceived anonymity of cryptocurrencies is what these studies cite as an enabling factor in facilitating crime (Cockfield 2016, Gruber 2013, Trautman 2013). Such studies echo Rogoff (2016) and his criticism of cash – the anonymity of physical cash and the difficulty in tracing its provenance enable criminal enterprise.

Bitcoin, the first and still the most popular of this new class of cryptocurrencies, was first announced in late 2008 as a "peer-to-peer version of electronic cash" (Nakamoto 2008, 1). It allows for the transfer of value across the internet without the use of a financial intermediary or

central bank. Having since inspired upwards of 1,600 other cryptocurrencies at the time of writing (see CoinMarketCap 2018), bitcoin introduced the technology known as 'blockchain', itself the consolidation and application of numerous other technologies and techniques including peer-to-peer networking, asymmetric (public-key) cryptography, consensus algorithms and game theory. In general, bitcoin solved the 'double-spend' problem by creating a publically auditable, immutable ledger which is maintained by a network of users and across which bitcoin are transacted (see Antonopoulos 2017, Narayanan et al. 2016, Swan 2015). This peer-to-peer network is a protocol which prevents users from double spending – where a user might spend the same coin in multiple transactions – without the need for a centralised body to maintain records of users' balances. However, the very nature of this new form of decentralised currency, and the way in which it solves the double-spend problem, provides a record of every bitcoin ever created and transacted, their history, and by extension the address which holds them.

The nature of public blockchains like bitcoin mean that transactions are public; transactions can be viewed by anyone with an internet connection. Bitcoin uses asymmetric (public-key) cryptography to allow users to generate transactions and receive payments. A private key allows a user to prove ownership, and transact, bitcoin that a user owns, and the public key, mathematically related to the private key, generates a 'pseudonymous' address into which a user can receive payments (Antonopoulos 2017). These addresses provide some level of anonymity, as they consist of a (usually) 34-alphanumeric string in Base58 notation[2]. Users are also able to create multiple addresses as they transact, which may aid in user anonymity (Antonopoulos 2017). These addresses are considered pseudonymous as they can provide a certain level of anonymity for the user due to their non-human readable format. For instance, the address below dates from January 3, 2009, and this address received the 'coinbase' transaction of the so-called Genesis block[3] – the very first transaction on the bitcoin network.

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

These pseudonymous addresses, such as the one above, do not in fact provide an absolute level of anonymity, and there are a number of techniques that can be used to identify the owner of such an address. Web (HTTP) cookies (Goldfeder et al. 2017), IP addresses (Koshy, Koshy, and McDaniel 2014), clustering techniques – where a number of bitcoin addresses can be identified

[2] Base58 notation consists of almost all upper-case letters, lower-case letters and numeric digits. In order to prevent confusion, upper-case 'I', lower-case 'l', upper-case 'O' and the digit '0' are excluded due to their similarity to the human eye (see Narayanan et al. 2016).

[3] The 'coinbase' transaction is a special type of transaction on the bitcoin network, and consists of new bitcoin created as part of the mining (block creation) process. When the software was released in 2009 the coinbase transaction consisted of 50 bitcoin, while this amount halves approximately every 4 years (Antonopoulos 2017). The Genesis block was the first block mined in 2009, and this block received the very first coinbase transaction (see Narayanan et al. 2016).

as being controlled by a particular user - (Meiklejohn et al. 2013), information provided by users to cryptocurrency exchanges when they sign up (Reynolds and Irwin 2017), as well as the public disclosure of addresses on social media (Reid and Harrigan 2013), are all ways in which addresses can be traced back to their owner. For instance, law enforcement agencies have been able to trace transactions as part of investigations into illicit activity; during investigations into the Silk Road Marketplace – the online marketplace where users could purchase illicit drugs and other goods using bitcoin – the FBI were able to track the provenance of over 700,000 bitcoin and connect individuals to illegal activities (Greenberg 2015). And while there are a number of techniques available which can make it more difficult to trace an individual back to an address (see Goldfeder et al. 2017, Narayanan et al. 2016, Reynolds and Irwin 2017), the publically auditable nature of blockchains such as the bitcoin ledger provide an opportunity to trace transactions back to individuals.

The public, and therefore traceable, nature of these transactions has resulted in some instances where these new digital currencies are not treated as fungible; based on their history, individual 'coins' may not be accepted as part of a transaction. Instances of discrimination towards bitcoin which have been associated with illicit activity indicates that individual units of the digital currency are not treated equally. Coinbase, one of the largest cryptocurrency exchanges, has reportedly refused to accept bitcoin which are known to be stolen, or have been involved in illegal activity (Vorick 2018). Similarly, the sale of seized cryptocurrency by law enforcement agencies (see Aitken 2018) raises the prospect for bitcoin sold in such a manner to be 'cleaned', and given a stamp of legitimacy. Indeed 144,000 seized bitcoins auctioned off by the FBI received a higher price than those trading on cryptocurrency exchanges, suggesting users were in fact placing a higher value on units which had been cleaned by such a process (Casey and Vigna 2018).

These characteristics have led to the development of new types of 'privacy coins. Privacy coins are one such attempt to create cryptocurrencies which eliminate the ability for other users to associate transactions with individuals and their activities. For instance, the Zcash cryptocurrency, a 'fork' of bitcoin[4], can be used to create 'shielded' transactions. These shielded transactions aim to dissociate the sender and the receiver in an exchange (Kappos et al. 2018), as well as obfuscate the amount being sent, through the use of zero-knowledge-proofs (Quesnelle 2017). Zcash achieves this level of anonymity through the use of a technique known as zero-

[4] Bitcoin, and many other cryptocurrency and blockchain protocols are open-source software. This enables users to copy the software on which these cryptocurrencies run, change some aspect of it, and release it as what is in some cases called an 'alt-coin'. In the case of bitcoin, different 'forks' of the protocol have changed the block size and hence increased transaction speeds, changed the maximum number of coins, or in the cash of Zcash, provided a way in which details of transactions can be kept private (see Berg and Berg 2017).

knowledge succinct non-interactive arguments of knowledge (zk-SNARKS), a type of zero-knowledge proof (Quesnelle 2017). Such a technique, a type first developed by Goldwasser, Micali, and Rackoff (1989), allows a user to prove that they know something, X, without revealing anything else apart from the fact that they know X. In the context of exchange, this allows users to prove they are the rightful owner of an amount of Zcash – and hence eligible to spend it – without revealing other information such as where that money came from, or how much other currency they hold. This allows users the ability, when they choose to use a shielded transaction, to disentangle the 'coins' they transact with any previous transactions they may have been associated with.

5. Conclusion

The development of private cryptocurrencies has revealed that fungibility and anonymity are effectively synonymous. This argument has implications for regulatory and economic processes that seek to earmark income or wealth for particular purposes. The implications of anonymous cash are well explored in Rogoff (2016). Privacy focused cryptocurrencies add a significant extra dimension to these arguments. The fungibility of privacy-centric cryptocurrencies such as Zcash is analogous to the role that physical cash has played in transactions up until more recent regulatory interventions. The use of cash has always played a role in obfuscating the types of transactions individuals engage in. Paying for goods and services using cash can hide information which we might otherwise prefer to keep secret; sensitive information related to legal matters and taxations records, medical issues, sexual activity and personal preferences can all be deduced given access to enough financial data. Paying for goods or services with a form of currency which has a high degree of fungibility provides a level of anonymity to the user.

6. References

Aitken, R. 2018. "U.S. Marshals To Hold Bitcoin Auction For $50 Million Worth Of Cryptocurrency." *Forbes.com*. Accessed 4 June 2018. https://www.forbes.com/sites/rogeraitken/2018/01/12/u-s-marshals-to-hold-bitcoin-auction-for-50-million-worth-of-cryptocurrency/#c9deb3a6127d.

Antonopoulos, A.M. 2017. *Mastering Bitcoin: Programming the Open Blockchain*: O'Reilly Media.

Berg, Alastair, and Chris Berg. 2017. "Exit, Voice, and Forking."

Berg, Alastair, Chris Berg, S. Davidson, and Jason Potts. 2018. "Identity as input to exchange." *SSRN*.

Carruthers, Bruce G. 2010. "The meanings of money: A sociological perspective." *Theoretical Inquiries in Law* 11 (1):51-74.

Casey, M.J., and P. Vigna. 2018. *The Truth Machine: The Blockchain and the Future of Everything*: HarperCollins Publishers.

Coase, Ronald H. 1937. "The nature of the firm." *economica* 4 (16):386-405.

Coase, Ronald H. 1960. "The problem of social cost." *The journal of Law and Economics* 56 (4):837-877.

Cockfield, Arthur J. 2016. "Big Data and Tax Haven Secrecy." *Florida Tax Review* 18 (8):483-539.

CoinMarketCap. 2018. "All Crypotocurrencies." https://coinmarketcap.com/all/views/all/.

Commonwealth of Australia. 2018. Budget Measures, Budget Paper No. 2, 2018-19.

Department of Home Affairs. n.d.-a. Anti-money laundering and counter terrorism financing. Accessed 1 June 2018.

Department of Home Affairs. n.d.-b. Threshold transaction reports (TTRs). Accessed 1 June 2018.

Durner, Tracey, and Liat Shetret. 2015. Understanding Bank De-Risking and its Effects on Financial Inclusion: An exploratory study.

Federal Bureau of Investigation. 2012. Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity.

Goldfeder, Steven, Harry Kalodner, Dillon Reisman, and Arvind Narayanan. 2017. "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies." *arXiv preprint arXiv:1708.04748*.

Goldwasser, Shafi, Silvio Micali, and Charles Rackoff. 1989. "The knowledge complexity of interactive proof systems." *SIAM Journal on computing* 18 (1):186-208.

Greenberg, A. 2015. "Prosecutors Trace $13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop." *Wired.com*. Accessed 4 June 2018. https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/.

Gruber, Sarah. 2013. "Trust, Identity and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion." *Quinnipiac L. Rev.* 32:135.

Kappos, George, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. 2018. "An Empirical Analysis of Anonymity in Zcash." *arXiv preprint arXiv:1805.03180*.

Koshy, Philip, Diana Koshy, and Patrick McDaniel. 2014. "An analysis of anonymity in bitcoin using p2p network traffic." International Conference on Financial Cryptography and Data Security.

Leiser, D., and Y. Shemesh. 2018. *How We Misunderstand Economics and Why it Matters: The Psychology of Bias, Distortion and Conspiracy*: Taylor & Francis.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. 2013. "A fistful of bitcoins: characterizing payments among men with no names." Proceedings of the 2013 conference on Internet measurement conference.

Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash system."

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*: Princeton University Press.

Passas, Nikos. 2018. "Report on the debate regarding EU cash payment limitations." *Journal of Financial Crime* 25 (1):5-27.

Quesnelle, Jeffrey. 2017. "On the linkability of Zcash transactions." *arXiv preprint arXiv:1712.01210*.

Raghubir, Priya, and Joydeep Srivastava. 2008. "Monopoly money: The effect of payment coupling and form on spending behavior." *Journal of experimental psychology: Applied* 14 (3):213.

Reid, Fergal, and Martin Harrigan. 2013. "An analysis of anonymity in the bitcoin system." In *Security and privacy in social networks*, 197-223. Springer.

Reid, Kenneth. 2013. "Banknotes and their vindication in eighteenth-century scotland." *University of Edinburgh, School of Law, Working Papers,*.

Reynolds, Perri, and Angela SM Irwin. 2017. "Tracking digital footprints: anonymity within the bitcoin system." *Journal of Money Laundering Control* 20 (2):172-189.

Rogoff, K.S. 2016. *The Curse of Cash*: Princeton University Press.

Sahm, Claudia R, Matthew D Shapiro, and Joel Slemrod. 2010. Check in the mail or more in the paycheck: does the effectiveness of fiscal stimulus depend on how it is delivered? : National Bureau of Economic Research.

Stanley, Rebecca L, and Ross P Buckley. 2016. "Protecting the west, excluding the rest: The impact of the AML/CTF regime on financial inclusion in the pacific and potential responses." *Melb. J. Int'l L.* 17:83.

Swan, M. 2015. *Blockchain: Blueprint for a New Economy*: O'Reilly Media.

Thaler, Richard H. 1990. "Anomalies: Saving, fungibility, and mental accounts." *Journal of economic perspectives* 4 (1):193-205.

Trautman, Lawrence. 2013. "Virtual Currencies: Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox." *Rich. JL & Tech.* 20:1.

Vorick, David. 2018. "Ensuring Bitcoin Fungibility in 2017 (And Beyond)." *Coindesk*. Accessed 22 April 2018. https://www.coindesk.com/ensuring-bitcoin-fungibility-in-2017-and-beyond/.

Williamson, Oliver E. 1979. "Transaction-cost economics: the governance of contractual relations." *The journal of Law and Economics* 22 (2):233-261.

Williamson, Oliver E. 1985. *The Economic Intstitutions of Capitalism*: Free Press.

Zelizer, V.A.R. 1997. *The Social Meaning of Money*: Princeton University Press.