

The Nuts and Bolts of Micropayments: a Survey

Syed Taha Ali
NUST School of Electrical Engineering
and Computer Science, Pakistan
Email: taha.ali@seecs.edu.pk

Dylan Clarke
Newcastle University
United Kingdom
Email: dylan.clarke@newcastle.ac.uk

Patrick McCorry
University College London
United Kingdom
Email: stonecoldpat@gmail.com

Abstract—We are witnessing a veritable explosion of interest in new electronic payments systems and modalities, such as digital wallets, mobile and contactless payments, and cryptocurrencies such as Bitcoin. One area of research and commercial interest at the confluence of these trends, which is also receiving reinvigorated attention, is micropayments. Indeed, a workable micropayments system, one that lets users purchase digital content in an easy and “hassle-free” manner with payments in the order of cents and lower, has long been regarded as the holy grail of web-publishing. The research community has actively worked on this problem over the past two decades, numerous creative solutions have been presented, business ventures have been launched, but a mainstream solution has yet to emerge.

In this paper, we undertake a comprehensive survey of key trends and innovations in the development of research-based and commercial micropayment systems. Based on our study, we argue that past solutions have largely failed because research has focused heavily on cryptographic and engineering innovation, whereas fundamental issues pertaining to usability, psychology, and economics have been neglected. We contextualize the range of existing challenges for micropayments systems, discuss potential deployment strategies, and identify critical stumbling blocks, some of which we believe researchers and developers have yet to fully recognize. We hope this effort will motivate and guide the development of micropayments systems.

Index Terms—micropayments, cryptocurrencies, electronic payments systems

I. INTRODUCTION

The ongoing popularity of Bitcoin has inspired keen interest in digital currencies in the research community, the financial sector, and even at the government level. This surge has also rekindled the conversation on developing systems to enable micropayments, i.e. low-value digital transactions, typically in the order of pennies and cents. Micropayment transactions may be considered the electronic equivalent of purchases made using pocket cash or spare change. Historically, the problem with low-value transactions has been that processing and transaction fees end up dwarfing the actual transaction amount¹. Payment processors impose these fees for a variety of reasons including infrastructure costs, administrative charges, and mechanisms for fraud prevention and dispute resolution. There has been considerable research in the past two decades on using digital communications and cryptography to minimize these costs, ideally down to the fraction-of-a-cent range.

The traditional argument goes that, if enabled, micropayments stand to be a key pillar of the information economy [2],

¹For instance, in 2014 UK-issued debit and credit cards (with chip and pin) typically averaged transaction fees of 14 and 81.5 pence respectively [1].

with direct and immediate applications in reviving journalism [3] and supporting the music industry [4]. The ability to economically transfer minuscule amounts of money at high speeds will empower dynamic new pricing models where digital content such as online newspapers, magazines, and music albums can be unbundled, allowing consumers to purchase individual news stories, articles, and songs. Furthermore, with pricing in the sub-dollar range, users will be encouraged to increase spending and also engage in impulse purchases, thereby opening up powerful new revenue streams.

There have been two main waves of innovation in designing and deploying micropayment systems, the first in the late 1990s and the second in the 2000s [5] [6]. Both efforts largely failed, and only a few systems have survived. Reasons include poor infrastructure support, cumbersome and non-intuitive system design, and conservatism on the part of financial institutions and users. Critics have also cited poor business cases and neglect of critical psychological factors [7] [8] [9].

Today, however, the landscape has changed in some fundamental ways. First and foremost, the business case for micropayments is validated. Large numbers of consumers now regularly make low-value payments for online content. Apple’s iTunes store has proved a resounding success [10]. In the smartphone universe, iOS app developers reportedly made over \$10 billion in 2014 from in-app purchases, to put in context, a figure greater than Hollywood’s box office earnings [11]. New multiplayer video games now enable millions of players to make in-game purchases as part of gameplay. The popular League of Legends singlehandedly earned \$624 million in 2013, and almost a billion dollars in 2014 [12], from these ‘microtransactions’ in which players purchase premium in-game items like characters, weapons, healing portions, etc. costing single digit dollar amounts.

Second, the current advertising-based web publishing model is in crisis. Web ads are intrusive, degrade user experience, and significantly increase data consumption [13], a particular concern for mobile users [14]. Users are also concerned about privacy and third party tracking [15] [16] [17], especially in the wake of the Snowden revelations [18].

Collectively these factors have given rise to the ‘ad-wars’ phenomenon: globally, some 198 million people deploy ad-blocking software, such as Ghostery and Adblock Plus, leading to a staggering \$22 billion in lost revenues [19]. Upcoming versions of Apples iOS9 and OSX 10.11 are both reported to feature default ad blocking functionality [20]. A recent study

[19] notes that adblockers pose an “existential threat” to the ad-based publishing model. Some commentators are therefore calling for a fundamental rethink of the current web publishing model [21] [22]. Micropayments are a leading alternative.

Third, there are promising developments on the ground. The technology has vastly improved in the last decade: high speed broadband is ubiquitous, public key infrastructure is widely deployed, Web browsers have far more functionality, and smartphone penetration is high. Public attitudes have also changed: millions regularly engage in online banking and participate on social networks. The concept of mobile wallets and cryptocurrencies is no longer alien. Surveys report people are now more willing to pay for online content [23] [24]. Charities have begun to leverage micropayments (or ‘microdonations’) for raising funds [25].

There is also the Bitcoin experiment. Whereas Bitcoin’s long term success is still an open question, its popularity has nonetheless inspired researchers to reimagine payments systems. Financial institutions and governments also appear more receptive to innovation. Some of the world’s largest banks are already in the process of appropriating Bitcoin’s key innovation, the blockchain, to reduce infrastructure costs by an estimated \$15-20 billion [26].

Due to these factors we are witnessing what we believe is the third wave of micropayment systems. Several new micropayments solutions have launched, several more are about to, and collectively several millions of dollars of startup capital has been raised. Blendle, an “iTunes for newspapers”, has received substantial press, and has made deals with the New York Times, the Washington Post, and the Wall Street Journal to sell individual articles for 20 cents on average [27]. WeChat, a leading Chinese content publishing platform, and one of the world’s largest, with 600 million active users intends to introduce a ‘like’ button which will allow readers to reward authors with micropayment donations ranging from under \$1 up to \$30 [28]. Google Contributor allows users to pay a small monthly fee for an ad-free browsing experience on supported websites [29]. And a slew of solutions, such as Bitwall, BitMonet and Flattr, piggyback on Bitcoin’s payment network [30] taking advantage of Bitcoin’s low transaction fees². Brave Software Inc. is currently trialling a micropayments solution integrated directly into the Brave Web browser [32].

We believe therefore that this is an opportune time to revisit the topic of micropayments. Our contributions are:

- 1) We undertake a comprehensive survey of micropayments solutions in the research literature and highlight the workings and key features of representative systems,
- 2) We classify past and present commercial micropayments systems and identify the strategies they use,
- 3) We identify key challenges ahead in design and deployment of these systems and formulate recommendations.

Based on our study, we find is that there is considerable room for work. Research-based systems consist almost entirely

of novel cryptographic solutions with the primary design focus being security and efficiency concerns, whereas commercial systems opt for simple and intuitive cost-cutting strategies such as aggregating multiple payments and automating payment processing. These two domains are mostly isolated from each other (with the notable exception of Bitcoin-based micropayments systems). However, the vast majority of micropayments solutions have failed, in large part due to neglect of critical non-technical concerns such as usability issues, ethical and legal concerns, poor business cases, and ineffective deployment strategies. However, we believe that once these challenges are fully recognized, technology may be successfully used to address them. For this reason, we do not restrict our study solely to the cryptographic literature, but also draw together critical insights from other domains impacting micropayments systems.

To the best of our knowledge, we are the first to perform such a broad study. We have located only two prior surveys on micropayment systems in the past decade: Párhonyi [6] documents micropayments systems with a focus on commercial solutions, whereas Jain et al. [33] specifically consider peer-to-peer schemes from the research literature. Surveys on digital currencies (e.g. [34] [35]) usually include some micropayments schemes but the emphasis is on aspects of electronic cash in general. Micropayments systems involve certain unique challenges (technological, psychological, and economic) differentiating them from general payments systems and necessitate a specialized study.

The rest of this paper is organized as follows: in Sec. II, we introduce key properties of micropayments systems and broadly summarize developments in this field. In Sec. III-IV, we examine the range of cryptographic and commercial solutions and emphasize their strengths and weaknesses. In Sec. V, we discuss key challenges ahead and present recommendations. We conclude in Sec. VI.

II. BACKGROUND

In this section, we qualify micropayments, discuss properties of micropayments systems and trace their development.

A. Definitions and Properties

There is considerable variance over how small a payment must be to qualify as a micropayment. One of the earliest solutions, Millicent, envisioned transactions in the sub-penny range [36]. Kniberg classifies them as payments of up to €1 [37], whereas a study of European online payments sets the threshold at €5 [38]. Commercial provider PayPal classes micropayments as typically under \$10 [39]. There is, however, broad agreement that the associated processing fees should be low enough to justify very small transactions and that these costs should ideally be significantly less than those charged by mainstream payment systems, such as credit cards.

The size of the payments broadly determine the requirements of the payment system. For macropayments (i.e. large and medium-sized payments), regulation may mandate that payments be recorded and that dispute-resolution mechanisms

²At the time of writing, the minimum transaction fees for Bitcoin Core version 0.11.1 stands at 0.00005 satoshis which equates to \$0.02 [31].

be implemented. Customers themselves may prefer extensive transaction records and fraud prevention mechanisms for large value payments, all of which result in higher processing costs. Furthermore, users typically make large transactions much less frequently than smaller ones and processing fees for the former may not seem too heavy a burden. User anonymity and processing fees are therefore generally of secondary importance in macropayments and assume primary concern as payment size approaches the sub-dollar range.

Processing fees for payments systems generally comprise infrastructure and clearing costs, i.e. costs due to equipment, computation, storage, communication and accounting. Certain systems may incur additional costs, depending on transaction type or payment modality. However, micropayments also involve what economists describe as cognitive or **mental transaction costs**, i.e. the “hassle-factor” associated with having to choose fine-grained bundling options at very low prices. Szabo [7] has argued persuasively that researchers often overlook the fact that these mental costs outweigh the technological and are a determining factor in system adoption.

In the context of e-commerce, micropayment systems are generally envisioned as incurring minimal processing delay and facilitating instant delivery of goods [40]. The micropayments ecosystem typically consists of three principal entities: **customer** or user denotes an individual or party which transacts goods and services from a **merchant**. The transaction is enabled or facilitated by a **broker**. This role often belongs to banks or financial institutions which issue the financial instrument or currency used in the transaction, maintain balance accounts for customers and merchants, redeem their funds, and arbitrate in dispute resolution³. Some systems may involve other entities such as peers, certificate authorities, or trusted third parties for various purposes.

System design and uptake is determined by which properties the system provides. We discuss here key properties pertaining to micropayments systems:

Anonymity: refers to the exposure of the customer’s identity and personal information to the merchant and the broker as a direct result of using the payment system. Anonymity in this sense is synonymous with customer privacy. Complete anonymity is achievable with physical cash, whereas with a credit card, both merchant and bank are privy to the customer’s identity and her purchase details. Some commercial systems offer strong anonymity. An example is paysafecard where customers acquire prepaid scratchcards from shops for later spending without revealing any personal information.

Considerable legal issues come into play as a truly anonymous payment mechanism can become a tool for money laundering and crime. Some systems achieve partial anonymity by using pseudonyms to shield personal information from merchants but not the banks. Indeed, in the majority of commercial systems we survey, anonymity from the bank is not a design goal. Another notion is that of revocable anonymity where customer privacy may be overturned in the event of

disputes [41]. Anonymity is ensured either through employing cryptography or defining special procedures. Anonymity is typically established when the customer acquires the currency from the broker or when she pays the merchant.

Security: refers to the integrity of the system, its resilience to fraud, and in particular its ability to prevent counterfeiting and double-spending. In most commercial systems such as PayPal, the broker maintains a customer balance and explicitly authorizes every transaction. Bitcoin extends this approach by employing a distributed and highly synchronized ledger called the blockchain. A novel strategy, used by MicroMint, is to use cryptography to mint crypto-tokens which are far too difficult and expensive to counterfeit.

Validation: indicates whether a system requires real-time contact with the broker to process transactions. Payments systems in the 1990s were limited by low-speed and unreliable dial-up Internet access. Furthermore, requiring the broker in every transaction effectively rendered him a communications bottleneck and a single point of failure in the system. Some solutions, referred to as ‘optimistic’ [42], resolved this issue by contacting the broker only for a small subset of transactions, generally those that proved exceptional or problematic. However, this restriction is now considerably relaxed due to ubiquitous high-speed broadband access and the prevalence of cloud computing.

Transferability: denotes the ease and extent of transferring funds using the system. This includes notions of system **coverage**, **acceptability**, and **penetration** among customers and merchants. Some systems permit a wider range of transactions, such as peer-to-peer transactions in which users may transfer funds directly to each other. Transferability also includes **interoperability**, i.e. permitting payments between different systems and financial institutions, and **versatility**, i.e. facilitating different payment options, such as offline payments, payments using handheld devices, etc.

Payment Mode: indicates how a system actually undertakes the transfer of value between parties. Pre-paid (or debit-based) systems require the customer to input funds into the system prior to making payments which are later deducted from her account. Post-paid (or credit-based systems) track customer spending and charge her at the end of the billing period.

Certain properties apply only to select systems. For example, **divisibility**, i.e. the ability of the system to make payments of arbitrary value, is a limiting factor for some token-based systems. Some systems assume specific **relationship models**, i.e. the service or user experience may be different depending on whether the customer and merchant have a long-term or persistent business relationship as opposed to casual or transient interactions. Some systems may be **hardware-reliant**, i.e. the payment solution relies on a physical device or card which stores cryptographic credentials or currency units. This category includes mobile wallets, smartcards such as Octopus, and Bitcoin wallets like Trezor [43] and Case [44].

In conclusion, there are certain properties common to electronic and networked systems in general. These include **usability**, the ease of use of a system, **scalability**, the ability of

³We use the terms broker and bank interchangeably in this paper.

a system to handle increasing numbers of users and larger payment volumes without significantly degrading performance, and **reliability**, the measure of how dependable a system is.

Next we briefly summarize developments in this field.

B. A Short History of Micropayment Systems

The motivation for micropayments derives primarily from the notion of the **information economy** [2]. Digital goods such as music mp3 files, blogposts, and software are distinct from their physical counterparts, CDs, newspapers, etc. in fundamental ways. For one, digital goods typically bear high fixed costs but negligible marginal costs, i.e. they are expensive to produce but the cost of reproducing these goods is near zero. Deriving from this notion, digital goods are also *non-rival goods*, i.e. they are not restricted to a single customer and may be consumed by multiple parties simultaneously.

These characteristics also apply to digital services which include not just traditional services such as stock quotes and newspapers delivered in electronic format but also interactive new paradigms such as massive multi-player online games (MMOGs). Furthermore, the Internet enables mass distribution of digital goods and services at low-cost: not only do customers have greater access to goods and services but electronic transaction costs are also significantly smaller. In this scenario, affixing very low fees to digital goods and services can prove a powerful source of long-term revenue for merchants.

Micropayment systems for digital content were envisioned as early as the 1960s, when visionary Ted Nelson conceived of intrinsically bidirectional hyperlinks, enabling users to electronically pay for content that they access [45]. In the late 1990s, pioneers Tim Berners-Lee and Marc Andreessen considered incorporating micropayments directly into the Web at the protocol level but were discouraged by conservative banking regulations [46].

Observers broadly agree that there have been two waves of innovation in micropayment systems [5] [6].

The first generation of systems surfaced in the mid-1990s, inspired by the electronic cash movement led by DigiCash. In keeping with the dial-up Internet infrastructure of the time and the relatively low processing power on computers, the main design goal for these systems was to minimize communication and computation costs. A popular strategy used by these systems was the **account-based approach**, used by systems such as CyberCoin, Mini-Pay and NetBill. In this case, the broker maintained accounting ledgers for customers and merchants and aggregated net flow of funds in and out of the system. A centralized ledger prevents double-spending and fraud, whereas aggregation of multiple low-value payments effectively amortizes the processing fees incurred in moving funds between the system and the banking infrastructure. A second strategy, the **crypto-token approach**, employed by systems such as PayWord and MicroMint, used cryptographic mechanisms to mint digital tokens which were computationally infeasible to counterfeit. Customers then used these tokens to transact with merchants.

Several of these solutions were commercialized in partnership with well-known brands, such as DEC, IBM, and Visa but efforts were to fail for a variety of reasons. The dial-up infrastructure was slow and unreliable. These systems had poor usability and suffered from high latency. CyberCash, for example, typically took 15-20 seconds to finalize a transaction [47]. Systems such as Mondex and CAFE also required trusted hardware. Furthermore, the business models have been heavily criticized [8] [9], the systems had poor interoperability, and consequently there was low penetration among merchants.

The second generation of micropayment systems, appearing around 2000, were mostly account-based offerings, such as PayPal and ClickandBuy. Users transferred funds into the system and then used the amount to make payments. This approach had a physical counterpart in prepaid cards, such as Wallie and paysafecard, which users purchased at shops for fixed denominations and then progressively ‘spent’ in online transactions. Another innovation was the use of communications infrastructure, such as email and mobile phones, to validate transactions, as done in systems like Zong.

Several of these systems have survived to the present day. Reasons include good usability, intuitive design, and low latency. For instance, ClickandBuy puts specific icons on merchant websites, which users click to access the payment portal, following which they get immediate access to purchased content. Legislation has evolved to protect users from fraud and safeguard their privacy.

However, the biggest difference is the cultural shift and change in user attitudes due to the advent of online banking and popular online marketplaces such as Amazon. Brand association also played a critical role in the success of payments systems, as evidenced in the example of Apple’s iTunes platform and PayPal’s partnership with eBay [48].

Over the last two decades, there have been efforts to standardize micropayment protocols by organizations such as the World Wide Web Consortium (W3C), the PayCircle consortium, and the Secure Mobile Payment Services (SEMOPS) project. These projects made valuable contributions, including designs for payment protocols, APIs for payment-enabled applications, and mobile payments solutions, but none of these proposals have thus far been ratified into full standards. These efforts are described in more detail in Appendix. B.

III. CRYPTOGRAPHY-BASED SYSTEMS

Here we present a representative selection of micropayments systems relying on cryptographic mechanisms.

We divide these systems into six categories: in centralized systems, brokers mediate customer-merchant interactions and may even authorize purchases in real-time. In voucher-based systems, customers buy vouchers from brokers which they use to make purchases directly from merchants. Commitment-based systems enable customers to pay using signed commitments, much like paying by cheque. In crypto-token solutions transactions are done using tokens that are computationally infeasible to counterfeit. Some systems rely on probabilistic

redemption, i.e. instead of processing multiple small transactions, they probabilistically choose one and inflate the transaction amount accordingly. Peer-to-peer systems adapt several of these solutions for peer-to-peer networks. Bitcoin has emerged as the most popular example of this type. We also discuss proposals to facilitate micropayments using Bitcoin.

A. Centralized Solutions

Chrg-http [49] invented by Tang and Low in 1996 is not a payment protocol per se, but essentially adapts the Kerberos authentication system to set up a secure channel between customer and merchant. Our customer, Alice, contacts a centralized broker who verifies her identity and issues her credentials to communicate with a merchant. Alice makes purchases and the merchant maintains a running balance and bills her at periodic intervals, thereby amortizing transaction costs. Chrg-http was implemented on the Mosaic web browser.

NetBill [50], developed at Carnegie Mellon University in 1995 in partnership with Visa, is a debit-based system for purchasing digital content.

The process flow is as follows: a NetBill server maintains accounts for customers and merchants. Prior to shopping, Alice charges her account by transferring funds into it. The server issues her credentials consisting of a unique user ID and a public/private key pair. An adaptation of Kerberos is used to authenticate communication between customer and merchant.

To purchase a digital item Alice clicks a button on the website, thereby contacting the merchant with her ID and a request for a price quote. The merchant verifies the ID and responds with a price offer. If Alice approves, she sends an acceptance message, resulting in provisional delivery, i.e. the merchant encrypts the item and sends it to Alice. Delivery of the decryption key, however, is conditional upon payment.

Alice next prepares and digitally signs an electronic payment order (EPO) which she sends to the merchant. The merchant appends the decryption key to the EPO, signs the whole package to endorse it, and forwards it to the NetBill server. The server checks if the details are in order, and if Alice's account has sufficient credit, it authorizes the payment. The payment amount is deducted from Alice's account and credited to the merchant, and the transaction is logged.

The server returns a signed copy of the receipt to the merchant with decryption key attached. The merchant forwards a copy to Alice who can now decrypt her purchased item.

The protocol may appear complicated but discourages fraud and facilitates dispute resolution. The EPO includes timestamps, customer and merchant IDs, and identifiers and hash fingerprints of the digital goods being purchased. Alice only signs the EPO after she has received the goods, thereby ensuring delivery. If the merchant reneges on his commitment after the payment is cleared by withholding the decryption key, Alice may contact the NetBill server directly for it.

NetBill has several advantages. No credit card numbers are sent over the Internet. Alice may maintain multiple NetBill accounts and use pseudonyms to protect her privacy. All transactions are handled within the NetBill system and there

are no inter-institution clearing costs. Initial transactions from outside the system to fund customer accounts are typically high volume to amortize transaction costs. Merchant earnings are similarly aggregated before they are transferred from his NetBill account to his bank.

However, there are some shortcomings. Alice may be anonymized to the merchant but NetBill is still privy to all her transactions. A relatively large number of messages have to be exchanged for a successful transaction. There is heavy usage of digital signatures which are compute-intensive operations. Proprietary NetBill software is required.

B. Voucher-based Solutions

In these systems, customers make purchases using digital vouchers obtained from the broker. These systems are intuitive and easy to understand. An advantage of this approach is that the broker need not be involved in transactions. Examples of such systems include Millicent and Foo.

Millicent [36] was invented by Mark Manasse at DEC in 1995, to facilitate sale of online content such as news articles and stock quotes, etc. It is a debit-based system which aimed to provide transaction fees in the sub-cent range.

Millicent vouchers are merchant-specific. Brokers purchase vouchers in bulk from merchants and sell them to customers in turn. Some brokers may obtain a license from the merchant to produce the vouchers themselves as per demand. Customers wishing to purchase items first contact the broker to purchase vouchers for the particular merchant. Vouchers are managed by wallet software on the customer's machine. Customers maintain accounts with brokers but not with merchants.

A Millicent voucher (referred to as *scrip*) comprises two parts: the first consists of identifiers, such as scrip ID and merchant ID. The body contains information pertaining to the voucher, such as its value and expiration date. To certify the voucher as genuine, the creator of the voucher concatenates the body of the voucher together with a master secret credential and uses a one-way collision-free hash function to generate an authenticator which is then appended to the voucher.

To initiate a purchase, Alice sends a content request to the merchant along with a voucher for payment. She certifies the request by concatenating it with her voucher and a secret credential she shares with the merchant, and using a hash function to generate an authenticator which she affixes to the request. The merchant checks if her request and voucher are genuine and then compares the voucher against a database of used vouchers to confirm that it has not been used before. He then dispatches her purchased content. Leftover change is issued in the form of a new voucher for the change amount.

Millicent's advantages include the fact that it only uses hash functions which are considerably more lightweight than public key cryptography. The broker does not have to be online during transactions as the merchant does verification at his end. Millicent also offers partial anonymity in that the merchant need not know the identity of the customer. However the broker maintains a record of all sold vouchers.

However, there are also disadvantages. For one, vouchers are merchant-specific and the system is best suited for long-term customer-merchant relationships. There are also potential dispute resolution issues as only the creator of the voucher can verify it as genuine, since he alone possesses the master credential used to certify it. Non-repudiation is not possible without public-key cryptography. Furthermore, there needs to be a process enabling customer and merchant to share a secret credential which the merchant later uses to verify the customer's purchase requests.

Millicent was briefly trialled in the United States in 1997. An integration of the Millicent payment system with the Minstrel Push system is described in [51].

A related scheme from Foo and Boyd [52] inverts Millicent's protocol for greater efficiency and easy implementation. In their scheme, Alice visits the merchant's website where she can download pre-encrypted copies of the content she is interested in purchasing along with payment vouchers. She then pays for the vouchers at the bank at which point the bank provides her with a decryption key for the goods. The advantage of this scheme is that the burden for processing transactions shifts completely onto the bank and minimal upgrading is required at the merchant's end.

Netcents [53] by Poutanen et al. overcomes merchant lock-in by using *floating scrips*, i.e. signed vouchers which may be passed from merchant to merchant, but valid only with one at a time. Vouchers are customer-specific, issued to them by banks, and contain a balance which customers can spend progressively making purchases from different merchants.

To make a payment, Alice sends the merchant a certified electronic payment order and a voucher. To pay a second merchant using the remaining balance on her voucher, Alice requests him to contact the first merchant directly. All three parties then engage in a protocol to transfer ownership of the voucher to the second merchant with an updated balance.

Netcents relies heavily on digital signatures and intensive communication. Each voucher also bears a signed history of its past which is visible to merchants. A proposed solution is to use blinding mechanisms to hide this history.

The influence of voucher-based schemes is clearly evident in peer-to-peer schemes such as PPay and Bitcoin (Sec. III-F) where the basic currency units are vouchers which are arbitrarily divisible and float from owner to owner.

C. Commitment-based Systems

In these systems customers make purchases using signed promissory notes from customer to merchant, which merchants encash at the bank at regular intervals. The bank also issues customers and merchants with credentials (ID and public/private key pair) enabling them to engage in transactions.

Agora [54], a credit-based system invented by Gabber and Silberschatz in 1996, is a representative example.

To initiate a purchase Alice requests a price quotation from the merchant. The merchant responds with the quote, which includes the price of the item, a unique transaction ID, merchant ID certified by the bank, and the merchant's public

key. Alice verifies that the merchant ID is current and the price is correct. She prepares a purchase order, which includes her certified customer ID and public key, the transaction ID, and the agreed item price. She digitally signs this order before sending it, thereby committing to the purchase of the item as specified by the merchant.

The merchant verifies that Alice's ID is authorized by the bank and the signature on the purchase order is valid, and then dispatches the item. At the end of the billing period, the merchant submits the transaction messages to the bank as proof of transaction. The bank debits the corresponding amount from Alice's account and credits it to the merchant.

Banks can facilitate partial anonymity by issuing customers with aliases. The unique transaction ID protects against replay attacks and double-charging, and the use of digital signatures prevents both parties from altering messages later to claim a different price, as well as protects communication over insecure channels. The authors recommend embedding a hash fingerprint of the purchased item in the exchanged messages for dispute resolution purposes.

In the possibility that a customer (or a thief who has stolen customer credentials) may make large transactions and not pay later, banks can mandate a limit for customer purchases, exceeding which the bank is required to explicitly authorize future transactions. Banks can also alert merchants by periodically broadcasting lists of revoked credentials.

The Agora protocol is remarkably lightweight. The authors develop a Java applet which piggybacks transaction messages onto regular HTTP communications between client and server.

MiniPay [55] developed in 1997 by Herzberg and Yochai innovates on the basic Agora protocol by incorporating Internet service providers (ISPs) as brokers and clearing houses. This idea has precedent in the example of premium telephone numbers used to pay for phone services, such as voting for TV shows and adult chat services.

Customers and merchants maintain accounts with their ISPs, which also issue credentials and specify spending limits. Merchants embed pricing information for items in HTML links. Customers make purchases using software wallets which generate signed commitments in a convenient 'click-and-pay' manner. At the end of the billing period, the merchant submits purchase proofs to his ISP which consolidates various payments and settles outstanding accounts with other ISPs.

MiniPay was successfully trialled and set to launch as a commercial solution by IBM, but this did not materialize.

D. Crypto-token Solutions

These systems use cryptography to mint unique non-forgeable tokens to use in transactions. There are two main approaches to generate tokens, both relying on hash functions.

1) *Hash structures*: These systems derive from Lamport's use of hash chains as one-time passwords [56], also the foundation of Haller's S/KEY protocol [57].

A representative system is **PayWord** [58] developed in 1997 by Rivest and Shamir. PayWord is a credit-based protocol.

In the PayWord ecosystem, the broker issues Alice a certificate validating her as an authentic customer. Alice then mints ‘paywords’, which are payment tokens she will use to pay the merchant. She picks a random seed value which is then repeatedly hashed using a collision-resistant one-way hash function (like SHA1) to generate a chain.

To initialize a purchase, Alice sends a digitally signed commitment to the merchant with information regarding the purchase, such as merchant ID, her customer certificate, and the very last value, or ‘root’, of the hash chain. Computing a signature over this root value essentially certifies the chain and bootstraps the payment process. Each preceding hash value is considered a valid payment token.

The merchant verifies the certificate and signature and authorizes the sale. Alice then sends him successive tokens, an amount corresponding to the price of her item. The merchant hashes the first token he receives to check if it matches the signed root in the commitment message. Each token is likewise checked to verify that it hashes to the previously received token. The one-way nature of the hash function ensures that the merchant can only traverse the chain in the reverse direction, i.e. he can verify tokens, but he cannot generate new ones himself. And due to the one-way nature of the hash function, it is computationally infeasible to forge tokens.

When payment is complete, the merchant sends Alice her item. He sends the commitment message and the final received token to the bank which verifies transaction details and the integrity of the hash chain, and debits Alice’s account by the corresponding amount, crediting it to the merchant.

Like Millicent, this scheme is fast and lightweight since hash operations are orders of magnitude faster than digital signature operations and is ideally suited for long-term customer-merchant relationships.

Receiving change is not straightforward and may require a reverse PayWord transaction from merchant to customer. However, Alice may vary denomination of individual paywords in consultation with the merchant and certify the decision by scripting it in the purchase commitment. PayWord can also be used in a debit-based scenario where brokers generate and sell paywords to customers who then use them to shop.

Similar schemes using hash chains were developed independently by multiple parties including Pederson [59], *micro-iKP* [60], and notably the NetCard project [61] which attempted to integrate this solution with existing banking infrastructure.

Researchers have also innovated further on PayWord. Kim et al. [62] describe a mechanism enabling a customer to transact with multiple merchants with a single hash chain operation. **PayTree** [63] amortizes signature costs by integrating PayWord chains with Merkle trees, so that one signature certifies multiple chains at once. The tree structure also opens up other interesting possibilities: different chains can be used to transact with different merchants concurrently, and chains may be efficiently initialized with various token denominations.

NetPay [64] adapts PayWord for decentralized scenarios. In this case banks issue customers with wallets of payword tokens which they use to purchase items. The first merchant verifies

tokens received from the customer by directly contacting the bank. The next merchant however contacts the first merchant to verify token he receives, and so on and so forth for other merchants. The bank therefore does not need to be involved every time the customer interacts with a new merchant.

2) *Hash Collisions*: These schemes exploit the inherent difficulty of finding hash collisions, i.e. two input values which map to the same 160-bit hash output value. As per the ‘birthday attack’ finding a single hash collision requires, on average, hashing through $1.2 \times 2^{160/2}$ values, which entails not just immense computation effort and time, but also enormous storage requirements (all input/output values have to be stored and searched to identify a collision).

Verifying a collision, however, is extremely easy: one just has to hash the input strings and confirm if the outputs match. This sharp asymmetry in generating and verifying collisions can be exploited by using partial hash collisions as tokens.

This is the approach taken by MicroMint [58], invented by Rivest and Shamir in 1997, a debit-based system which uses k -way hash collisions as payment tokens.

A k -way collision is a set of k distinct input strings which yield the same partial hash output, i.e. the outputs agree for a specific number of bits. Different combinations of these input strings are packaged into tokens which customers use for transactions. Merchants check the authenticity of tokens when accepting them by verifying the collisions, and later redeem them with the broker. It is impractical to counterfeit these tokens but they can easily be duplicated. To prevent double-spending, brokers only redeem spent tokens once.

We describe here the intuition of how collisions are generated: the broker sets up a number of storage bins to classify input strings based on their hash output, such that strings which create partial hash collisions will end up in the same bin. The authors anticipate that tokens are minted over a month-long period using special-purpose hardware optimized for hash computations, and it is highly likely that many bins will end up with multiple strings. The broker then packages strings in separate bins into individual tokens.

This system calls for substantial initial investment on the part of the broker. Researchers have since proposed optimizations for the minting process [65] [66] [67] and discussed implementation concerns [68] [69]. Some prototype implementations have also been described [70] [71].

MicroMint has not inspired many derivative schemes, but the notion of using hash function collisions has proved influential in other domains and inspired the notion of proof-of-work schemes [72] [67] which force a party to undertake computational effort in return for some privilege. Hashcash [73], a prominent example, was originally proposed to limit spam email and denial-of-service attacks and has since been adopted by Bitcoin and other cryptocurrencies.

E. Probabilistic Audit and Redemption Mechanisms

These systems reduce processing costs by probabilistically selecting and processing individual micropayments from a

set of many such that the odds of identifying fraud or fair compensation are maximized.

1) *Probabilistic Auditing*: Jarecki and Odlyzko [74] attempt to bridge the gap between solutions relying on real-time availability of the broker, like NetBill, and those which necessitate only periodic access at the end of the billing period, examples like PayWord and MicroMint. The goal is to reduce communication overhead while still detecting if the customer tries to cheat or exceed her credit limits.

The solution is for merchants to accept customer payments and use a probabilistic mechanism to determine whether or not to forward the transaction to the bank in real-time. The frequency with which payments are sent to the bank are calculated as a function of the monetary values of the transactions and the amount of risk the bank is willing to take. As transactions grow larger, therefore, the merchant contacts the bank more frequently, whereas, for low value amounts, typical of micropayments, the contact is much less.

Probabilistic auditing can simply be grafted on top of existing systems, and indeed has been proposed as extensions for the NetCents and Agora solutions.

2) *Probabilistic Redemption*: Wheeler initially floated the idea that **weighted bets** could efficiently amortize transaction costs [75]. A simple illustration: for Alice to make a payment of 37 cents currently requires a transfer of at least four coins. Furthermore, lets assume that Alice only possesses dollar bills. One solution is to toss a 100-sided die; if it yields a number between 1 and 37, Alice pays a dollar to the merchant, and if not, she gives him nothing. If this transaction is repeated often enough, the average payment Alice makes to the merchant is 37/100 dollars, i.e. 37 cents.

Rivest's lottery-based scheme [76], developed in 1997, extends this notion to PayWord. In this case, the bank issues Alice with a book of "lottery tickets" essentially consisting of a PayWord chain with a specified lifetime. As with a PayWord purchase, Alice uses successive values in the chain as payment tokens and the merchant verifies each token accordingly before sending over the corresponding items.

After the lifetime of the chain expires, the bank announces that one individual lottery ticket in each book is a "winning" ticket. If Alice has transferred this ticket to the merchant in the course of her purchase, she is obligated to pay. In this case, the merchant presents the winning ticket to the bank which debits Alice's account for the full value of her purchase and credits the amount to the merchant's account. However, if Alice retains the ticket (i.e. she hasn't spent it), she pays nothing. In the long run, when thousands of such transactions have happened, the probability is very high that the amount Alice is charged will converge to the actual amount she owes the merchant. Processing costs are minimized because the bank only has to process winning tickets.

This scheme suffers drawbacks: the bank has to organize the lotteries, circulate details of winning tickets, and the merchant can only be paid after the lottery concludes. Rivest extends the protocol to address these concerns and proposes a fair

mechanism allowing Alice and the merchant to decide among themselves whether a ticket is a winning ticket or not [77].

Ostrovsky and Lipton propose a similar scheme to minimize the bank's involvement [78]. Here Alice and the merchant both exchange roots of pre-computed hash chains prior to the transaction, as well as cryptographic commitments to the seed values from which the chains are generated. In each round, both parties produce their tokens which are then XOR-ed to yield the output for the round. Since both tokens are pseudo-random values, the process is analogous to tossing a coin. Alice pays the merchant depending on the result of the toss.

Rivest revisited the topic with Micali in 2001 [79] [80] to present **Peppercoin**, a non-interactive version of the lottery scheme. In this case, winning tickets are selected by a cryptographic process: the merchant digitally signs a token and checks if the signature result is less than a pre-determined value. It is important that a deterministic digital signature scheme be used (such as RSA), so that the merchant can convince the bank that a ticket is a winning ticket. Given the cryptographic nature of digital signatures, neither Alice nor the merchant can game the system in their favour. Furthermore, to protect Alice from being charged too much at once, Peppercoin brings in banks as intermediaries, or buffers, who pay the merchant the inflated amount but charge her only the aggregated value of the payments she has made.

Peppercoin launched as a commercial system in 2001, starting services in 2003, but closed in 2007.

F. Peer-to-peer Systems

The emergence of large-scale peer-to-peer (P2P) networks in the early 2000s necessitated research on payment solutions for this new paradigm. There were two main motivations: first P2P networks suffered from the free-rider problem, i.e. certain peers would solely use network resources without contributing any themselves. One solution is to deploy a metering or micropayment solution to incentivize participation and ensure fairness in the network [81] [82].

The second reason is commercial. Networks like Napster and Kazaa suffered immense backlash and heavy litigation from the recording industry for freely sharing pirated content, leading researchers to examine possibilities for transitioning these networks to legal marketplaces.

PPay [83], presented by Yang and Garcia-Molina in 2003, is one of the earliest and most influential P2P micropayment systems. PPay is a debit-based protocol that adapts several innovations from past systems to a P2P environment.

In the PPay ecosystem, a broker issues coins to Alice which are essentially certified vouchers of fixed denomination, bearing identifying information such as a unique serial number and Alice's identity. To make a payment, Alice prepares a reassignment message, consisting of identity of the merchant, the coin's information, and an assigned sequence number which increments every time the coin changes hands. Alice signs this message and sends it to the merchant who then becomes the official 'holder' of the coin (as opposed to Alice who is the 'owner' of the coin).

The merchant may then use the coin, in the role of a customer, to make a purchase from another merchant. In this event, he sends Alice a reassignment request, i.e. a digitally signed message with details of his last transaction with Alice and the identity of the new merchant. Alice prepares and sends back to both a reassignment message with the identity of the new merchant and incrementing the assigned sequence number. Alice also logs the reassignment request, as evidence that the first merchant relinquished the coin. The broker is only approached when users want to cash out of the system.

PPay has considerable strengths: first, broker involvement is considerably reduced as coin owners manage security of the coin. All messages are digitally signed by all parties, thereby enabling forensic analysis later on to identify any instances of double-spending or fraud.

However, there are also some weaknesses: coin owners are required to be online to facilitate transactions. A solution, the authors suggest, is to enable coin holders to issue reassignment messages themselves which are ‘appended’ to the coin, giving rise to the notion of “layered” coins. Each layer is a new reassignment message, which can be “peeled” back later on to validate the provenance of the coin by verifying signatures and sequence numbers. Another alternative is to allow brokers and coin-owners to conduct probabilistic audits of transactions and reassignment requests.

PPay has proved immensely popular and several schemes have built on its basic features. A notable example is **WhoPay** [84], by Wei et al. which provides revocable anonymity to coin holders (not owners) by employing group signatures. The identity of the current coin holder is concealed as one within a group but, in exceptional circumstances, may be unmasked by cooperation of the broker and a trusted authority. Coins are not represented by serial numbers but by public keys, such that the owner of the corresponding private key is the holder of the coin. For each transaction, the merchant generates a new public/private key pair, and the original owner signs the coin along with the new public key, to designate the reassignment. The authors also suggest a public log for all transactions which peers can check in real-time to detect double-spending.

FairPeers [85] [86], by Catalano and Ruffo, adapts PPay for selling copyright content. A Copyright Granter entity, issues digital certificates testifying to the authorship of a file. A merchant offers to sell the file. To purchase it, Alice will need two different coins, one sent to the merchant and the other to the original author of the file. Unfortunately, in this scenario the requirement that authors always be online for payments can be problematic. Some solutions are considered in [87].

Another influential system, **Karma** [88], addresses the free-rider problem in a decentralized manner. Coins are replaced with the concept of *karma*. A new node, say Alice, entering a P2P network is associated with a set of peers (called the *bank-set*) which act as a semi-trusted authority, tracking the resources Alice consumes and contributes, and maintaining a record replicated across all the peers. When Alice makes a transaction with a merchant by transferring him an amount of karma, all the peers in her bank-set send messages to

all the peers in the merchant’s bank-set, testifying to Alice’s balance of karma, thereby validating the transaction. The merchant’s bank-set uses a majority voting protocol to confirm the transaction is in order, and the merchant then sends Alice her purchased items. This system assumes that the majority of peers in the network are honest.

A drawback of Karma is that bank-set peers need to be online to validate transactions. This limitation is addressed by **Offline-Karma** [89], where each reassignment adds a new “layer” of provenance to a coin. Coins have a fixed lifetime after which the layers are peeled back to check for double-spending and fraud. This function is undertaken by a distributed set of nodes, known as the reminders, who then affix a multisignature to the coin, re-certifying it for use.

CPay [90] takes a different route to resolving the peer-availability problem. Instead of relying on multiple peers to authorize a transaction, the customer runs a function to select one peer from a set of online peers who have been designated Broker Assistants by the broker. The Broker Assistant then verifies the transaction.

Other P2P schemes in this vein include Zuo and Li’s Fair Exchange File Market [91], which describes how to integrate a payment solution between customer and merchant in a BitTorrent-type scenario where file pieces are distributed among multiple peers and have to be retrieved. Attacks on this system are described in [92] [93]. P2P-NetPay [94] adapts the PayWord-based NetPay protocol described earlier for P2P networks. A prototype implementation is described in [95].

The most popular and influential system in this category though is undoubtedly Bitcoin. Developed by Satoshi Nakamoto in 2008, **Bitcoin** has achieved mainstream success and is currently the world’s leading cryptocurrency with a market cap of around \$11 billion [96]. Bitcoin brings together and harmonizes several of the innovations we have discussed thus far: the currency units, bitcoins, are essentially floating vouchers. Users maintain a public/private key pair. A hash of the public key is considered the user’s ‘Bitcoin address’. To make a payment the user digitally signs a transaction message using her private key and the balance of bitcoins is transferred to the receiver’s Bitcoin address.

Bitcoin’s most important innovation is the blockchain, a distributed public ledger which records all transactions on the network and enables peers to detect double-spending. This is literally a chain of blocks, each of which contains recent transactions. A decentralized set of miners is responsible for the creation of new blocks and they compete among themselves to solve a computationally difficult puzzle. The winner creates and appends the next block in the chain. This leads to Bitcoin’s second innovation, a monetary reward that incentivizes miners to maintain the Blockchain.

A detailed description of the Bitcoin payment system goes beyond the scope of our paper (interested readers are directed to [97]). We note in brief some key properties of the system. Most importantly, the network is distributed and trustless, i.e. no centralized broker or bank is required to authorize transactions or check for fraud. Bitcoin users transact using

pseudonyms which confers a degree of anonymity, but research has evolved methods to attack it [98]. Bitcoin transactions generally include a transaction fee (typically in the order of cents or lower) to incentivize miners to include the transaction in the blockchain. An important distinction here is that transaction fees are not a function of payment amount but rather depend on the amount of data in the transaction.

Bitcoin is described as a general payments system but its relatively low transaction fees qualifies it as a micropayments system in its own right. Indeed several commercial micropayments systems (some of which are described in Sec. IV) already use the Bitcoin network to process payments.

However, researchers have innovated mechanisms to further drive down processing costs using Bitcoin. We consider some of these next.

G. Enabling Micropayments on Bitcoin

The most straight-forward approach to limit transaction fees is to amortize transaction costs by conducting **off-chain transactions** and only settling their accounts on the Bitcoin network. The easiest way to achieve this is by introducing a broker like ChangeTip or Coinbase to maintain accounts for customer and merchant on their own system. However, this strategy is not recommended: Bitcoin exchanges have a notoriously poor track record of protecting customers' funds [99]. We discuss this point in more detail in Sec. V-A.

Protocols have been proposed to enable off-chain transactions without a trusted third party [100]. Referred to as **micropayment channels**, these solutions rely on the blockchain to resolve payment disputes. We consider an example: two users wishing to transact set up a channel by depositing funds into a special transaction which is then stored on the blockchain. Access to the funds is prohibited without authorization of both parties. The users then make multiple low-volume transactions to each other privately off-network which effectively redistribute this deposit among themselves. To terminate the channel and redeem their funds, either party can broadcast the last transaction they exchange on the Bitcoin network. As a safety mechanism, the initial transaction bears an expiry time, after which, if no payments have been made, the deposit is automatically refunded.

We briefly describe some basic micropayment channels:

A **uni-directional channel** permits micropayments to be made strictly in one direction only, that is from one user to another. Only the sender has to make the initial deposit onto the blockchain. Each micropayment then increases the receiver's share of the deposit. The amount of the deposit sets the upper limit on the funds the sender can transfer to the receiver for the session.

Interestingly, timers can extend support for **bi-directional micropayments**. The timer determines the minimum block height at which the transaction is accepted into the blockchain and setting the appropriate timer value ensures that one transaction takes precedence over others. In this case, when the sender makes a payment and the receiver wishes to make one back, the sender can broadcast another transaction reducing

TABLE I
CLASSIFICATION OF CRYPTOGRAPHIC SYSTEMS

Scheme	Strategy	Properties			Payment	
		Anonymity	Guaranteed Delivery	Non-reputation	Pre-paid	Post-paid
Chrg-http	Centralized				●	
NetBill	Centralized		●	●	●	
Millicent	Voucher-based				●	
Netcents	Voucher-based				●	
Agora	Commitment-based	⊖	⊖	●		●
Mini-pay	Commitment-based	⊖	⊖	●		●
Payword	Crypto-tokens			●		●
PayTree	Crypto-tokens			●		●
NetPay	Crypto-tokens			●	●	
MicroMint	Crypto-tokens	●			●	
Peppercoin	Probabilistic			●		●

the balance of his last transaction by the appropriate amount. Decrementing the timer value ensures the second transaction with the amended balance is included in the blockchain and the first is not.

Poon and Dryja propose **Lightning Channels** [101] that supports bi-directional payments with infinite lifetime. The channel has an active transaction representing the current balance of both users and a list of revoked transactions. Sending a micropayment entails revoking the active transaction and replacing it with a new one that represents the new balance of both parties. If a user circulates a previously revoked transaction on to the Bitcoin network, the other user has a time-period to broadcast a penalty transaction and acquire all the bitcoins in the transaction. Either party can close the channel by broadcasting the latest active transaction or both parties can co-operate to settle the final balance.

Other approaches are being developed independent of off-network micropayments channels: for instance, **MicroPay** [102] provides a version of probabilistic payments system that is compatible with Bitcoin. Recent research proposals have also attempted to extend ZeroCash, a new and more privacy-conscious cryptocurrency, to support micropayment channels and probabilistic payments in the offline setting [103].

H. Discussion

There is a clear evolutionary trend in the systems we have thus far examined. Early systems like Millicent, Agora, PayWord, and MicroMint, showcase a variety of broad innovative approaches towards micropayments. There is considerable cryptographic innovation with an emphasis on security and efficiency. Later systems, such as P2P systems are more application-oriented and tend to synthesize these different approaches.

We also observe a visible shift in design priorities and limitations as technology advances and infrastructure improves. Early schemes like Millicent and PayWord went to great

lengths to minimize usage of digital signatures and transaction latency whereas P2P schemes have no such restrictions.

IV. COMMERCIAL SOLUTIONS

We examine a selection of commercial micropayment systems that are currently in use, or have had significant impact.

We divide these systems into four categories: in pre-paid systems customers deposit funds into their accounts which they then progressively spend. Several systems facilitate payments in various ways, either by allowing an existing payment method to be used in a new area, or enabling customers and merchants to manage their payments and purchases better. Other systems amortize transaction costs by aggregating multiple payments into smaller numbers of transactions. Many of these systems support both small and large payments, and the target markets and benefits they provide differ considerably.

A. Pre-paid Systems

These systems involve a user making an advance payment to the payment provider via cash or credit/debit card. This payment is converted into funds inside the system which can be used to pay participating merchants.

Paysafecard [104], launched in 2000, is a system based around pre-paid scratchcards. Customers buy scratchcards in advance that have a value (€5, €10, €25, €50 or €100) and a 16 digit PIN. When the customer makes a payment she enters the PIN to authorise the payment. If there is not enough balance on the card for the whole payment she can enter additional PINs and use up to 10 cards.

Merchants receive monthly payments from paysafecard that combine all of the transactions made for that month, thereby reducing processing costs. Transaction fees depend on the location and business area of the merchant.

PayPal [105], established in 1998, is an account-based system where users deposit and withdraw money via credit/debit card. Transactions are made in real-world currencies and merchants pay fees for every transaction that occurs.

PayPal has special merchant accounts for micropayments. These accounts function like normal merchant accounts, but have a different transaction fee structure, charging \$0.05 plus 5% of the transaction. Normal merchant accounts charge \$0.30 plus 2.9% of the transaction, with the possibility for merchants with large transaction volumes or non-profit status to negotiate a fee as low as \$0.30 plus 2.2% of the transaction.

PayPal also offers direct carrier billing for customers whose mobile service providers are part of the PayPal carrier network. The PayPal carrier network has a wide coverage worldwide due to PayPal's acquisition of direct carrier billing company Zong and partnership with Deutsche Telekom.

Flattr [106], launched in 2010, is a system enabling users to support content creators such as artists, musicians or writers. The user sets a monthly budget which is pre-paid into the system by bank transfer or credit/debit card each month. The user also maintains a list of people they choose to support. Each month the monthly budget is divided equally among the people on the list.

As only one payment is taken each month, only one transaction cost is accrued, regardless of the number of people on the list. Similarly, content creators are given one monthly payment combining all of the payments sent to them by users during that month. This reduces the fixed portion of the transaction fees to one fee per user and one fee per content creator, a significant reduction when users are paying small amounts to many content creators.

Flattr also reduces mental transaction costs, as users do not have to decide how much to pay each creator, instead simply adding people to the list when they see something they like, and removing people they no longer wish to support.

ChangeTip [107], founded in 2013, is designed to allow users to make small one-off payments to people, businesses and organizations they wish to support. Users deposit money into their accounts via Bitcoin or credit/debit card. Transfers of any amount from one user to another are free and withdrawals are charged a small transaction fee, set at different levels for dollars and bitcoins.

As with Flattr, ChangeTip amortizes processing costs as one large transaction deposits money into the system and enables multiple small payments to be made without further costs.

Click and Buy [108], founded in 1999, is an account-based system where customers deposit money via credit card and bank transfer. A 3.9% transaction fee is levied for credit card deposits, with bank transfer deposits being free of charge. Merchants are charged both a fixed fee per transaction and a percentage of their total revenue. The amount charged is based on the average transaction amount, with merchants who generally receive smaller amounts per transaction having a smaller fixed fee and a larger percentage than merchants who generally receive larger amounts per transactions.

Merchants can opt to be paid by Click and Buy on a schedule ranging from once a day to once every 30 days, with merchants who opt for longer payment schedules being rewarded by smaller transaction fees.

M-Pesa [109], founded in 2007 is a mobile phone-based account-based system where users can deposit and withdraw money through businesses acting as agents. Users can transfer money both to other users and non-users.

M-Pesa's largest market is Kenya, where direct transfers to and from bank accounts are possible. The system is also available in a number of other countries. Transaction fees are based on transaction size, with a fixed charge being levied for transfers within particular size categories. Different transaction fees are charged for transfers to users and non-users.

League of Legends [110], released in 2009, is one of the most popular online games and uses a free-to-play model. Revenue is generated by the sale of in-game upgrades to players. These upgrades are bought with Riot Points, a currency used only for this purpose. Riot Points can be purchased with credit/debit cards, PayPal, paysafecard, bank transfer or using pre-paid cards from a variety of retailers. Transaction fees are kept low by selling Riot Points in relatively large blocks, so that the lowest purchase price is between \$2.00 and \$10.00, depending on the purchase method.

As with most in-game currencies, Riot Points are not convertible into other currencies, and players are generally prevented from selling or transferring their points to others.

Blendle [111], founded in 2013, is a news aggregation site that sells articles using a pay-per-article model. Customers deposit funds into their Blendle account using a credit card, and then buy access to articles or entire editions of periodicals. Content providers are allowed to set a price (currently between €0.99 and €1.99) for each article they provide, with Blendle charging a fee of 30% of this price to the merchant.

Blendle allows customers a refund on any article they have purchased, with the requirements that the customer requests the refund within 24 hours and provides a reason for it. This step is designed to prevent customers paying for articles that were misleadingly advertised or badly written.

The **Starbucks card** [112] is an account-based system that allows customers to buy beverages and food from Starbucks. Customers begin by buying a physical card with a pre-loaded value. This card has a unique card number and security code that are stored in a central database along with the balance on the card. The balance can be spent at Starbucks stores like a traditional gift card. The card can even be registered online as belonging to a particular user.

A registered card can have additional value added to it in-store or online, and registered users can also download iPhone and Android applications that allow the mobile device to be used in place of the card. Users are also able to transfer value to other registered cards, allowing the Starbucks card to be used as a form of currency among users, and use of a registered card is linked to a customer rewards program.

Bitwall [113], is a system designed to allow the purchase of access to web content. The system is currently in beta stage and the pricing model is still being determined. At present users can buy access to one article for \$0.01, 24 hour access to an entire site for \$0.03 or 3 hour access to the site by advertising the site on Twitter. Payments are made via Bitcoin, using the current Bitcoin to US dollar exchange rate.

Mondex, VisaCash, Proton and Octopus are systems based around a smart-card that is pre-loaded with funds and used to make in-person payments. Of the four, only Octopus [114], launched in 1997, has achieved commercial success, being used heavily for public transport, car parking charges, fast-food and vending machine purchases in Hong Kong. Octopus cards can be reloaded with funds using cash at a range of participating retailers, and can also be linked with a credit card using the “Automatic Add Value Service,” causing funds to be added whenever the card reaches zero balance.

Merchants are charged a percentage of each transaction for the use of Octopus (this percentage can vary between merchants and the factors that decide the percentage charge are not publicly available) but no fixed transaction cost.

B. Facilitating Merchants

These systems improve the ease with which merchants can accept payments. They generally work as gateways or aggregators, enabling merchants to collect payments from

multiple systems without having to hold accounts with each, thereby reducing both expense and effort for the merchant.

Mollie [115], founded in 2004, is a payment gateway allowing payments to be made by various means into one account. It does not provide a micropayment system of its own, but instead allows merchants to accept payments by credit card, PayPal, Bitcoin, paysafecard and various bank transfer systems. Fees depend on the payment method used, with most methods including a fixed fee of €0.25.

Previously, Mollie allowed customers to make payments via SMS or by calling telephone numbers, with the payment amount being added to their telephone bill. This payment method is no longer offered.

C. Facilitating Customers

These systems use technology to improve the payment experience for customers.

Android Pay [116], established in 2015 is an Android device-based system that can store credit card, debit card and other card details and enables secure payment via NFC or over the Internet. **Apple Pay** [117], established in the US in 2014, is a similar offering based around Apple technology.

Merchants require a payment processor for the underlying card and are only charged for the card used; Android Pay and Apple Pay do not add any additional fees. While these systems change the user experience and the security properties of the transaction, they do not change the fee structure of the underlying payment method.

Paym [118] is a system allowing payments between individuals who are identified by their mobile telephone numbers. Both parties in a transaction must have bank accounts with participating UK banks, and both parties must have registered their mobile phones with the Paym system. The payment sender can then use the Paym mobile app to make a payment to the recipient, by entering the amount and the recipient’s mobile telephone number.

At present Paym payments bear no charge, but many banks restrict use of the system with business accounts or levy charges on transfers to and from these accounts.

D. Aggregation

These systems combine multiple payments together where possible to minimize the transaction fees charged by payment processors.

iTunes [119], founded in 1998, accepts standard credit and debit card payments. Payments are often delayed by a short time (such as one or two days) to increase the likelihood that the customer will make further purchases. All of the payments are then lumped together before clearing them to reduce transaction fees.

eMusic [120], initially founded in 1995 and relaunched in 2004, uses a business model that can be thought of as a combination of aggregation and pre-paid systems. Users choose a monthly payment level, which then entitles them to download a number of songs during that month. One transaction is made by debit/credit card for the monthly payment, resulting in a

TABLE II
SYSTEM PROPERTIES

System	Target Market	Pre-paid	Anonymity	Accepts Cash
paysafecard	Online markets	●	●	●
PayPal	Online markets	●		
Flattr	Flattr users	●		
ChangeTip	ChangeTip users	●		
Click and Buy	Online markets	●		
M-Pesa	All payments	●		●
Points	LoL upgrades	●		●
Blendle	Online articles	●		
Starbucks Card	Starbucks products	●		●
Bitwall	Online articles	●		
Octopus	In-person payments	●		●
Mollie	Online markets			
Apple Pay	Online markets			
Android Pay	Online markets			
Paym	Money transfers			
iTunes	iTunes store			
eMusic	eMusic store	●		

guarantee that only one transaction fee will be paid to the payment processor each month.

This system forces users to commit to buying a certain number of tracks each month, allowing more aggregation of purchases than may occur with a more flexible system.

E. Summary

The commercial systems we have listed all appear to have grown around a specific problem or application, rather than being formulated to produce a general micropayment system. The majority of the systems do not provide anonymity, with paysafecard as the notable exception (with the possibility for anonymity by a technically skilled user in the cases of Bitwall and League of Legends Riot Points). Privacy is generally handled by policy rather than technical safeguards. The system properties are summarised in table II.

It is also notable that none of these systems rely on novel cryptographic protocols for properties like non-repudiation of transactions or to prevent double spending. Instead, all of the systems are account-based, relying on a trusted third party to authenticate transactions. Even paysafecard, which doesn't rely on a traditional notion of an account, requires a central authority to distinguish between valid and invalid PINs.

V. OUTSTANDING CHALLENGES AND FUTURE DIRECTIONS

Here we outline key challenges facing design and deployment of micropayments systems. Payments systems today are particularly vulnerable to security threats and we present relevant insights from the Bitcoin experience. We then consider ethical and legal issues that need to be resolved to integrate micropayments successfully into the financial infrastructure.

This is followed by a discussion of cognitive costs and mental models for micropayments. There is very little work

done in this domain, and we anticipate that research may enable improved usability for micropayments systems and successful business models. In conclusion we discuss potential deployment strategies for upcoming micropayments systems.

A. Security Challenges

Security is a pronounced concern for online payments systems in general. A 2013 report by CyberSource calculates that for online shopping with card in the UK, i.e. the card-not-present paradigm (CPN), the fraud rate dominates and is about ten times higher than for physical credit card fraud [121]. A concurrent study by FICO discovered that the US credit card fraud rate is spiking, surging 17% over two years [122].

The trend is even more ominous in the Bitcoin community [123]. A key reason why Bitcoin's transaction fees are so low is that the systems has no fraud protection or dispute resolution mechanisms. Bitcoin exchanges, marketplaces, and wallet services are routinely hacked, resulting in thefts and losses of hundreds of thousands of customers' bitcoins. Mt. Gox is a most prominent example: the world's largest Bitcoin exchange lost over half a billion dollars worth of bitcoins in an incident, impacting user confidence in the currency itself. One study documents that of 40 Bitcoin exchanges established recently, 18 shut down soon after [99].

In parallel, researchers from Dell indicate a near ten-fold increase in malware designed to steal bitcoins from users' computers, the rate of creation loosely tracking the increase in Bitcoin's own exchange rate [124]. Some of these even employ keyloggers to crack password-protected wallets. 50% of these malware successfully bypass most antiviruses.

Micropayments systems are particularly vulnerable because system security is not an isolated feature. Instituting fraud protection mechanisms in a system will almost certainly add to payment processing costs and cut into the broker's profit margins. This increase can be justified for macropayments; for instance, debit card transactions in the US average \$39 per transaction and the interchange fee is about 24 cents per transaction of which 1 cent goes to fraud protection [125]). But for very low-value payments, this increase is significant.

A related concern is that adding a fraud protection feature to a system will likely impact system usability and add further cognitive burdens on the user. For example, a user may be amenable to the extra "hassle" of two-factor authentication for making a macropayment, but for very low-value transactions, the amount might not justify the effort.

Any solution addressing security for micropayments systems will have to harmonize these concerns.

B. Legal and Ethical Concerns

Micropayment systems, like most real-world applications, will require legislative protection as well. Some scenarios simply cannot be prevented with technology alone (for instance the supply of defective goods in a conventional e-commerce scenario) and others may be independent of technology (such as assigning liability if a payment system suffers losses due to faulty implementation or mismanagement). Legislators need to

decide how best to balance interests of users and merchants, and merchants and brokers have to decide if there is a business case to absorb more risk themselves in the interest of gaining market share and consumer confidence.

New payment systems may also introduce the risk of losses beyond what the system can absorb. Bitcoin exchanges have shown that it is possible for a company to suffer losses far in excess of its assets when things go wrong [126]. This has troubling implications for consumer confidence and is an important concern for both legislators and businesses.

Legislators also have a role in regulating payments systems and preventing customer exploitation. Recent EU legislation has capped interchange fees for using credit and debit cards at 0.3 and 0.2 % respectively [127]. It has also required that card processors provide information to consumers about costs associated with each transaction and a breakdown of the fees. Micropayments systems will require similar oversight.

There are privacy issues as well. Already, concerns have been voiced about companies amassing and monetizing user data [128]. A good example is Octopus (discussed in Sec. IV): in 2010, the Hong Kong Privacy Commissioner for Personal Data found Octopus Rewards Ltd. to have breached data protection principles with regard to the sale of customer data to business partners for direct marketing purposes [129].

As we observed in Sec. III-IV, very few micropayments systems offer the user anonymity from both merchant and broker. If micropayments are used to purchase individual articles, videos or audio recordings then users' purchase histories can leak sensitive information such as their political inclinations, religious values and sexual preferences.

However, strict anonymity also poses a problem for governments. While many governments might wish to protect the privacy of their citizens, at the same time there will generally be legislation against large anonymous payments, as part of money laundering and anti-terrorism legislation.

Anonymity becomes even more of a concern in the digital-only, 'cashless' vision of society emerging in countries like Denmark, Sweden, and Finland [130]. As digital payments become commonplace, banks and payment processors can blacklist parties for political reasons. A real-world example of a payment blockade occurred in 2010 when US companies refused to process payments sent to Wikileaks [131].

Discovering ways to allow massively scalable micropayments systems which protect customer privacy and free speech while at the same time preventing tax evasion and terrorism financing is both a legislative and technological challenge.

C. Micropayments and Psychology

As we noted in Sec. II, payments systems impose mental transaction costs, i.e. the cognitive effort involved in deciding whether an item is worth buying or not, regardless of price. These costs arise due to various reasons: for instance, a large variety of choices can pose a mental bottleneck. As an example, it is simply less mental effort for a user to buy a whole newspaper for a set amount than to compare the

TABLE III
CHANGE TIP AMOUNTS

Label	Amount	Currency
Beer	3.50	USD
Buck	1.00	USD
Cent	0.01	USD
Cerveza	3.50	USD
Coffee	1.50	USD
Cookie	1.50	USD
Dime	010	USD
Dollar	1.00	USD
Donut	0.35	USD
Euro	1.00	EUR
Gold-star	0.50	USD
High-five	5.00	USD
Nickel	0.05	USD
Pie	3.14	USD
Pint	3.50	USD
Quarter	0.25	USD
Quid	1.00	GBP

anticipated merits and prices of individual articles. This may explain the appeal of flat fees.

In an influential position paper on the topic, Szabo [7] contends that as prices go down, these mental costs tend to dominate over technological costs, they set the effective lower bound on pricing of goods, and therefore, may play a determining role in the adoption of micropayments systems.

Szabo makes some recommendations for systems developers. First, rather than focus on technological innovation alone, it is imperative to recognize mental transaction costs. Technology may then be applied to alleviate these costs.

One proposed approach is to employ metaphors to simplify the mental effort involved in making choices. We present here an example employed by ChangeTip (described in Sec. IV) which presents users with payment options labelled as real-world items of similar cost (shown in table III). For example, a user can choose to reward a party by "buying them a coffee", press the requisite button, and the system will transfer the corresponding amount of money. Users may also define their own custom amounts on ChangeTip.

Branding and quality control is another approach. If a brand consistently delivers good quality for money, users may be more inclined to trust its product and exert less mental effort in choosing to buy it. One way to implement this would be the strategy taken by Blendle (described in Sec. IV), which is to offer readers an easy refund option on purchased articles as a way to reward quality content.

Unfortunately there has been very little research done on mental models for micropayments systems to date. This is a widely neglected area that could use input from the fields of psychology, human-computer interaction (HCI), and behavioral economics. Understanding the psychology behind micropayments will not only improve system usability but also assist in crafting appropriate business models and successful deployment strategies.

D. Business Models and Deployment

There are important open research questions regarding pricing for a micropayments ecosystem. For example, is there perhaps a pricing threshold at which micropayments become viable? While there is currently no definite answer to this question, there may be some evidence for it. The Chicago Sun-Times launched a Bitcoin-based micropayment donation option for 24 hours in February 2014 and collected over 700 payments, ranging from a penny to over \$ 1000 [132]. 63% of these payments were for 25 cents, the apparent “sweet spot”.

The question of how to optimally monetize digital goods and services is itself an open and active area of research. Novel business models are emerging for digital content beyond the traditional subscription and pay-as-you-go paradigms and interesting results are being reported. We present a brief overview on this topic in Appendix A. Readers interested in a more detailed discussion on this topic are referred to surveys [133] [134].

Regarding mass deployment of micropayments system, there are certain desirable properties a system should have that would great help with success. For instance, a micropayments solution should be inter-operable across a wide range of merchants and integrate with existing payment infrastructures. Not only does this give consumers more opportunities to use the solution, but it will also open up new sources of revenue for merchants.

Standardization is an essential step in that direction, and that has been recognized by the W3C who have renewed their efforts in this direction with the recent launch of the Web Payments Working Group (described in Appendix. B). An alternative proposal is to interconnect different micropayments systems using payments gateways, allowing conversion, collaboration and interoperability [135].

The current marketplace also requires that any solution should be supported on multiple platforms. This is for two reasons: the customer should not be restricted to only being able to make micropayments on a single platform only (this was a marked drawback of certain first-generation schemes like Millicent). Second, to cut down on roll-out costs and the network effects problem, Odlyzko suggests that it is a good strategy to piggyback micropayments onto an existing and widely-used infrastructure [9]. Mobile phones are an ideal candidate. Smartphone usage is high and phones now support considerable more resources (computing, memory, bandwidth). Currently there is also a tremendous opportunity here for merchants: a Gartner study [136] predicts that by 2017, mobile payments will make up to 50% of e-commerce revenue in the United States. Goldman Sachs predicts that by 2018 mobile phone purchases will constitute 50% of e-commerce globally [137].

This may help address the chicken-and-egg problem with micropayments systems. Users are more likely to trust and adopt new payment systems if they have a positive reputation [138], but merchants are reluctant to adopt new payment systems unless they are widely used. Piggybacking micropay-

ment solutions onto the mobile phone infrastructure (or social media) may solve this problem.

VI. CONCLUSION

In this paper we have undertaken a detailed survey of micropayments systems. We discuss their security properties and briefly document their development. Next we classify the multitude of research-based cryptographic and commercial systems as per their salient features and describe in detail the workings of representative solutions and highlight the intuition behind them. This is followed by a discussion of outstanding challenges for micropayment systems, important gaps in research, and relevant recommendations.

Our intention in this paper has been not just to provide a comprehensive technical resource, but also to highlight lessons from the past and articulate promising new directions. For this reason, we do not restrict our study to the cryptographic literature, but bring together and systematize critically important insights from a variety of fields impacting micropayments.

We hope our work has a positive impact on the future development of these systems.

REFERENCES

- [1] Stephen Hart. Breakdown of credit and debit card fees, September 2014. <http://www.cardswitcher.co.uk/2014/09/breakdown-of-credit-debit-card-fees/>.
- [2] Carsten Schmidt and Rudolf Müller. A framework for micropayment evaluation. *Netnomics*, 1(2):187–200, 1999.
- [3] Frank Fisher. Saving journalism, a farthing at a time, 18 May 2009. <http://www.theguardian.com/commentisfree/2009/may/18/news-online-payment-journalism>.
- [4] Ben Sisario. As Music Streaming Grows, Royalties Slow to a Trickle, 28 Jan. 2013. <http://www.nytimes.com/2013/01/29/business/media/streaming-shakes-up-music-industry.html>.
- [5] Michael Lesk. Micropayments: An idea whose time has passed twice? *Security & Privacy, IEEE*, 2(1):61–63, 2004.
- [6] R Parhonyi. Micropayment systems. *Handbook of Financial Cryptography and Security*. CRC, 2011.
- [7] Nick Szabo. Micropayments and mental transaction costs. In *2nd Berlin Internet Economics Workshop*, 1999.
- [8] Clay Shirky. The case against micropayments. *OpenP2P OReilly*, 2000.
- [9] Andrew Odlyzko. The case against micropayments. In *Financial Cryptography*, pages 77–83. Springer, 2003.
- [10] Brandon Griggs. Apple’s App Store hits 50 billion downloads, May 15 2013. <http://edition.cnn.com/2013/05/14/tech/web/itunes-50-billion/>.
- [11] Rob Price. The App Industry Is Bigger Than Hollywood, 22 Jan. 2015. <http://uk.businessinsider.com/app-industry-hollywood-comparison-2015-1>.
- [12] Andy Chalk. League of Legends has made almost \$1 billion in microtransactions, 24 Oct. 2014. <http://www.pcgamer.com/league-of-legends-has-made-almost-1-billion-in-microtransactions/>.
- [13] Jeff John Roberts. Ad-blockers could cut enterprise data load 25%, study suggests, 8 July 2015. <http://fortune.com/2015/07/08/adblock-data/>.
- [14] Felix Salmon. Ad tech is killing the online experience, 19 July 2015. <http://www.theguardian.com/media/2015/jul/19/ad-tech-online-experience-facebook-advertising>.
- [15] Farah Chanchary and Sonia Chiasson. User perceptions of sharing, advertising, and tracking. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, 2015.
- [16] Lalit Agarwal, Nisheeth Shrivastava, Sharad Jaiswal, and Saurabh Panjwani. Do not embarrass: re-examining user concerns for online tracking and advertising. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 8. ACM, 2013.
- [17] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 4. ACM, 2012.
- [18] Online Consumer Privacy Study, Q2 2013. <http://www.annalect.com/annalect-q2-2013-online-consumer-privacy-study/>.

- [19] The cost of ad blocking, 2015. http://downloads.pagefair.com/reports/2015_report-the_cost_of_ad_blocking.pdf.
- [20] John Naughton. Is this really the beginning of the end for web ads?, 23 Aug. 2015. <http://www.theguardian.com/commentisfree/2015/aug/23/beginning-of-the-end-for-web-ads>.
- [21] Rachel Stern. From 10 Cents Per Article: Micropayments For Journalism, June 5 2015. <http://en.ejo.ch/media-economics/business-models/from-10-cents-per-article-micropayments-for-journalism>.
- [22] Walter Isaacson. Big Idea 2015: The Coming Micropayment Disruption, Dec. 22 2014. <http://time.com/3636720/2015-micropayment-disruption/>.
- [23] Gill Plimmer. Britons more willing to pay for online content, 26 May 2013. <http://www.ft.com/cms/s/0/48e73568-c5fb-11e2-99d1-00144feab7de.html#axzz3p7V4u0B>.
- [24] Anne Lu. More Consumers Are Willing to Pay for Streamed Content, 30 May 2015. <http://www.ibtimes.com.au/more-consumers-are-willing-pay-streamed-content-1450359>.
- [25] Hugh Radojev. Pennies has now raised 7.5m through 32 million micro-donations, Sept. 9 2016. <https://www.civilsociety.co.uk/news/pennies-has-now-raised-7-5m-through-32-million-micro-donations>.
- [26] Cassandra Khaw. Nine major banks working on Bitcoin-like block chain tech for market trading, 16 Sept 2015. <http://arstechnica.com/business/2015/09/nine-major-banks-working-on-bitcoin-like-block-chain-tech-for-market-trading>.
- [27] Lara O'Reilly. The New York Times, Wall Street Journal, and The Washington Post have signed up with a startup that lets readers pay to read individual articles online for 20 cents each, 12 March 2015. <http://uk.businessinsider.com/the-new-york-times-wall-street-journal-the-washington-post-sign-up-to-read-individual-articles-online-for-20-cents-each-2015-3>.
- [28] Josh Horwitz. A like button with cash attached: Chinas WeChat offers the option to tip writers for posts, 13 Aug. 2015. <http://qz.com/478732/a-like-button-with-cash-attached-chinas-wechat-offers-the-option-to-tip-writers-for-posts>.
- [29] Samuel Gibbs. Google Contributor: can I really pay to remove ads?, 21 Nov. 2014. <http://www.theguardian.com/technology/2014/nov/21/google-contributor-pay-remove-ads>.
- [30] Daniel Cawrey. Bitcoin's role in the future of micropayments, 30 Sept. 2013. <http://www.coindesk.com/bitcoins-role-future-micropayments/>.
- [31] Bitcoin core version 0.11.1 released. 15 Oct. 2015.
- [32] Allen Scott. Brave Browser Finally Unleashes Bitcoin Micropayments, Sept. 1 2016. <https://news.bitcoin.com/brave-browser-bitcoin-micropayments/>.
- [33] Mohit Jain and Siddhartha Lal. Peer2peer (p2p) micropayments: A survey and critical analysis. *DA-IICT, Gandhinagar*, 2008.
- [34] Anil Kumar Venkataiahgari, J William Atwood, and Mourad Debbabi. A survey of secure b2c commerce for multicast services. In *Electrical and Computer Engineering, 2006. CCECE'06. Canadian Conference on*, pages 288–293. IEEE, 2006.
- [35] M Belenkiy. E-cash. *Handbook of Financial Cryptography and Security*. CRC, 2011.
- [36] Mark S Manasse et al. The millicent protocols for electronic commerce. In *Proceedings of the First USENIX Workshop on Electronic Commerce*, volume 7, 1995.
- [37] Henrik Kniberg. What makes a micropayment solution succeed. *Institution for Applied Information Technology. Kista, Kungliga Tekniska Högskolan*, 2002.
- [38] Gérard Carat. epayment systems database: Trends and analysis. *Electronic Payment Systems Observatory (ePSO)*, 2002.
- [39] What are micropayments? <https://www.paypal.com/us/webapps/helpcenter/help/article?solutionId=FA066&topicID=&sr=ARA>.
- [40] Róbert Párhonyi. *Micro payment gateways*. University of Twente, 2005.
- [41] Markus Stadler. *Cryptographic protocols for revocable privacy*. PhD thesis, Swiss Federal Institute of Technology, 1996.
- [42] N Asokan, Matthias Schunter, and Michael Waidner. Optimistic protocols for multi-party fair exchange. 1996.
- [43] TREZOR: The Bitcoin Safe. <https://www.bitcointrezor.com/>.
- [44] Case. <https://choosecase.com/>.
- [45] Theodor Holm Nelson. A THOUGHT FOR YOUR PENNIES: MICROPAYMENT AND THE LIBERATION OF CONTENT. <http://transcopyright.org/hcoinRemarks-D28.html>.
- [46] Walter Isaacson. How Bitcoin Could Save Journalism and the Arts, 7 Oct. 2014. <http://time.com/3476313/can-bitcoin-save-journalism/>.
- [47] Ricarda Weber. Chablis-market analysis of digital payment systems. *Institutsbericht, Technische Universitaet Muenchen, Institut fuer Informatik*, 1998.
- [48] Conner Forrest. How the 'PayPal Mafia' redefined success in Silicon Valley. <http://www.techrepublic.com/article/how-the-paypal-mafia-redefined-success-in-silicon-valley>.
- [49] Lei Tang and Steven Low. Chrg-http: A tool for micropayments on the world-wide web. In *6th USENIX Security Symposium, San Jose, CA July*, 1996.
- [50] Marvin Sirbu and J Doug Tygar. Netbill: An internet commerce system optimized for network-delivered services. *Personal Communications, IEEE*, 2(4):34–39, 1995.
- [51] Michael Pührerfellner. *An implementation of the Millicent micropayment protocol and its application in a pay-per-view business model*. Citeseer, 2000.
- [52] Ernest Foo and Colin Boyd. A payment scheme using vouchers. In *Financial Cryptography*, pages 103–121. Springer, 1998.
- [53] Tomi Poutanen, Heather Hinton, and Michael Stumm. Netcents: A lightweight protocol for secure micropayments. In *USENIX Workshop on Electronic Commerce*, pages 25–36, 1998.
- [54] Eran Gabber and Abraham Silberschatz. Agora: A minimal distributed protocol for electronic commerce. In *The Second USENIX Workshop on Electronic Commerce Proceedings*, pages 223–232, 1996.
- [55] Amir Herzberg and Hilik Yochai. Minipay: charging per click on the web. *Computer Networks and ISDN Systems*, 29(8):939–951, 1997.
- [56] Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, 1981.
- [57] Neil Haller. The s/key one-time password system. Technical report, 1995. Internet draft RFC 1760.
- [58] Ronald L Rivest and Adi Shamir. Password and micromint: Two simple micropayment schemes. In *Security Protocols*, pages 69–87. Springer, 1997.
- [59] John R. Pedersen. Electronic payments of small amounts. In *Security Protocols*, pages 59–68. Springer, 1997.
- [60] Ralf Hauser, Michael Steiner, and Michael Waidner. *Micro-payments based on iKP*. Citeseer, 1996.
- [61] Ross Anderson, Charalampos Maniavas, and Chris Sutherland. Net-carda practical electronic-cash system. In *Security Protocols*, pages 49–57. Springer, 1997.
- [62] Sunhyoung Kim and Wonjun Lee. A pay word-based micropayment protocol supporting multiple payments. In *Computer Communications and Networks, 2003. ICCCN 2003. Proceedings. The 12th International Conference on*, pages 609–612. IEEE, 2003.
- [63] Charanjit S Jutla and Moti Yung. Paytree: "amortized signature" for flexible micro-payments. *IACR Cryptology ePrint Archive*, 2012:10, 2012.
- [64] Xiaoling Dai and John Grundy. Netpay: An off-line, decentralized micro-payment system for thin-client applications. *Electronic Commerce Research and Applications*, 6(1):91–101, 2007.
- [65] David Wheeler. Micromint extensions. *Notes*, 1996.
- [66] David Wagner and Ian Goldberg. Parallel collision search: Making money the old-fashioned way the now as a cash cow. *unpublished report*, 1997.
- [67] Markus Jakobsson and Ari Juels. Proofs of work and bread pudding protocols. In *Secure Information Networks*, pages 258–272. Springer, 1999.
- [68] Zulfikar Ramzan. A preliminary outline of a proposed micromint design specification. 2000.
- [69] Nicko Van Someren. The practical problems of implementing micromint. In *Financial Cryptography*, pages 71–80. Springer, 2002.
- [70] Vesna Hassler, Robert Bihlmeyer, Michael Fischer, and Manfred Hauswirth. Mimi: A java implementation of the micromint scheme. In *WebNet*. Citeseer, 1997.
- [71] Jeffrey Burstein. *An implementation of MicroMint*. PhD thesis, Massachusetts Institute of Technology, 1998.
- [72] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In *Advances in Cryptology CRYPTO92*, pages 139–147. Springer, 1993.
- [73] Adam Back et al. Hashcash—a denial of service counter-measure, 2002.
- [74] Stanisław Jarecki and Andrew Odlyzko. An efficient micropayment system based on probabilistic polling. In *Financial Cryptography*, pages 173–191. Springer, 1997.
- [75] David Wheeler. Transactions using bets. In *Security Protocols*, pages 89–92. Springer, 1997.
- [76] RL Rivest. Lottery tickets as micro-cash. In *proceedings of Financial Cryptography*, 1997.

- [77] Ronald L Rivest. Electronic lottery tickets as micropayments. In *Financial Cryptography*, pages 307–314. Springer, 1997.
- [78] Richard J Lipton and Rafail Ostrovsky. Micro-payments via efficient coin-flipping. In *Financial Cryptography*, pages 1–15. Springer, 1998.
- [79] Silvio Micali and Ronald L Rivest. Micropayments revisited. In *Topics in Cryptology CT-RSA 2002*, pages 149–163. Springer, 2002.
- [80] Ronald L Rivest. Peppercoin micropayments. In *Financial Cryptography*, pages 2–8. Springer, 2004.
- [81] Philippe Golle, Kevin Leyton-Brown, Ilya Mironov, and Mark Lillibridge. Incentives for sharing in peer-to-peer networks. In *Electronic Commerce*, pages 75–87. Springer, 2001.
- [82] Kavitha Ranganathan, Matei Ripeanu, Ankur Sarin, and Ian Foster. To share or not to share: An analysis of incentives to contribute in collaborative file sharing environments. In *In Workshop on Economics of Peer-to-Peer Systems*. Citeseer, 2003.
- [83] Beverly Yang and Hector Garcia-Molina. Ppay: micropayments for peer-to-peer systems. In *Proceedings of the 10th ACM conference on Computer and communications security*, pages 300–310. ACM, 2003.
- [84] Kai Wei, Alan J Smith, Yih-Farn Robin Chen, and Binh Vo. Whopay: A scalable and anonymous payment system for peer-to-peer environments. In *Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on*, pages 13–13. IEEE, 2006.
- [85] Dario Catalano, Giancarlo Ruffo, and Rossano Schifanella. A p2p market place based on aggregate signatures. In *Parallel and Distributed Processing and Applications-ISPA 2005 Workshops*, pages 54–63. Springer, 2005.
- [86] Giancarlo Ruffo and Rossano Schifanella. Fairpeers: Efficient profit sharing in fair peer-to-peer market places. *Journal of Network and Systems Management*, 15(3):355–382, 2007.
- [87] Giancarlo Ruffo and Rossano Schifanella. Scalability evaluation of a peer-to-peer market place based on micro payments. In *Hot Topics in Peer-to-Peer Systems, 2005. HOT-P2P 2005. Second International Workshop on*, pages 10–17. IEEE, 2005.
- [88] Vivek Vishnumurthy, Sangeeth Chandrakumar, and Emin Gun Sirer. Karma: A secure economic framework for peer-to-peer resource sharing. In *Workshop on Economics of Peer-to-Peer Systems*, volume 35, 2003.
- [89] Flavio D Garcia and Jaap-Henk Hoepman. Off-line karma: A decentralized currency for peer-to-peer and grid applications. In *Applied Cryptography and Network Security*, pages 364–377. Springer, 2005.
- [90] Zou Jia, Si Tiange, Huang Liansheng, and Dai Yiqi. A new micropayment protocol based on p2p networks. In *e-Business Engineering, 2005. ICEBE 2005. IEEE International Conference on*, pages 449–455. IEEE, 2005.
- [91] Min Zuo and Jianhua Li. Constructing fair-exchange p2p file market. In *Grid and Cooperative Computing-GCC 2005*, pages 941–946. Springer, 2005.
- [92] Fabio R Piva, José RM Monteiro, and Ricardo Dahab. Strand spaces and fair exchange: More on how to trace attacks and security problems. *Anais do VII SBSeg, Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 80–93, 2007.
- [93] Fabio R Piva, José RM Monteiro, and Ricardo Dahab. Regarding timeliness in the context of fair exchange. In *Network and Service Security, 2009. N2S'09. International Conference on*, pages 1–6. IEEE, 2009.
- [94] Xiaoling Dai and John Grundy. Off-line micro-payment system for content sharing in p2p networks. In *Distributed Computing and Internet Technology*, pages 297–307. Springer, 2005.
- [95] Kaylash Chaudhary and Xiaoling Dai. P2p-netpay: an off-line micropayment system for content sharing in p2p-networks. *Journal of Emerging Technologies in Web Intelligence*, 1(1):46–54, 2009.
- [96] Crypto-currency market capitalizations. <https://coinmarketcap.com/>. Accessed: 2016-11-03.
- [97] Florian Tschorsch and Bjorn Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. 2015.
- [98] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140. ACM, 2013.
- [99] Tyler Moore and Nicolas Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk. In *Financial Cryptography and Data Security*, pages 25–33. Springer, 2013.
- [100] Patrick McCorry, Malte Möser, Siamak F Shahandashti, and Feng Hao. Towards bitcoin payment networks. In J.K. Liu and R. Steinfield, editors, *Information Security and Privacy: 21st Australasian Conference*, number pt. 1 in Lecture Notes in Computer Science, pages 57–76. Springer International Publishing, 2016.
- [101] J. Poon and T. Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, 2016.
- [102] Rafael Pass et al. Micropayments for decentralized currencies. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 207–218. ACM, 2015.
- [103] Alessandro Chiesa, Matthew Green, Jingcheng Liu, Peihan Miao, Ian Miers, and Pratyush Mishra. Decentralized Anonymous Micropayments, 2016. <https://eprint.iacr.org/2016/1033.pdf>.
- [104] Paysafecard. <http://www.paysafecard.com>. Accessed: 2015-11-03.
- [105] Paypal. <http://www.paypal.com>. Accessed: 2015-11-03.
- [106] Flattr. <https://flattr.com>. Accessed: 2015-11-03.
- [107] Changtip. <https://www.changtip.com>. Accessed: 2015-11-03.
- [108] Click and buy. <https://www.clickandbuy.com>. Accessed: 2015-11-03.
- [109] M-pesa. <http://www.safaricom.co.ke/personal/m-pesa>. Accessed: 2015-11-03.
- [110] League of legends prepaid game cards. <http://www.leagueoflegends.com>. Accessed: 2015-11-03.
- [111] Blendle. <http://www.blendle.com>. Accessed: 2015-11-03.
- [112] Starbucks card. <http://www.starbucks.co.uk/card>. Accessed: 2015-11-03.
- [113] Bitwall. <https://www.bitwall.io>. Accessed: 2015-11-03.
- [114] Octopus. <http://www.octopus.com.hk>. Accessed: 2015-11-03.
- [115] Mollie. <https://www.mollie.com>. Accessed: 2015-11-03.
- [116] Android pay. <https://www.android.com/pay/>. Accessed: 2015-11-03.
- [117] Apple pay. <http://www.apple.com/uk/apple-pay/>. Accessed: 2015-11-03.
- [118] Paym. <http://www.paym.co.uk>. Accessed: 2015-11-03.
- [119] itunes. <http://www.apple.com/itunes>. Accessed: 2015-11-03.
- [120] emusic. <http://www.emusic.com>. Accessed: 2015-11-03.
- [121] 2013 Online Fraud Report, 2013. <http://forms.cybersource.com/forms/fraudreport2013>.
- [122] FICO Data Shows the U.S. Credit Card Fraud Incident Rate Rose 17 Percent Over Two Years, Oct. 10 2013. <http://www.bloomberg.com/bb/newsarchive/aFeg868hdPKK.html>.
- [123] Syed Taha Ali, Dylan Clarke, and Patrick McCorry. Bitcoin: Perils of an unregulated global p2p currency. 2015.
- [124] Andy Greenberg. *Nearly 150 Breeds Of Bitcoin-Stealing Malware In The Wild, Researchers Say*. Forbes, Feb. 26 2014. <http://www.forbes.com/sites/andygreenberg/2014/02/26/nearly-150-breeds-of-bitcoin->
- [125] Board of Governors of the Federal Reserve System. *2013 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions*, Sept. 18 2014. http://www.federalreserve.gov/paymentsystems/files/debitfees_costs_2013.pdf.
- [126] Tyler Moore and Nicolas Christin. *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, pages 25–33. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
- [127] Interchange. <http://www.theukcardsassociation.org.uk/Interchange/index.asp>. Accessed: 2016-11-03.
- [128] Christopher Riederer, Vijay Erramilli, Augustin Chaintreau, Balachander Krishnamurthy, and Pablo Rodriguez. For sale : Your data: By : You. In *Proceedings of the 10th ACM Workshop on Hot Topics in Networks, HotNets-X*, pages 13:1–13:6, New York, NY, USA, 2011. ACM.
- [129] Office of the privacy commissioner for personal data - report number: R10-9866. https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_re. Accessed: 2015-11-03.
- [130] Reuters. Denmark moves step closer to being a cashless country, 6 May 2015. <http://www.telegraph.co.uk/finance/economics/11586778/Denmark-moves-step-closer->
- [131] Angela Daly. Private power and new media: The case of the corporate suppression of wikileaks and its implications for the exercise of fundamental rights on the internet. In Christina M. Akrivopoulou and Nicolaos Garipidis, editors, *Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies*, pages 81–96. IGI Global, Hershey, PA, 2012.
- [132] David Morris. Bitcoin's digital tip jar: Microtransactions reborn, 5 March 2014. <http://fortune.com/2014/03/05/bitcoins-digital-tip-jar-microtransactions-reborn/>.

- [133] Sudip Bhattacharjee, Ram D Gopal, James R Marsden, and Ramesh Sankaranarayanan. Digital goods and markets: Emerging issues and challenges. *ACM Transactions on Management Information Systems (TMIS)*, 2(2):8, 2011.
- [134] Anja Lambrecht, Avi Goldfarb, Alessandro Bonatti, Anindya Ghose, Daniel G Goldstein, Randall Lewis, Anita Rao, Navdeep Sahni, and Song Yao. How do firms make money selling digital goods online? *Marketing Letters*, 25(3):331–341, 2014.
- [135] Róbert Párhonyi, Aiko Pras, and DAC Quartel. Collaborative micropayment systems. 2004.
- [136] Gartner Inc. *Gartner Says By 2017, U.S. Customers’ Mobile Engagement Behavior Will Drive Mobile Commerce Revenue to 50 percent of U.S. Digital Commerce Revenue*, Jan. 28 2015. <http://www.gartner.com/newsroom/id/2971917>.
- [137] Bill Siwicki. *Mobile commerce will be nearly half of e-commerce by 2018*. InternetRetailer, March 10 2014. <https://www.internetretailer.com/2014/03/10/mobile-commerce-will-be-nearly-half-of-e-commerce-by-2018>.
- [138] Dennis Abrazhevich. *Electronic payment systems: A user-centered perspective and interaction design*. Dennis Abrazhevich, 2004.
- [139] Everything you need to know about youtube red. <https://www.cnet.com/how-to/youtube-red-details/>. Accessed: 2016-11-03.
- [140] Gillian Reagan and Lauren Hatch. Five Failed Paywalls And What We Can Learn From Them, 28 April 2010. <http://www.businessinsider.com/failed-paywalls-2010-4?op=1&IR=T>.
- [141] Josh Halliday. Times loses almost 90% of online readership, 20 July 2010. <http://www.theguardian.com/media/2010/jul/20/times-paywall-readership>.
- [142] World Wide Web Consortium (W3C). <http://www.w3.org/>.
- [143] Phillip M Hallam-Baker. Micro payment transfer protocol (mptp) version 0.1. *W3C Working Draft*, 1995.
- [144] World Wide Web Consortium et al. Common markup for micropayment per-fee-links. *W3C Working Draft (25 August)*, 4, 2002.
- [145] PayCircle Completed Its Mission After Three Years – Specification Submitted to OMA, 8 March 2005. <http://www.businesswire.com/news/home/20050308005339/en/PayCircle-Completed-Mission-After-Three-Years---Specification-Submitted>.
- [146] András Vilmos and Stamatis Karnouskos. Semops: design of a new payment service. In *null*, page 865. IEEE, 2003.
- [147] Stamatis Karnouskos, András Vilmos, Antonis Ramfos, Balázs Csik, and Petra Hoepner. Semops: a global secure mobile payment service. *chapter in the book of W.-C. Hu, C.-W. Lee, and W. Kou (editors), Advances in Security and Payment Methods for Mobile Commerce, Nov, 2004*.
- [148] Press Release. W3C Starts Web Payments Standards Work to Streamline the Online “Check-out” Process, 21 Oct. 2015. <http://www.w3.org/2015/09/webpaymentswg.html>.
- [149] Minutes of micropayments breakout at tpac 2016. <https://github.com/interledger/rlfcs/blob/master/micropayments-w3c.md>. Accessed: 2016-11-03.

However, there are also a number of negatives. The tracking of consumer behaviour often infringes on privacy, sometimes in noticeable ways when consumers are delivered targeted advertisements that may leak information to onlookers about their private behaviour. Video advertisements may waste the consumer’s time, and use an unacceptable amount of bandwidth for some mobile users. Increasing numbers of consumers are using ad-blocking software, which is a serious threat to businesses using this model.

Paywalls: The second prominent model for Web publishing is via **paywalls**, where users are directly charged to access digital content. Paywalls can take on several forms. The most popular model is **subscription**. This model is used by well-known brands such as Spotify, NetFlix, which charge members monthly fees to access their media catalogue. Then there are soft paywalls (also referred to as Freemium services), which offer differentiated service. Users can access certain basic content for free, but to access premium or customized content or service requires a subscription or a payment. Free content may be actual content or a preview or free trial. Premium content may include complete articles or quicker access (as in the case of stock quotes) or even customized content (such as digital newspapers for the iPad). This is the route taken by brands such as the Wall Street Journal, the New York Times, and Amazon’s Prime service. Some firms which are primarily rely on the advertisement-based model may offer an ad-free service for subscribers. YouTube has launched such a paywall for consumers in the US [139] at \$9.99 a month, and intends to extend this to the rest of the world at a later date. Google Contribute is a similar offering. A third type of paywall is the pay-as-you-go paywall in which a charge is levied for each article read.

Paywalls have yielded mixed results thus far and they are recognized as being a difficult strategy to implement. The paid-subscription model has notably failed in several cases, such as with the New York Times’ Times Select [140], Time [141], and The Sun. It has proved successful in other instances, such as when the New York Times retried it in 2011, and with ESPN and The Spectator. The reasons for success and failure are still being debated, but quality of content appears to be a strong factor.

APPENDIX A

A PRIMER ON BUSINESS MODELS FOR WEB PUBLISHING

Advertising: The dominant model for Web publishing is along the lines of television and print media, i.e. by **incorporating advertisements** or “selling eyeballs”. Advertisements constitute the primary revenue stream for the Web’s most popular sites, such as Google, YouTube, and Facebook. Advertisements are incorporated in the content, along sidebars or before videos start, and the customer does not pay anything from her own pocket. This open access is appealing to customers. However, it is technically incorrect to conceive of these services as ‘free’. Advertising costs are passed down to the customer in the prices of the advertised goods.

This model has several positives: highly customized advertisements can be delivered very easily to consumers. Consumer behavior can also be easily tracked, providing a rich source of information for merchants and businesses. Furthermore, there are minimal mental transaction costs for the customer.

APPENDIX B STANDARDIZATION

In the mid 1990s, the World Wide Web Consortium (W3C) [142] (the predominant international standards organization for the Web, consisting of technology firms, merchants, research laboratories and standards bodies, including support from the European Commission and DARPA) launched a Micropayment Markup Working Group (MPM-WG). This working group developed a Micropayment Transfer Protocol (MPTP) [143] to handle money transfers online in a secure manner, and a language to embed micropayment initiating instructions in web pages, Common Mark-up for Micropayment per-fee-links [144]. None of these contributions became full standards, but they are available in the public domain, and some of these

ideas were implemented in certain micropayment solutions, such as the NewGenPay micropayments system. The Working Group ceased activities in 2001.

The PayCircle consortium, founding members of which included CSG Systems, Hewlett-Packard, Oracle, Siemens, and Sun Microsystems, commenced work on developing standards for mobile payments and micropayments in 2002 [145]. PayCircle developed open application interfaces (APIs) to enable software developers to build universal payment-enabled applications for mobile business which interoperate with payment service providers such as telecom operators and banks. A public draft was submitted for consideration to the Open Mobile Alliance (OMA). PayCircle concluded operations in 2005.

Secure Mobile Payment Service (SEMOPS) was an EU funded project formed in 2002 by banks, technology companies, and research institutions, including names such as Motorola, Deloitte and Millenium Bank. It aimed to develop universal electronic payment solutions for peer-to-peer payments, mobile and Internet payments, real-time payment transfers between accounts, and micropayments. The project lasted two years and their contributions are described in [146] [147]. A follow-up project ran from 2007-08 with a focus on launching mobile payment services in some European countries.

In October, 2015, the W3C launched the Web Payments Working Group [148], to develop standards which “will support a wide array of existing and future payment methods, including debit, credit, mobile payment systems, escrow, and Bitcoin and other distributed ledger technologies.” Micropayments were one issue they discussed at TPAC 2016 [149].