Evolution of an electronic currency: network payment, and electronic commerce technologies.

Electronic financial transactions and payment systems have traditionally relied on third party institutions, such as banks or credit card companies, to ensure secure transfers between parties. Users of such systems must trust that third party institutions will be honest and follow through with their claims. Trust-based systems are difficult to establish in the digital realm without a governing body regulating and securing transfers. Systems using this model have many downfalls that make them risky and undesirable for Internet use. With the requirement of all transactions being completely digit, how can we transfer funds securely without a trusted third party? [1]. All types of currencies share many common problems such as stability, control, and inflation. As time passes, the relative value of a currency usually decreases (meaning that prices increase). If this happens too quickly, it can cause major problems if prices increase beyond the means of the populace who uses the currency. Another problem is stability because the currency should not be subject to dramatic exchange rate fluctuations under the influence of a single individual or party. Control over a currency, or lack thereof, is also important. Typical fiat currencies depend on a mint and the promise that the mint will continue its operations. If the mint were to close indefinitely, the currency would likely die out in a relatively short period of time. Therefore, the mint has some level of control over the currency. Bitcoin is a digital currency introduced in 2009, based on a self-published paper by Satoshi Nakamoto[2]. Bitcoin enables payments that are based on proof, rather than trust, in a manner that is similar to cash. A seller given a cash payment can inspect the currency and, with a good degree of confidence, assert whether the payment is valid or invalid. Bitcoins works using a similar concept that make coins and coin ownership easy to verify. An important difference between this virtual currency and typical fiat currency is that Bitcoin's validity can be verified. During this workshop we showed attendees the verification process as well as the algorithms and technologies that make verification possible. The audience learned about online money transaction, then analyzed standard techniques and form comparisons between them. The workshop then proceeded to discuss the history and purpose of Bitcoins along with an overview of its concepts and terminologies. The workshop continues to compare Bitcoins with other transaction techniques discussed and talk about the pros and the cons. We also go to the problems that Bitcoin will be able to solve and what new problems it will introduce. Attendees will learn the details of Bitcoins and its implementations. From Asymmetric cryptography algorithms to hashing and digital signatures to proof of work, the audience will be walked through all the

technologies that make Bitcoin possible. The workshop will take attendees through actual Bitcoin transactions and the details of the transaction process as it will allow them to see how the Bitcoin system overcome problems such as double spending. The audience was also taught about Bitcoin generation and how Bitcoins are generated out of thin air. For context, we covered how much coins are worth and how people are already profiting from services other than mining. The details of Bitcoin "blocks" and "chains" were demystified in a manner that was detailed but simple to understand. The Bitcoin network was one of the main focuses - how a distributed and completely public network can maintain the anonymity of its users. It was discussed in detail about how transactions are validated through the network and about the transaction databases that is on the distributed network. The audience learned how the distributed database handles failures, delay, and is able to work effectively with only a subset of the entire database. The audience learned concepts such as Merkle trees and how they help the Bitcoin network to maintain the database. We answer questions such as how Bitcoins control the expansion of its own currency when the Bitcoin network may double in size in a short period of time. The many interesting characteristics of the network were unveiled during this engaging demonstration. Attacks and malicious hosts are constantly a threat to modern day electronic transactional systems and this also applies to Bitcoin. We mapped out the architectural features that make Bitcoin naturally resilient to many common attacks, as well as the features that make it vulnerable. We discussed possible attacks on the Bitcoin network as well as attack mitigation and ways in which end users can protect themselves. Another interesting issue is anonymity. Bitcoin is regarded as being anonymous by many people, yet Bitcoins can be traced from the original miner all the way to the current owner. A Bitcoin address itself is just a number and cannot identify anyone. However if a person manages to collect enough information about the owner of that address (perhaps through forums) then the owner can be exposed. To conclude, in this workshop we explored everything from cryptographic algorithms to the massive peer-to-peer network. We took a security perspective for an in-depth exploration of Bitcoin attacks and attack mitigation. We ended our workshop with a look at how Bitcoin might change the e-commerce landscape, followed by an open discussion. The NetCheque[3] payment system is an electronic payment system for the Internet developed by Clifford Neuman and Ari Medvinsky at the Information Sciences Institute of the University of Southern California. At present the implementation is a research prototype and is available for licensing by companies implementing commercial payment service. It is not presently supported as consumer product or service. Small companies and individuals looking for a way to accept payment on the web may find the tutorial material on this site useful, but until the NetCheque

system is offered as a commercial service, it is not an option available for their use. Direct questions and requests send to NetCheque@isi.edu. Users registered with NetCheque accounting servers are able to write electronic checks to other users. These checks may be sent through e-mail or as payment for services provided through other network protocols. When deposited, the check authorizes the transfer of account balances from the account against which the check was drawn to the account to which the check was deposited. The strengths of the NetCheque system are its security, reliability, scalability, and efficiency. Signatures on checks are authenticated using Kerberos. Reliability and scalability are provided by using multiple accounting servers. The NetCheque system is well suited for clearing micropayments; its use of conventional cryptography makes it more efficient than systems based on public key cryptography. The NetCheque system will enable creation of new Internet services that charge small fees, on the order of pennies, for access to information, processing queries, and consumption of resources. Such services are a critical component of electronic commerce. Anonymous Network Payment using NetCash. Payments using the NetCheque payment system originate from named user accounts. ISI has also developed a research prototype for an electronic currency system called NetCash supporting anonymous payments. NetCash will use the NetCheque system to clear payments between currency servers. Pay Per View (PPV) is a transaction handling protocol for use on the World Wide Web (WWW) developed in 1995 as part of the NetCash and NetCheque payment systems. Using PPV, merchant WWW servers make certain documents available on a pay-per-view basis. PPV is built on top of ARDP and HTTP for transport, and the software developed for PPV accepts both NetCheque and NetCash payments. A comprehensive index of electronic payment schemes and a brief overview of their relationship to the framework is provided [4, 5]. The framework consists of two axes, the levels of abstraction at which the protocol is analyzed and the payment model considered. A three layer model is used to compare payments schemes. The semantics of the payment scheme includes refunds policies, and the liabilities incurred by customers, merchants and financial institutions. The requirement for storage of data by communications between the parties includes not only the data flows for payments themselves but also for refunds, account enquiries and settlement. Mechanism is the methods by which the necessary security requirements for messages and stored data are achieved. All three abstraction levels are tightly coupled since policy makes requirements of data flow and data flow makes requirements of mechanism. Cash consists of a token which may be authenticated independently of the issuer. This is commonly achieved through use of self-authenticating tokens or tamper proof hardware. Bill is payment instruments whose validity requires reference to the issuer. Card

payment schemes provide a payment mechanism through the existing credit card payment infrastructure. Such schemes have many structural similarities to bill models except that solutions are constrained by that structure. A key feature of card payment systems is that every transaction carries insurance. The following list was compiled with the aid of indices maintained by the World Wide Web Consortium, Cornell, SIRENE, IBM, AT&T Bell Labs, and the Home Page of the www-buyinfo mailing list. See also pages by Stefan Brands Robert Hettinga and Michael Peirce. Yahoo e$ sites of interest . Additional payments schemes may be announced via a fill in form. These announcements may be viewed in un-moderated form. Anonymous Internet Mercantile Protocol, Anonymous Credit Cards *AT&T Bell Labs* A card model protocol which implements a policy which balances strong guarantees of confidentiality with the needs of law enforcement. A formal approach is employed with comprehensive details of mechanism and data flow. BankNet Electronic Banking Service *Marketnet* Full electronic banking service offers ability to write bills. Uses PKCS enveloped formats. BarclayNet *Barclaycard* is an electronic mall run by one of the world largest credit card companies. Preventing disclosure of the credit card number to the merchant is thus superfluous and a simple secure socket communication mechanism to prevent eavesdropping is sufficient. CAFE *is the* cash based scheme with strong guarantees of anonymity backed by a 13 member European consortium. Now the details are not available. e-Cash DigiCash is anonymous digital cash. Few details are given about the specific scheme employed but voluminous archives of papers by the company founder, David Chaum are provided. Mark Twain Bank has deployed this scheme. Electronic commerce payments *Financial Services Technology Consortium* No public details on this project are available at present. Electronic cheque *Financial Services Technology Consortium* is a bill scheme designed to provide an upgrade path from the existing bill system. Green Commerce *First Virtual* is the first Virtual's Green Commerce payments model is one of the first payments schemes to become established on the internet. The major novel feature of this scheme is its satisfaction guaranteed policy which protects customers from dishonest merchants by allowing them an unconditional right to refuse payment for individual items. A statistical mechanism is used to identify over frequent use of this option and exclude habitual non-payers. Identification of customers is via an email call back loop scheme. Internet Keyed Payment Protocols(iKP) *IBM (Zurich & Watson Labs)* is a card based model of payment which mainly addresses the questions of data flow and mechanism. Public key cryptography is used to ensure the privacy of a customer's card number and PIN number and provide non-repudiability. iKP has three options,, 1KP, 2KP and 3KP in which the acquirer alone, acquirer and merchant and acquirer merchant and

customer respectively have a public key. See also the SEPP protocol which is based upon iKP. CheckFree company provides various payments schemes on a number of models. FBOI *First Bank of Internet* is a novel payments system employs ATM cards and PGP provides strong guarantees which prevent loss of money by the bank. Protection for the customer is less apparent. LETSystems *LETSgo Manchester* LETSystems presents a novel policy view in the radical tradition of Northern England. A system of local currencies is proposed and a pilot project in Manchester, England described. NetBill *Carnegie Mellon University INI* is an implementation of a bill payment model employing a symmetric key cryptography mechanism based on Kerberos. NetCash/NetBank *Software Agents, Inc.* Policy allows transactions for free but a charge of 2% is levied for transfers into or out of the system. No security mechanism or data flow is described. NetCash *USC* A cash model. NetCheque *USC* is an implementation of a bill payment model employing a symmetric key cryptography mechanism based on Kerberos. NetPay *Boston Automation* is an EDI based transaction settlement system developed by Advantis. NetChex is the payments scheme based on a bill mode but using credit cards for account settlement. Mechanism is proprietary and a detailed description is not provided. The mechanism appears to employ a shared secret. Magic Money *Cypherpunk's is t*he ultimate in privacy policy, even the originators of the scheme are anonymous. Mechanism seems to be based on PGP. Used to implement a scheme by Chaum NexusBucks and by the Phantom Exchange Millicent *DEC (Systems Research Center)* is a payments protocol with a scrip based variant of a bill model. Mondex *Mondex* is the cash scheme based on a hardware "purse" device. This provides the portable and network independence of physical coin. Secure Courier *Netscape* is a card payment scheme based upon public key technology built on the Secure Sockets Layer protocol. Secure Electronic Payment Protocol *MasterCard* is MasterCard sponsored payments protocol based upon the IBM iKP protocol. Developed in association with IBM, Netscape, CyberCash and GTE Corp. Secure Internet Payment Service *CyberCash* is an established payments scheme employing public key cryptography to protect the customer authentication data and provide non-repudiablity. STT *Microsoft*, *VISA* Details to be announced. Stored Value Card *VISA* A planned cash scheme based on a hardware device permitting purchases of up to $10. Vishnu *Hewlett-Packard Labs Bristol* is a mechanism for bill/card based payment. Employs a Diffie Helleman based cryptographic mechanism which permits novel data flow optimization[6-24].

References

1. Martins S., Yang Y. Introduction to bitcoins: a pseudo-anonymous electronic currency system // http://dl.acm.org/citation.cfm?id=2093944
2. Bitcoin P2P Digital Currency // http://bitcoin.org/
3. The NetCheque // http://www.netcheque.org/
4. Evolution of Network Payment and E-Commerce Technologies // http://www.bcneuman.com/ecommerce/
5. *Dr Phillip M. Hallam-Baker* Electronic payment schemes // http://www.w3.org/ECommerce/roadmap.html
6. Slaves of a New Machine: Exploring the For-Free / For-Pay Conundrum *Laura Fillmore* Considers the impact of electronic payments on publishing with examples drawn from personal experience.
7. *XIWT* Another National Information Infrastructure consortium. This one provides a comprehensive breakdown of the requirements for electronic cash.
8. Electronic Money and Money in History *Roy Davies* Two articles on the history of money with a well designed annotated index.
9. Making Money on Internet Conference proceedings, University of Texas at Austin, Austin -- May 8-10, 1994
10. The First International Conference on Electronic Commerce University of Texas at Austin, Austin -- October 30-31 1995
11. Provision is made for unlisted schemes to be registered. At present no facilities are provided to provide alternative analysis according to a taxonomy of their choice such as performance or to provide comment on a particular proposal.
12. AltaVista for a current list of links.
13. WEBster--The Cyberspace Surfer, Oct. 3, 1995 [3Oct95]
14. www-buyinfo Home Page [10Nov95]
15. Whitey's Web Works - Online Marketing and Research [3Dec95]
16. Agorics, Inc. References to Interesting Documents [2Dec95]
17. Communication Links [20Nov95]
18. Network Payment Collected Information [30Nov95]
19. Privacy-on-Demand (PoD) - ECommerce [6Nov95]
20. egBanks: example Banking links [27Nov95]
21. egMedia: example Media links [18Nov95]
22. Electronic Commerce [28Nov95]
23. Jiri Baum - e-cash vs. cash and CC [3Nov95]

24.e$ sites of interest [29Nov95]