# ‘Live as Friends and Count as Enemies’: On Digital Cash and the Media of Payment

# Eduard de Jong, Nathaniel Tkacz and Pablo Velasco

Currency experiments are enjoying something of a renaissance. Some have the number of digital currencies as high as 143, most of which have emerged over the last five years. How did we get here? These experiments have been praised and rallied around by dedicated followers. For some, dedication approaches religious fervor. Critique has also been quick to the scene: constructive critique by insiders or fence-sitters; critique from the outside; critique on the grounds of politics, of economics, ecology, or gender – the list is long and pointed.

The duration of these experiments is also roughly equivalent to the global economic downturn, which is to say that most people have had less money of the non-experimental kind. Money is perhaps the primary media of economic *crisis* in that it translates abstract global disasters into felt hardship, into lack. It is felt most as a medium of crisis when it is in retreat, when its function as a medium of exchange falters. The same cannot be said of technology over the same period. Personal computational devices are only getting ‘smarter’. Moore’s law rolls on. The Hacker Ego is at an all time high. Is this how we got here? Perhaps. But among this general backdrop is a more specific history, of digital cash and technologies of payment. It is a history of developing standards, of road toll systems, magnetic stripe (magstripe) cards and cards with processors (smart card), of radical prototyping and blue-sky experiments, of international cooperation, of banks mixing (or fighting) with telcos, of privacy and security, of failed experiments, of failures that were also successes. This is a history of those who ‘live as friends and count as enemies’.

These are Eduard de Jong’s words, and his personal history is woven through that of digital payment. In June 2014 de Jong visited Nathaniel Tkacz in the English Midlands and over a series of interviews at The University of Warwick, he mapped out some of this largely untold history. Pablo Velasco Gonzalez sorted through the raw material and turned it into something coherent. The arrangement, style, and references are thanks to him. Below, the passages in bold are extracted directly from the interviews. All originate with de Jong and they function to punctuate the rest of the material. The text surrounding the extracted material is collaboratively written, at times summarizing and others elaborating the interview material. Like the history of digital cash itself, de Jong’s story begins with David Chaum’s enterprise, DigiCash.

…

In 1990, Chaum was already a renowned cryptographer working at The University of Amsterdam’s Center for Mathematics and Informatics (CMI). At the time, the Minister of Transport in the Netherlands was considering the introduction of road pricing: the automatic collection of a toll for the use of the motorway system. Chaum took this as an opportunity to implement his ideas for electronic money and start a business. His goal was to provide a working prototype of a payment system that was capable of making complete transactions at speeds of up to 80 km/h, and which were *secure* and protected the *privacy* of the payer. Chaum gathered a group of skilled engineers, mostly from his Eindhoven University former contacts,[[1]](#footnote-1) and started building his e-Cash system with a smart card to hold the funds. De Jong was hired to document the implementation of this system. Specifically, he came up with a formal method to describe the implementation of the e-Cash algorithms, which acted as a bridge of sorts between the algorithms and the assembly language implemented in a smart card. In less than three months, a prototype was ready that included a smart card, a card terminal for use in a car, and a central system unit dubbed the ‘bank’.

**‘This was really the first fully electronic payment system ever. There was a body of knowledge; the 80s had seen a lot of progress, a lot of theories and analyses about how to implement cryptographic algorithms for electronic money efficiently and securely. So the theoretical basis was there, but it was the first time it all came together into building something that could work.’**

The smart card was first of all a store of value. The stored value was securely transferred with a cryptographic key and algorithm also stored in the card. It was in the tradition of prepaid phone and credit cards, but focused much more on security and privacy. To protect privacy in public key cryptography Chaum had invented ‘blind signatures’ in the early 80s.[[2]](#footnote-2) A first draft of his currency system – without any attempt at implementation – was also already published in 1982, when he was still a Professor at UCLA.[[3]](#footnote-3) The blind public key signature that protected the transfer of e-Cash money was cleverly mixed with the Data Encryption Standard (DES – which was developed at IBM by Mathias and Meyer and based on the work of Horst Feistel). For an e-Cash transfer to occur a cryptogram based on a pre-generated digital signature was inscribed with the value to transfer and the smart card software subtracted the value from its stored ‘spendable money’ before sending out the cryptogram. One would spend one signature to encode a quantity of money and the card stored about 20 or 30 usable payment signatures, cleverly wrapped into a small number of blind signatures (and loading money in the card also loaded new signatures). For security purposes each payment signature could only be used once. E-Cash mimicked the qualities of traditional cash: transfers were immediate and one could not spend more than one had. Another unique characteristic of the first e-Cash implementation was that it used a ‘cold processor’ protocol: the terminal receiving the money guided the card through all the needed steps to do the cryptography. This protocol enabled e-Cash to overcome the processing limitations in the smart card for the use of public key cryptography. From a purely technological perspective, e-Cash was a success. However, the first prototype to be used in cars was never tested on the road.

**‘Politics in the Netherlands changed and there was no longer support for a toll road payment system. E-Cash was ready, but it was no longer relevant.’**

The DigiCash team had fulfilled its first goal of making a working prototype for the national road-pricing scheme, ready to be converted by manufacturers into the roadside and in-car equipment. But Chaum was more of a cryptographer than a technology marketer. He failed to recognize the complexity involved in creating a market for this new technology. He underestimated the *nontechnical effort* involved in turning the prototype into a product. DigiCash struggled along without a successful implementation of its prototype. Two years later it realized a second prototype of e-Cash, this time for general payment and with a bank as lead customer, but with a similar result. De Jong learned from these early experiences, and years later, the market failure of e-Cash shaped his thinking about how to approach the market after the development of Java Card technology, which is based on his patents. For Java Card the initial marketing cost were five times the development costs.

**‘DigiCash was not looking at the market. All the focus was on the prototype. Where DigiCash completely failed was in realizing how much work it would be to get a foothold in the market with what they had. Instead, they were spending their money on even more advanced technologies. They completely lost the link with reality, of how to market a technology so advanced, and how to get people to buy into it. DigiCash was certainly way more advanced than any solution that society was willing to accept at the time. It's probably fair to say that it was *too early* in its insistence and successful implementation of *absolute* security.’**

In 1992, de Jong left DigiCash and together with another former DigiCash employee, he started a consultation company on smart cards and cryptographic techniques. By September 1998, after failing to attract more than a handful of strategic partners, DigiCash had declared bankruptcy. Attempts to keep its technology together failed, and one company took up the smart card operating system, while the Intellectual Property portfolio was sold to a Canadian company. Its communication technology, in a simpler and less secure way, was deployed in other kind of ledger-oriented enterprises, such as E-tag in Australia.

Fifteen years earlier banks had started to look at smart cards as the next technological step in the use of payment cards. Credit cards, and in Europe also debit cards, equipped with magstripe and complemented by data communication to back office computers with an account database, were the majority of electronic payments at that the time. They invested manpower in international standardization of this emerging technology, both in Europe within CEN (Centre European des Normes) and in ISO, where the standards for the embossed credit card and the magstripe card had already been developed. However, the banks were not interested in cash; that is, in digital cash systems as the opposite of their traditional ledger systems – at least not as a priority. If anything, the emergence of the first electronic cash systems, systems without the need for a ledger, was met with some trepidation by the banks. They were concerned about their role in payments being reduced. Such fears were not completely without ground, as a number of large European telecom operators were looking at new opportunities to use their experiences with successfully replacing physical cash in payphones. Expanding to other small payments, newspapers, snacks, vending machines and so on, looked like good business opportunities for these telcos. As we will see below, some banks took up the challenge and got involved in experiments with electronic-cash smart cards.

After DigiCash was established, the next attempt to realize electronic cash was Danmønt, in 1991. It was a smart card with a disposable ‘electronic purse’ for small payments, developed by a subsidiary of PBS (Danmønt S/A) and endorsed by KTAS, the Copenhagen Telephone Company, and HT (Capital Traffic, a transport institution). Its pilot started in 1992 and it was introduced on a nation-wide scale in 1993, mostly as a payment method for launderettes and telephone booths.[[4]](#footnote-4) With Danmønt, the payer smart card sent a message with value to a merchant smart card that was authenticated by a secret key using the DES algorithm. Keys were stored in the smart cards, as was the amount of money to spend or receive, respectively.

A year later, Mondex followed. Initiated by the cryptographer David Everett, who worked at NatWest bank at the time, Mondex, like e-Cash and Danmønt, used an exchange of messages to transfer a value. The Mondex team started building a system with technology that had already been patented in 1990 by Tim Jones and Graham Higgins, who refer in their patent application to Chaum’s ideas. In the Mondex scheme a secure computer acted as ‘originator’, one per country, to create units of electronic cash, which were then sold for traditional currency to ‘issuers’ (banks) that could sell them – again, in exchange for traditional currency – to final Mondex users. A transaction between two users was validated by secret keys and algorithms stored on the smart cards held by each user. Electronic money received by an end user could only be exchanged back to legal tender by transferring it back to an issuer. The Mondex originator, its issuers and end users all used the same basic security protocol to transfer value, with the issuers expected to deploy racks filled with smart cards. According to de Jong, the fully off-line security provided a potential fatal security weakness. Mondex was put to a consumer test in July 1995 in Swindon, U.K.. McDonald's, BP, Sainsbury's, and other major retailers were involved in the test.[[5]](#footnote-5) NatWest and Midland Bank (now part of HSBC) were shareholders of Mondex. The Bank of Scotland was also a sub-franchise holder, and both the Royal Bank of Canada and the Canadian Imperial Bank had planned a pilot program for it in 1996.[[6]](#footnote-6) The system was eventually sold to Mastercard, which kept it alive for the smart card operating system, Multos,[[7]](#footnote-7) which was developed to support the electronic money system. Mondex’s security protocol has not been published[[8]](#footnote-8) and consisted of public key signatures to validate messages with a public key from the Mondex originator protecting the authenticity and the privacy of the per card unique transfer key. In 1996, smart card chips could not yet perform public key cryptography efficiently and the Swindon trial for Mondex used a modified protocol using the DES algorithm and shared secret keys.

Smart cards had already been used as pre-paid phone cards from the mid-1970s. But consciousness of their much broader possible application, in medical records, banks transfers, driver’s licenses, public transport, and electronic payments, for example, only emerged through the 1980s and 90s. The 1987 Smart Card 2000 conference co-organized by Chaum is testimony to this growing awareness. International standardization for smart cards started in 1984 as an extension to standardisation on credit cards, which had started in 1970. Advanced technology people from banks, researchers at telco-labs, and representatives of the fledgling smart card industry came together four or five times a year under the banner of ISO/IEC SC 17WG4 to discuss standards for physical design aspects, like the size and placement of the chip in the card, the size and shape of the chip contacts for communication with the processor, and for the basic operations to be supported, such as reading and writing to memory and doing cryptography. By 1989, work in ‘WG4’ on the first aspects of standardization resulted in three standard documents. Like all standardization work these documents reflected the ‘give-and-take’ negotiations of the participating companies. Consensus for the location of the contacts, for example, proved hard to achieve and the first standard allowed for two different places. One chip location, called, with some chuckles, the ‘French position’ specified in the first standard was phased out in later documents. Finally in 1995 a fourth standard was published: ISO/IEC 7816-4. For those involved, this result was celebrated by handing out T-shirts with the text: ‘survivor of ISO/IEC 7816-4’. De Jong joined the ISO standardization group just before this milestone.

European countries had identified these cards as an area in need of European regulation and standardization beyond what was happening in the ISO group. In particular they were looking for standards for card applications. The European Standardization Body (CEN TC224) was set up to do this work in 1990. Within TC224 an Electronic Money Group (WG10) was established with someone sponsored by Danmønt as its first convenor, and included members from the Bank Union in Norway (Edmond Alnianakian), Masterpay in Belgium (Phillipe Duhamel), the U.K.’s telecommunications, RATP (Régie Autonome des Transports Parisiens) (Phillipe Vapperau) also in France, and de Jong as the independent technology provider from DigiCash. He joined in 1991, while still at DigiCash, mostly to decide what should be added to the standard to ensure that it would be compatible with the more complex security protocols used by DigiCash. The collision between people from the electronic cash, banks, transport and payment industries, and across five countries, created difficulties in achieving a technical agreement or even an understanding of the standard. All the parties had different interests in the different aspects of the technology. Indeed, initially in WG10 there was no clear understanding of the nature of an electronic money system as something that is actually different from traditional cash. This general understanding did emerge, but further difficulties arose with the specification of the actual protocols. De Jong recalls that the main discrepancies were on the structure of data stored in the smart cards and their security attributes. The Germans on the task force wanted something more structured than the other parties were willing to accept, and for a long time representatives from Mondex, who joined the group later, were unwilling to modify their message protocol to fit with the standard’s idea for a unified set of messages.

**‘In standardization for IT, agreeing has come to mean: we agree to have a label for each other, for our technology, and you implement my technology using my label and I implement your technology using your label.’**

More parties joined later, including Chris Stanford of the U.K.’s GEC Traffic Automation Company and Ram Banarjee, one of the founders of General Information Systems Ltd (GIS). Established in 1985 in Cambridge, GIS was an early Mondex supporter, designing and building ‘wallets’ to give a Mondex user an interface to review transactions in the card as well as the overall balance. Five years and 20 meetings after de Jong’s inclusion in the electronic purse standardization group, the number of people had grown from 6 to 60 (in 1996). It was the peak time of the electronic cash systems’ deployment.

**‘They all believed this was going to happen soon. I mean, DigiCash proved that there was a lot of interest. It had generated a lot of hype. They believed, if they could just all come together, get organized, get a standard and get the implementations deployed…’**

The test in Swindon was happening at this time, both in banking and transport. Another bankcard was deployed in Germany (but with government specifications that demanded the strong involvement of a telco), and Carte Bancaire deployed a least one in France. In the Netherlands two cards were deployed, one supported by telcos and one by banks.

**‘We are in 1996. Everybody is ready to deploy and everybody deploys. And then, basically, nothing happens.’**

Why? According to de Jong, the banks remained primarily interested in strengthening their existing cashless payment systems, the credit and debit card transactions at the point of sale. To that end, the three international payment associations that handle the majority of these transactions, Europay, Mastercard and Visa, got together to form yet another standardization organization (EMV). In other words, there were multiple energies going in different directions and multiple strategies being deployed or tested simultaneously. EMV developed a standard for actually using a smart card at the point of sale, to recognize the type of payment (credit, debit, electronic cash), and with user elements like entering a PIN. A smart card system for debit or credit cards was a migration from the familiar magstripe cards. Towards the end of the 90s these standards were all but ready, and once in place the banks became very focussed on actually introducing smart cards as payment cards. They wanted to reap the benefits of reduced card fraud that smart cards promised. That is, they were more interested in smart cards as a security technology and less interested in its capacity to facilitate digital cash transactions.

Getting ‘PIN&Chip’ (as the use of smart card in point-of-sale payments became known) introduced took a full decade. As a migration from magstripe cards, smart cards did not fundamentally alter the centralized model of banking. This banking model is a known as a ledger system, where the actual transfer of value does not take place at the point of interaction between payer and payee but rather through the administrative action of an intermediary. The word ‘ledger’ comes from the large flat books that banks traditionally used to keep records of the financial transactions they performed for their customers.

With the introduction of smart cards for debit and credit payments well underway, two more payment networks, American Express and JCB (originally Japanese) join EMV. By that time – in the early 2000s – banks reduce their direct involvement in smart card standardization, and instead channel their influence through EMV and Global Platform – yet another smart card related standards organization. The banks’ interest in digital cash had lost momentum, and had begun to look more like a defensive, knee-jerk reaction to Chaums’ e-Cash implementation. Despite standardization agreements and ‘technically’ successful deployment in many countries in Europe, most electronic cash systems are not widely adopted by the public. As a result, the interest of operators, banks, and telcos wanes. The banks stick with their ledgers and the ‘sufficient’ security offered by the emerging pin-and-chip cards. With Moore’s law ensuring ever more processing power, the implementation of the large database systems to implement a ledger payment eventually became so efficient that each single transaction was effectively free of costs. The European standards group TC224 WG10 that de Jong had joined in 1991 to initially develop card application standards beyond the ISO, was shutdown in 2009.

In terms of electronic cash not gaining much traction with the public, Danmønt is perhaps a notable exception. Through its integration with the Danish launderette system, Danmønt enjoyed levels of usage and social penetration beyond most other implementations, managing to stick around until 2005. The relative success of Danmønt holds lessons that need to be examined in future experiments.

**‘They (electronic cash systems) worked technically, but there is no longer an incentive to actually make them work commercially.’**

While interest in smart cards for banking settled on deploying PIN&Chip, another application of a ledger-based smart card system had been enjoying huge successes. The telecommunication industry had focused its attention on smart cards to use in the then emerging mobile telephony industry. To support mobile telephony the Telecommunications Commission of the CEPT (Conférence Européenne des Postes et Télécommunications) had created a standardization group, GSM (Groupe Spéciale Mobile, and later renamed as Global System for Mobile Communications). By 1989, its first phase of specifications were approved based on the ISO standards for card size and communication. Once the European (and later global) standard was developed, phone-embedded GSM smart cards enjoyed a ready-made (phone) market and were very easy to massproduce.[[9]](#footnote-9)

**‘What really takes off with smart cards is GSM. There was a made in heaven combination of technologies and that led to the take off of the smart card production. At one point banking would do about 100 million smart cards a year, and there were 3 billion smart cards in phones, per year.’**

Smart card manufactures were interested in the success of the GSM standard because it allowed them to make secure transactions and encrypt communication. Handset manufacturers were equally invested because the standard would allow them to focus on making machines that would do the radio communication and network deployments, which made the link between the phone and the person. Common interest resulted in the fast implementation and deployment of a chip-based secure model for wireless phones – the GSM standard – in 1998. The standard had two central goals: *protect the communication* and *ensure its payment*.

**‘The privacy threatening nature of centralized accounting […] if there is anything that David inspired in me, it is the concern of fundamentally privacy sensitive systems.’**

Privacy and security had been the quintessential concerns for much of the developer and hacker community. Chaums’ invention of blind signatures was specifically motivated by the protection of privacy. It was a clear political motivation. He is on the record stating that, ‘The difference between a bad electronic cash system and well-developed digital cash will determine whether we will have a dictatorship or a real democracy’.[[10]](#footnote-10) Cash and ledger systems manage two fundamentally different types of value transfer messages. In the former, the message *is* the value and in the latter the message is an *instruction to transfer* a value. E-Cash, Danmønt, and Mondex differed in terms of cryptography and architecture, but they were all *cash* systems. The information stored in the cards was itself spendable. To lose a card meant losing the money. With ledger systems, where the message only carries information about the transfer of value, the actual transfer happens later. The ledger generates centralized traces of all activity and these are almost always tied to accounts with real identities. The existence of the ledger is why losing a credit or debit card doesn’t necessarily mean losing money (because an individual *account* is kept at a distance from the media and messages that inform the ledger about transactions), and equally why ledger-based transactions are not difficult to reverse (because the ledger is the actual site of the transaction). The same attributes of the ledger that separate message from transaction and enable reversibility, make it a political target for people like Chaum.

Money had been what de Jong refers to as ‘transubstantiated’ into electronic information much earlier than the birth of digital cash. In the 1920s Amsterdam had seen the first automatic ledger system, processing transactions by updating account cards with mechanical retrieval and sorting. For de Jong, the ledger is the crucial technology – or ‘cultural technique’– that transforms money into information for the first time. This ‘other great transformation’,[[11]](#footnote-11) sets the quest for the re-creation of the *qualities* of cash into motion. Ledgers are anathema to supporters of digital cash.

In the 1970s, electrons are being stored in silicon in early phone cards to represent a stored value, still a good ten years before magstripe technology used the ledger system to identify account information on paper slips or with a networked connection. Telco companies like GSM used a ledger system that was a lot simpler than those of the banks, but it was nevertheless a centralized accounting system designed to keep efficient control of airtime through its quantification, and reconciled with monthly payment or a prepaid account. The step from this purely administrative system to a transfer and ultimately a payment system, like the one used today in mobile money transfers, was not a big one. Indeed, the cost of entering a ledger transaction approaching zero, combined with the ability to buy discrete quantities of airtime (made possible by an efficient database implementing the ledger), was enough for phones to become money systems with no initial strategic oversight. Phones had slowly become money-machines, technologies of payment, which is not the same as exchange. Payment *colors* exchange, it augments but also colonizes it in various ways. We are dealing with payment when all of the mirco-mediations of exchange are understood as forming a value chain, as comprising a unique political economy. This becoming payment machine of phones partly explains what happened in Kenya with M-Pesa.

**‘Apart from cash (notes and coins) all the money systems are ledger based. Everything is balances, records of aggregated amounts received and paid. Every balance has an identifier attached, an account, and that identity-based accounting is the core of banking. We can criticize the use of the system, but the system is all that exists. Our current money system has proven itself a very close fit with a wide array of societal needs. Maybe we haven’t realized how integrated it is into society. By trying to create alternatives, you discover how finely tuned traditional money is to all kind of needs in society.’**

The recent proliferation of cryptocurrencies modelled after or inspired by Bitcoin, enact a novel combination of cash and ledger systems. In these systems, the ledger is hosted across multiple servers and geographically decentralized, but the ledger very much remains the foundation of these systems. Indeed, in some ways these systems are even more centralized because – at least in the minds of believers – the ledger becomes the ultimate authority, with no possibility for appeal if things go wrong. The ledger is conflated with sovereign authority.

De Jong says there is once again an interest in cash systems. For him, digital cash is a spectre haunting the new ledger-hybrids. Right now he is working on a community currency system, capable of integration with existing currencies. Its protocol uses asymmetric security, allowing the payer to be stay anonymous but not the payee, as in traditional cash payments, and will be usable through a phone user interface. There are plans to deploy it in Canada.

## References

Böhle, Knud, Michael Rader, and Ulrich Riehm. ‘Electronic Payment Systems in European Countries: Country Synthesis Report’, Forschungszentrum Karlsruhe*,* September 1999,<http://www.itas.kit.edu/pub/v/1999/boua99b.pdf>.

Chaum, David. ‘Blind Signatures for Untraceable Payments’, in David Chaum, Ronald L. Rivest, and Alan T. Sherman (eds), *Advances in Cryptology*, New York: Springer, 1983, pp.199-203, <http://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18>.

Clemons, E.K., D.C. Croson, and B.W. Weber. ‘Reengineering Money: The Mondex Stored Value Card and Beyond’, in *Proceedings of the Twenty-Ninth Hawaii International Conference on System Sciences*,Vol. 4, 1996: 254-61, doi:10.1109/HICSS.1996.495345.

Greenberg, Andy. *This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cypherpunks Are Freeing the World’s Information*, New York: Random House, 2012.

Haug, Thomas. ‘A Commentary on Standardization Practices: Lessons from the NMT and GSM Mobile Telephone Standards Histories’, *Telecommunications Policy* 26 (2002): 101-7.

[‘How DigiCash Blew Everything’], January 1999, <http://cryptome.org/jya/digicrash.htm#15>.

Landrock, Peter. ‘Mondex’,. in *Encyclopedia of Cryptography and Security*, Henk C. A. van Tilborg (ed.) New York: Springer, 2005, p. 394, <http://link.springer.com/referenceworkentry/10.1007/0-387-23483-7_262>.

Polanyi, Karl. *The Great Transformation: The Political and Economic Origins of Our Time*. 2nd edition, Boston, MA: Beacon Press, 2002.

Schellhorn, Gerhard, Holger Grandy, Dominik Haneberg, and Wolfgang Reif. ‘The Mondex Challenge: Machine Checked Proofs for an Electronic Purse’, in Jayadev Misra, Tobias Nipkow, and Emil Sekerinski (eds) *FM 2006: Formal Methods*, Lecture Notes in Computer Science 4085, Berling and Heidelberg: Springer, 2006, p.16-31, <http://link.springer.com/chapter/10.1007/11813040_2>.

1. ‘How DigiCash Blew Everything’], January 1999, <http://cryptome.org/jya/digicrash.htm#15>. [↑](#footnote-ref-1)
2. David Chaum, ‘Blind Signatures for Untraceable Payments’, in David Chaum, Ronald L. Rivest, and Alan T. Sherman (eds) *Advances in Cryptology*, New York: Springer, 1983, pp. 199-203, <http://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18>. [↑](#footnote-ref-2)
3. Andy Greenberg, *This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cypherpunks Are Freeing the World’s Information*, New York: Random House, 2012. [↑](#footnote-ref-3)
4. Knud Böhle, Michael Rader, and Ulrich Riehm, ‘Electronic Payment Systems in European Countries: Country Synthesis Report’, Forschungszentrum Karlsruhe*,* September 1999,<http://www.itas.kit.edu/pub/v/1999/boua99b.pdf>. [↑](#footnote-ref-4)
5. E.K. Clemons, D.C. Croson, and B.W. Weber, ‘Reengineering Money: The Mondex Stored Value Card and Beyond’, in *Proceedings of the Twenty-Ninth Hawaii International Conference on System Sciences 1996*, Vol. 4, (1996): 254-61, doi:10.1109/HICSS.1996.495345. [↑](#footnote-ref-5)
6. Clemons, Croson, and Weber, ‘Reengineering Money’. [↑](#footnote-ref-6)
7. Peter L-, ‘Mondex’, in *Encyclopedia of Cryptography and Security* (ed.) Henk C.A. van Tilborg, Berlin and Heidelberg: Springer, 2005, p. 394, <http://link.springer.com/referenceworkentry/10.1007/0-387-23483-7_262>. [↑](#footnote-ref-7)
8. Gerhard Schellhorn et al., ‘The Mondex Challenge: Machine Checked Proofs for an Electronic Purse’, in Jayadev Misra, Tobias Nipkow, and Emil Sekerinski (ed.) *FM 2006: Formal Methods*, Lecture Notes in Computer Science 4085, Berlin and Heidelberg: Springer 2006, pp. 16-31, <http://link.springer.com/chapter/10.1007/11813040_2>. [↑](#footnote-ref-8)
9. Thomas Haug, ‘A Commentary on Standardization Practices: Lessons from the NMT and GSM Mobile Telephone Standards Histories’, *Telecommunications Polic* 26 (2002): 101-7. [↑](#footnote-ref-9)
10. [‘How DigiCash Blew Everything’]. [↑](#footnote-ref-10)
11. Karl Polanyi, *The Great Transformation: The Political and Economic Origins of Our Time*, 2nd edition, Boston, MA: Beacon Press, 2002. [↑](#footnote-ref-11)