Digital Cash and Anonymous Fair-Exchange Payment Protocols[1]

Authors

Danushka Jayasinghe, MSc (Royal Holloway, 2013)

Konstantinos Markantonakis, ISG, Royal Holloway

Abstract

Unlike in traditional POS transactions, e-commerce transactions are carried out in a virtual environment where transacting parties do not see each other physically. This raises concerns of fair-exchange, especially in Bitcoin due to payments being anonymous and irreversible. Therefore, it is vital to restore fairness in anonymous e-commerce transactions. In this article we sketch a protocol that ensures fairness as well as anonymity in Bitcoin transactions.

Introduction

Modern technological advancements have given a dramatic boost towards the evolution of the Internet. A strong outcome of this global expansion of internetworked technology is the emergence of electronic commerce. E-commerce touches every aspect of our day to day lives; *from* shopping with your local supermarket chain to get your necessities delivered *to* making an online payment for your music downloads to a merchant who operates in the other side of the world.

However, a buying and selling transaction in e-commerce is very different from a traditional Point-of-Sale (POS) transaction. E-commerce transactions between the consumers and sellers occur over the internet in a virtualised environment. Such an environment, where transacting parties do not see each other physically, makes it possible for a dishonest party to misbehave. As such, a merchant could simply not deliver the goods to a consumer once the payment is received or a consumer could simply disappear without paying a merchant once goods have been received. This places immense pressure upon e-commerce services, genuine merchants and payment solution providers to implement mechanisms that would guarantee payment settlement for purchases. Due to this reason, unlike in conventional cash payments during a POS transaction, in an e-commerce setting a consumer might lose privacy by having to provide personal and financial information to merchants and third parties.

Most of the current electronic payment methods do not provide *anonymity of the consumer* to protect consumer privacy and provide *security of financial information* to guarantee the security of the transferred value at the same time. This makes it a trade-off between *security of financial information* and *anonymity of the consumer*.

---

[1] This article is to be published online by Computer Weekly as part of the 2016 Royal Holloway information security thesis series. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full MSc thesis is published on the ISG's website.

In addition, current payment schemes have failed to replace real cash (notes & coins) by providing users with properties such as *anonymity*, *divisibility* (ability to break into smaller denominations) and *transferability* (ability to pass from one owner to the other).

Recently, consumers have shown interest in alternative payment methods other than credit/debit card based transactions. In this report we identify these payment methods as Alternative Payments. This fact is further established by the online survey carried out by the author. Some of the info-graphic analysis of the survey finding are shown below. The online survey attracted 73 anonymous participants.

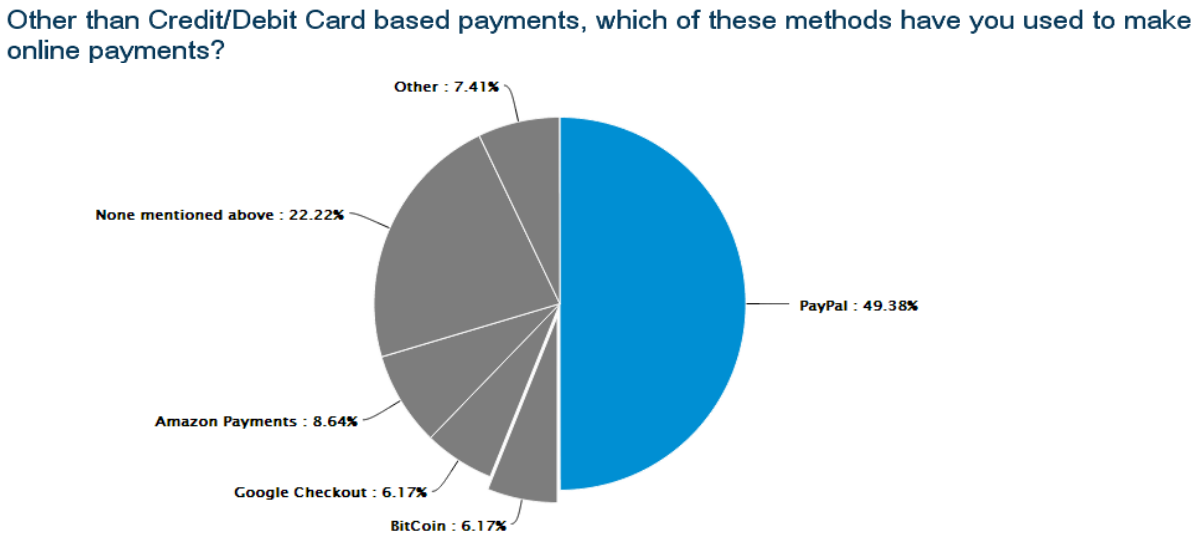

Figure 1: Alternative Payment methods.

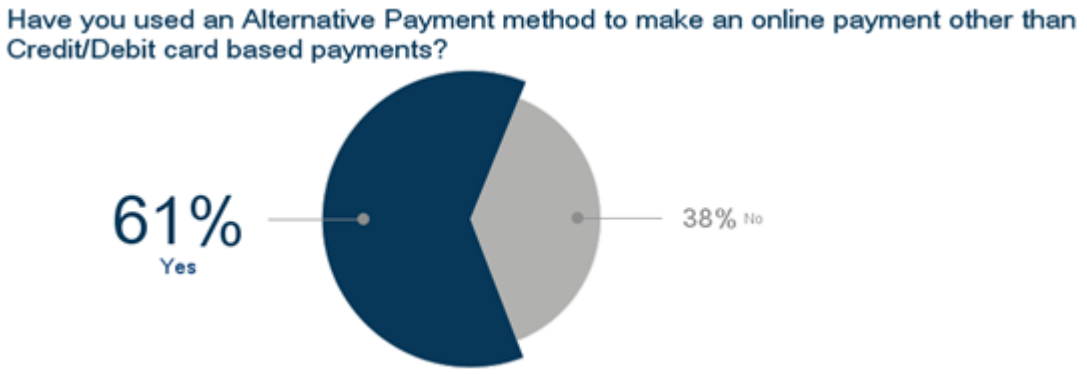

Figure 2: Use of Alternative Payment methods.

There are some important attributes to be considered to make a payment system gain recognition by consumers. In the online survey, participants rated some of these attributes in the order of importance as follows.

Question	Count	Score	Least Important	Somewhat Important	Neutral	Very Important	Extremely Important
1. Security of payment system	72	4.85					
2. Privacy of personal information & spending habits	72	4.38					
3. Anonymity of user identity	70	3.81					
4. Convenience of making payments	72	4.00					
5. The speed of payment processing time	70	3.80					

Figure 3: Attributes of payment methods.

In brief, receiving goods that you paid for and receiving payments for the goods that you delivered is called fair-exchange. If an e-commerce payment system guarantees fair-exchange for transactions, the participants also rated their perspective to the following question as below.

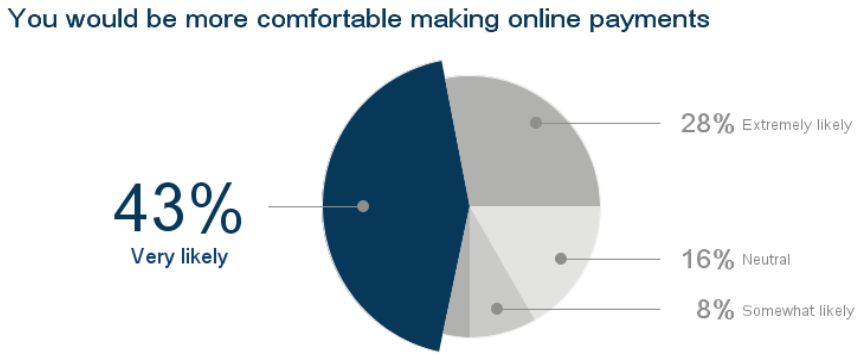

Figure 4: Consumers' perspective.

Electronic Money

Electronic Money in the context of e-commerce can be broadly defined as an electronic storage of monetary value on hardware or software system that is used to make payments and can be exchanged electronically. Electronic Money can be categorized into two distinct types: identified e-money and anonymous e-money.

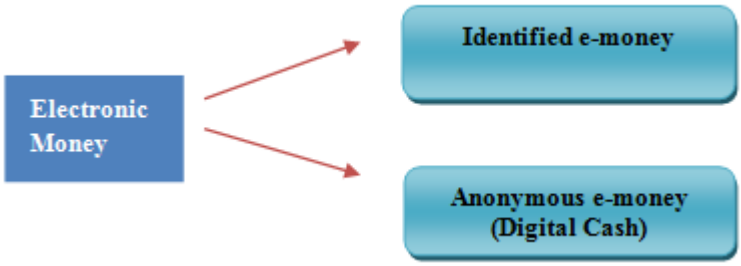

Figure 5: Two Distinct Types of Electronic Money

Identified e-money reveals the payer's identity, who initially withdrew electronic cash from the issuing bank. As the money gets transferred through the economy an audit-trail of payers and payees are also left by these identified e-money schemes. Examples of identified e-money include PayPal accounts, Amazon pay and Google Pay. In contrast, anonymous e-money does

not reveal the identity of the payer or payee and does not leave any transaction trail. Digital Cash comes under this category of Electronic Money and provide anonymity for the user.

What is Digital Cash?

The concept of providing anonymity in payment schemes was first proposed by David Chaum in 1982. He introduced *Blind Signatures* as a cryptographic primitive that would allow the construction of untraceable payment solutions. Digital Cash provides anonymity for the user by safeguarding the identity of the digital cash holder, financially sensitive information and consumer spending habits from Merchants, Banks and other third parties. Some properties of digital cash is illustrated in Figure 6 below.

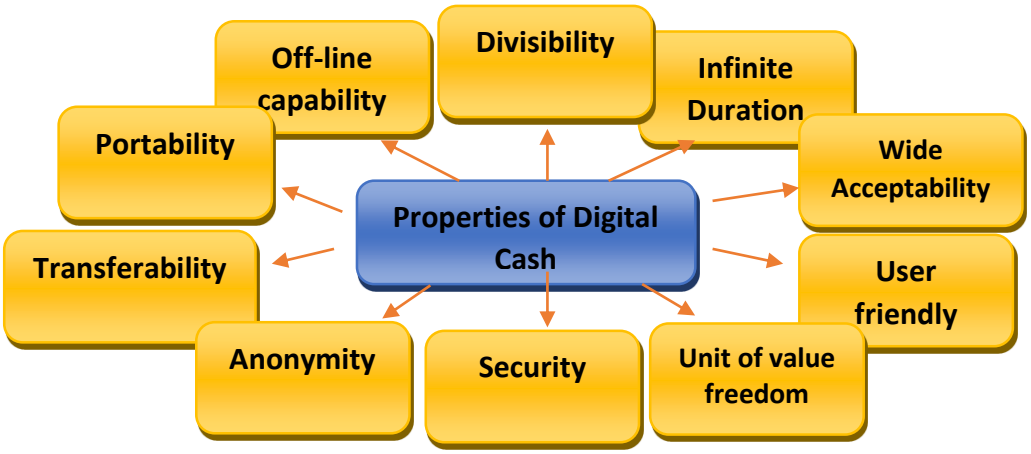

Figure 6: Properties of Digital Cash

Bitcoin

Bitcoin is a decentralised digital cash system which works on a peer to peer network. The system was first proposed and developed by Satoshi Nakamoto who self-published his proposal in a crypto forum in October 2008. Soon after Nakamoto's paper, an open-source project was started to work on the development of Bitcoin. The main innovation that came out of Bitcoin is the concept of something called the "Block Chain" technology. The Block Chain is a publicly available ledger which keeps a permanent record of all the Bitcoin transaction that ever took place. These transactions are represented in SHA256 hash outputs and stored in hash blocks. In 3rd January 2009, the first hash block called the Genesis Block was created and the Block Chain was broadcasted on the Bitcoin peer to peer network. Transactions authorising and creating new blocks are called Bitcoin mining. The concept of "proof of work" rewards the miners with Bitcoins for spending computational power. While Bitcoin was gaining its momentum, Nakamoto moved away while leaving the project with the Bitcoin community. Finding the real identity of Satoshi is a big mystery in Bitcoin.

Has fair-exchange got even more difficult??

Bitcoin payments are anonymous and irreversible. Once a consumer makes a Bitcoin payment in an e-commerce transaction, the payment is one-way and cannot be reversed. If the purchased content is not delivered, a refund or redelivery is not always guaranteed due to the anonymity of the payment. Because of this many consumers and merchants are reluctant to use Bitcoin.

Protocols that are built to achieve fairness in e-commerce transactions are called *Fair-exchange Protocols* – at the end of the protocol either each party receives the item it expects, or none of them does. Protocols that help realise anonymity and user privacy during payment are called *Anonymous Payment Protocols*. A combined solution that would realise fairness as well as anonymity is called an *Anonymous Fair-exchange Payment Protocol*.

Proposed Solution

The main contribution of this work is the *Anonymous Fair-exchange Payment Protocol* proposed to achieve fair-exchange in an e-commerce transaction which can be used in conjunction with Bitcoin with improved unlinkability.

Proposed protocol message flow

- *C = Consumer*
- *M = Merchant*
- *TTP = Trusted Third Party*
- *BP2P = Bitcoin Peer to Peer Network*

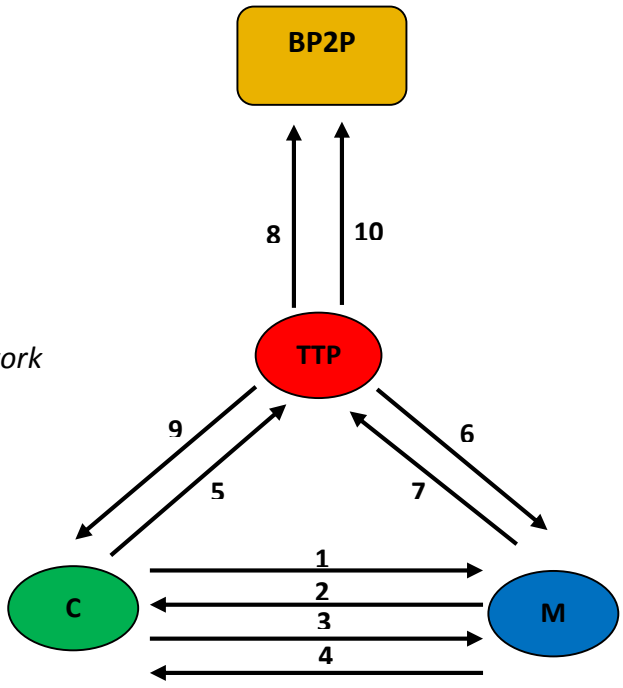

Figure 7: The proposed protocol message flow

The protocol uses an online trusted third party (TTP) to achieve true fair exchange and dispute resolution. The transacting parties register with the TTP using pseudo IDs. The TTP issues shared symmetric keys to both C and M respectively. These keys provide confidentiality to the communication between the TTP and the two participants.

Illustrated in *Figure 7* is a diagram of the proposed protocol's message flow in the numbered order between the protocol entities. The overall protocol includes ten messages to complete an anonymous fair-exchange transaction using Bitcoin as an anonymous payment method. The protocol can be broken down to three main phases. The first two messages of the protocol fall under the *"Product/Price Negotiation Phase"* and can be exchanged by the consumer and merchant any number of times until they agree to continue. Messages three to seven fall under the *"Digital Content Delivery Phase"* and messages eight to ten fall under the *"Payment Phase"*.

In the first two messages the consumer and the merchant agrees on the digital content (product) and negotiate the price for that particular product. Once the product/price negotiation is completed, the merchant sends the consumer an encrypted copy of the digital content but without the decryption key. Once the consumer receives the encrypted product he/she forwards Bitcoin payment details to the TTP. The product is encrypted by the merchant and the TTP does not store the product. The TTP request the merchant's Bitcoin address and the decryption key for the consumer. The TTP after receiving these details forwards a message to the Bitcoin peer-to-peer network to transfer the consumer's Bitcoins to the TTP. Upon securing the Bitcoin transaction the TTP forwards the key to the consumer to decipher the digital content and make another payment arrangement for the merchant in a Bitcoin transaction. Unlike in an ordinary Bitcoin transaction, the protocol proposes a TTP key generation, key management and key tracing solution that improves Bitcoin transaction anonymity.

The proposed protocol involves an on-line TTP to realise anonymity and fairness. The protocol while guaranteeing anonymity and fairness of transactions further improves the consumer-merchant anonymity by improving the Bitcoin transaction unlinkability. This unlinkability is achieved by the proposed TTP key generation, key management and transaction tracking solution as illustrated in *Table 1*.

TTP BitCoin Key Generation, Key Management & Tracking Solution

	TTP Private ECDSA Key	TTP Public Elliptic Curve Digital Signature Algorithm (ECDSA) Key	TTP BitCoin Address
Eg: Pseudo-Random Function with static secret	453435E9827F0C4009C700E91B15BA8D4E86F9B7A0FF9374F1F272EC2BAEC3F6	048F4840C54CDA164F53EEBFD1CB2BCFF1F80CFBFC8F73E531836F215A655D2C7A802E00F39DCA1757EAF31772BCD3D08BB3EDF67442325E6E0C1BF52A078E75C7	1ET8iJSUr3cJsVWTysxLC7QTo7t5neiCwy

Transaction -ID	Consumer BitCoin Address (Payer)		TTP Pseudo-Random Public Keys		Merchant BitCoin Address (Payee)
2981	1Es8sjMKMYn81XGD46Seme6tgN5JszUY2E	→	1ET8iJSUr3cJsVWTysxLC7QTo7t5neiCwy		1245hqXy4V3GtRXnojyPbthQN1s9E8KRAF
2982	1MkcpyQ2Jj6X9SwqZTtPUhTG6gfR5UJvam	→	1FfGzimzGbTssZDSwmrEco1tJ6Bmn2o7Yd		12NxhdZqJ2S8B82bnSodcN2kd3cSUML5aX
2983	138PYYUgsFLBxxQSXoDurSo9hG6vSPvaBX	→	1KQJgyFkxisYLqktJTLpitfFcXdB1ur22KB		1L8x5c2kfnxwuAF6ztR51KfDe8mcUUs96Q
2984	12JqZL8ycNb7hu6zxJfd8u3EqPQD7PUcDS	→	1KzugzvhkidNJTY68TwF2zLBxpPLujVF8t		13HyjGHoSpba9zcbhM1ZpUTscXFgmBJKUA
2985	1DjA6RDS86QNKufxZfnK6dL2vSDuGhw2zi	→	16xV1EEbaa1zLzYRBToGfrsuw5ebNt8Q5c		1Nb5TkcnDoymyNpNYB4SvJE6jYc3NqHDxy
2986	157hBfXqqXFJzJrCSKdqFn1tzM256QaKYV	→	1m2cWd9fLgEj6okVk7fw9rUAX5AdJZ22B		1DsWCFh6i83xhgeSPvZHcvJ4e5UE5jKRNE
2987	1BmV6da53JgEAB5v7WPWcYGdaoz6YqgTta	→	12Be8Dmt2p5dqLVRZxhmJJrTbqvBG9ffR1		17nDii6QuRk3KWHRV2KWsnsgQ177U9inFE
2988	1Ak1e3SXai9ECzjUYbffB5q44TMCiJXMNk	→	13T2q5aJK1ow8VmPBukrrUSe1vVbr6MjyE		1N9nmZYwn2Ms37JJk7bHrWvaD4kG6nUjkH

Table 1: TTP Bitcoin Keys Generation, Key Management & Tracking Solution

The protocol achieves "Real-time" dispute resolution within the protocol run rather than "After the fact" dispute resolution. If any misbehaving is identified by the TTP that makes the protocol unfair, then the protocol is forced to abort. If the TTP identifies a resolvable dispute such as an incorrect message has been sent, the TTP may request a re-send of that particular message from a party. Furthermore, due to the use of registered pseudonym-ID and digital signatures the protocol provides non-repudiation of messages.

The proposed protocol and other TTP based protocols were compared against the criteria of anonymity, fair-exchange, whether the TTP stores the exchange digital content, services provided and the number of total protocol messages. The result is shown in Table 2. The proposed protocol achieves full anonymity, strong-fairness, payment, TTP does not store purchased products and the protocol achieves all these aspects within a total of ten protocol messages.

	Protocol	Anonymity	Fairness	TTP stores product	• **Payment** • **Digital content** • **Physical delivery**	Number of messages
1995	Netbill Protocol	No	Strong fairness	No	• No • Digital content • No	8
1996	Zhang N. & Shi Q. Protocol	No	Strong fairness	Yes	• No • Digital content • No	3 + Pre-protocol messages
1996	Zhou J. & Gollmann D. protocol	No	Strong fairness	No	• No • Digital content • No	5 + Pre-protocol messages
2005	Zhang Q., Markantonakis K. and Mayes K. Protocol	Weak anonymity (Only between C & M)	Strong fairness	Yes	• Payment • Digital content • Physical delivery	12 (Including delivery messages)
	**The Proposed Protocol in this project**	**Fully anonymous**	**Strong fairness**	**No**	• **Payment** • **Digital content** • **Can be improved**	**10 (Exactly)**

Table 2: Comparison between the proposed protocol and other TTP based protocols

Conclusion

The purchase of goods with notes and coins has been around for centuries. It is not an easy task to switch from traditional payment methods to digital cash in a short period of time. However, humans have been exposed to a lot of technological advancements in the last decade than they ever have. This has made behavioural changes in the way humans adapt new tools to make their day to day tasks more convenient. The need for a migration into a combined solution that provides anonymity as well as fair-exchange is foreseeable.

The full project (available on the ISG website) contains a report on the extensive research into *Anonymous Payment and Fair-exchange Protocol Schemes and Implementations* as well as a thorough examination of the Bitcoin payment system. Here we have sketched the main ideas of a new protocol guaranteeing strong fair-exchange while preserving anonymity in e-commerce transactions by using Bitcoin as a payment method with improved unlinkability.

Biographies

Danushka Jayasinghe holds a BSc (Hons) degree in Computer Networking from the University of Greenwich. He completed his MSc in Information Security at the ISG, Royal Holloway, University of London in 2013. He joined the Smart Card Centre to follow a PhD under the

supervision of Dr Konstantinos Markantonakis. His research interests are on modern electronic payment systems with the consideration of security, privacy and efficiency of the underlying payment protocols and platforms. He is also interested in alternative payment schemes other than conventional card-based payment methods including digital cash and anonymous & fair-exchange payment protocols.

Dr Konstantinos Markantonakis B.Sc. (Lancaster University), M.Sc., MBA, Ph.D. (London) received his BSc (Hons) in Computer Science from Lancaster University in 1995, his MSc in Information Security in 1996, his PhD in 2000 and his MBA in International Management in 2005 from Royal Holloway, University of London. He is currently a Reader (Associate Professor) in the Information Security Group and the director of ISG Smart Card Centre. His main research interests include smart card security and applications, secure cryptographic protocol design, embedded system security, mobile phone operating systems/platform security, NFC/RFID security, grouping proofs, electronic voting protocols, IoTs and avionics security. Since completing his PhD, he has worked as an independent consultant in a number of information security and smart card related projects for a number of clients. He is a member of the IFIP Working Group 8.8 on Smart Cards. He is a vice-chair of the IFIP "WG 11.2: Pervasive Systems Security" and one of the two UK representatives for the COST action (*ICT COST Action IC1204*) onTrustworthy Manufacturing and Utilization of Secure Devices. He has published more than 130 papers in international conferences and journals. He continues to act as a consultant on a variety of topics including smart card security, key management, information security protocols and mobile devices, for financial institutions, transport operators and technology integrators.