Digital cash and anonymous fair-exchange payment protocols

Danushka Jayasinghe

Abstract:

The e-commerce market is growing and is expected to double from a value of €755 billion in 2010 to an expected €1460 billion in 2015 [57]. Recently, consumers have shown interest in Alternative Payment methods other than credit/debit card based transactions. This fact is further established by the online survey carried out by the author of this project. The online survey attracted 73 anonymous participants. The full results analysis is attached in Appendix C.

Anonymity and Fair-exchange are two important attributes that consumers anticipate in e-commerce payment transactions. The main contribution of this project is the proposed protocol discussed in Chapter 6. The protocol guarantees anonymous fair-exchange in e-commerce transactions by using BitCoin with improved unlink-ability. The proposed protocol is a practical and widely deployable solution in the current e-commerce system.

This project carried out an extensive research to thoroughly identify Digital Cash and Anonymous Fair-exchange Payment Protocols. The report thoroughly examined the BitCoin payment system and identified a vulnerability of BitCoin transactions that significantly draw anonymity and privacy concerns. The vulnerability makes it possible to link BitCoin transactions from the payer to payee which in some cases could reveal their identity.

The proposed protocol uses BitCoin as the anonymous payment method and finds a solution to resolve BitCoin transaction linking. The protocol involves a Trusted Third Party (TTP) to achieve strong-fairness. The previously mentioned BitCoin transaction unlink-ability is achieved by the proposed TTP key generation, key management and transaction tracking solution as illustrated in Table 6.2.

Lastly the report suggests recommended future work based upon the project achievements and online survey results analysis. The recommended work addresses further improvements to the proposed protocol and research in the field of Digital Cash & Anonymous Fair-exchange.