What You Don't Know About Crypto Currency, But Think You Know!
Why No Malaysian Has Mentioned This Truth Before?

By Matthias Chang – Future Fast-Forward

I am going to blow your mind and demand that you start thinking. No more time wasting.

Malaysian Intel Apparatus Did Not Know

- **The NSA was investigating crypto-currencies in 1996.**
- **I have read the entire Report: "How to Make a Mint: The Cryptography of Electronic Cash," which was published by the National Security Agency back in 1996.**

I stand to be corrected, if the Intel Apparatus knew, why did they remain silent? The then Prime Minister was not informed at all. The only conclusion to be drawn is that Malaysia was not aware. Neither Bank Negara!

Knowledge is NEVER a threat to National Security. Ignorance and the "Tongkat Mentality" are grievous threats!

For you to be the judge whether I have the Report and read it, I will quote in extenso:

National Security Agency Office of Information Security Research and Technology
Cryptology Division
18 June 1996

CONTENTS

My Whatsapp warning message this morning (17.6.2024) about certain Malaysian intellectual masturbators' inability to read and understand simple English, and thereafter distort my articles, has cautioned me to be more circumspect in sharing my research and financial intelligence. Hence, I will only share a limited amount of my research, enough to spur the genuine Truth-seeker to do the heavy lifting.

Extracts of the Report

"Introduction"

With the onset of the Information Age, our nation is becoming increasingly dependent upon network communications. Computer-based technology is significantly impacting our ability to access, store, and distribute information. Among the most important uses of this technology is electronic commerce: performing financial transactions via electronic information exchanged over telecommunications lines. A key requirement for electronic commerce is the development of secure and efficient electronic payment systems. The need for security is highlighted by the rise of the Internet, which promises to be a leading medium for future electronic commerce.

Electronic payment systems come in many forms including digital checks, debit cards, credit cards, and stored value cards. The usual security features for such systems are privacy (protection from eavesdropping), authenticity (provides user identification and message integrity), and nonrepudiation (prevention of later denying having performed a transaction) .

The type of electronic payment system focused on in this paper is electronic cash. As the name implies, electronic cash is an attempt to construct an electronic payment system modelled after our paper cash system. Paper cash has such features as being: portable (easily carried), recognizable (as legal tender) hence readily acceptable, transferable (without involvement of the financial network), untraceable (no record of where money is spent), anonymous (no record of who spent the money) and has the ability to make "change." The designers of electronic cash focused on preserving the features of untraceability and anonymity. Thus, electronic cash is defined to be an electronic payment system that provides, in addition to the above security features, the properties of user anonymity and payment untraceability..

In general, electronic cash schemes achieve these security goals via digital signatures. They can be considered the digital analog to a handwritten signature. Digital signatures are based on public key cryptography. In such a cryptosystem, each user has a secret key and a public key. The secret key is used to create a digital signature and the public key is needed to verify the digital signature. To tell who has signed the information (also called the message), one must be certain one knows who owns a given public key. This is the problem of key management, and its solution requires some kind of authentication infrastructure. In addition, the system must have adequate network and physical security to safeguard the secrecy of the secret keys.

This report has surveyed the academic literature for cryptographic techniques for implementing secure electronic cash systems. Several innovative payment schemes providing user anonymity and payment untraceability have been found. Although no particular payment system has been thoroughly analyzed, the cryptography itself appears to be sound and to deliver the promised anonymity.

These schemes are far less satisfactory, however, from a law enforcement point of view. In particular, the dangers of money laundering and counterfeiting are potentially far more serious than with paper cash. These problems exist in any electronic payment system, but they are made much worse by the presence of anonymity. Indeed, the widespread use of electronic cash would increase the vulnerability of the national financial system to Information Warfare attacks. We discuss measures to manage these risks; these steps, however, would have the effect of limiting the users' anonymity.

This report is organized in the following manner. Chapter 1 defines the basic concepts surrounding electronic payment systems and electronic cash. Chapter 2 provides the reader with a high level cryptographic description of electronic cash protocols in terms of basic authentication mechanisms. Chapter 3 technically describes specific implementations that have been proposed in the academic literature. In Chapter 4, the optional features of transferability and divisibility for off-line electronic cash are presented. Finally, in Chapter 5 the security issues associated with electronic cash are discussed.

The authors of this paper wish to acknowledge the following people for their contribution to this research effort through numerous discussions and review of this paper: Kevin Igoe, John Petro, Steve Neal, and Mel Currie.

1.3 Electronic Cash

We have defined privacy as protection against eavesdropping on one's communications. Some privacy advocates such as David Chaum , however, define the term far more expansively. To them, genuine "privacy" implies that one's history of purchases not be available for inspection by banks and credit card companies (and by extension the government). To achieve this, one needs not just privacy but *anonymity*. In particular, one needs

- *payer anonymity* during payment,
- *payment untraceability* so that the Bank cannot tell whose money is used in a particular payment.

These features are not available with credit cards. Indeed, the only conventional payment system offering it is cash. Thus Chaum and others have introduced *electronic cash* (or *digital cash*), an electronic payment system which offers both features. The sequence of events in an electronic cash payment is as follows:

***withdrawal*,** in which Alice transfers some of her wealth from her Bank account to her card.
***payment*,** in which Alice transfers money from her card to Bob's.
***deposit*,** in which Bob transfers the money he has received to his Bank account.

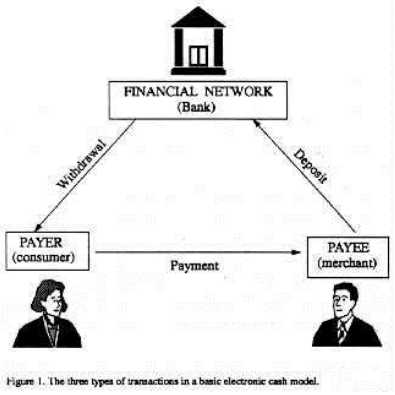

Figure 1. The three types of transactions in a basic electronic cash model.

Conclusion

This report has described several innovative payment schemes which provide user anonymity and payment untraceability. These electronic cash schemes have cryptographic mechanisms in place to address the problems of multiple spending and token forgery. However, some serious concerns about the ability of an electronic cash system to recover from a security failure have been identified. Concerns about the impact of anonymity on money laundering and tax evasion have also been discussed.

Because it is simple to make an exact copy of an electronic coin, a secure electronic cash system must have a way to protect against multiple spending. If the system is implemented on-line, then multiple spending can be prevented by maintaining a database of spent coins and checking this list with each payment. If the system is implemented off-line, then there is no way to prevent multiple spending cryptographically, but it can be detected when the coins are deposited. Detection of multiple spending after-the-fact is only useful if the identity of the offender is revealed. Cryptographic solutions have been proposed that will reveal the identity of the multiple spender while preserving user anonymity otherwise.

Token forgery can be prevented in an electronic cash system as long as the cryptography is sound and securely implemented, the secret keys used to sign coins are not compromised, and integrity is maintained on the public keys. However, if there is a security flaw or a key compromise, the anonymity of electronic cash will delay detection of the problem. Even after the existence of a compromise is detected, the Bank will not be able to distinguish its own valid coins from forged ones. Since there is no way to guarantee that the Bank's secret keys will never be compromised, it is important to limit the damage that a compromise could inflict. This could be done by limiting the total value of coins issued with a particular key, but lowering these limits also reduces the anonymity of the system since there is a smaller pool of coins associated with each key.

The untraceability property of electronic cash creates problems in detecting money laundering and tax evasion because there is no way to link the payer and payee. To counter this problem, it is possible to design a system that has an option to restore traceability using an escrow mechanism. If certain conditions are met (such as a court order), a deposit or withdrawal record can be turned over to a commonly trusted entity who holds a key that can decrypt information connecting the deposit to a withdrawal or vice versa. This will identify the payer or payee in a particular transaction. However, this is not a solution to the token forgery problem because there may be no way to know which deposits are suspect. In that case, identifying forged coins would require turning over all of the Bank's deposit records to the trusted entity to have the withdrawal numbers decrypted.

We have also looked at two optional features of off-line electronic cash: transferability and divisibility. Because the size of an electronic coin must grow with each transfer, the number of transfers allowed per coin must be limited. Also, allowing transfers magnifies the problems of detecting counterfeit coins, money laundering, and tax evasion. Coins can be made divisible without losing any security or anonymity features, but at the expense of additional memory requirements and transaction time.

In conclusion, the potential risks in electronic commerce are magnified when anonymity is present. Anonymity creates the potential for large sums of counterfeit money to go undetected by preventing identification of forged coins. Anonymity also provides an avenue for laundering money and evading taxes that is difficult to combat without resorting to escrow mechanisms. Anonymity can be provided at varying levels, but increasing the level of anonymity also increases the potential damages. It is necessary to weigh the need for anonymity with these concerns. It may well be concluded that these problems are best avoided by using a secure electronic payment system that provides privacy, but not anonymity.

Report's References

1. Stefan Brands, Untraceable Off-Line Cash in Wallets with Observers, Advances in Cryptology CRYPTO '93, Springer-Verlag, pp. 302-318.
2. David Chaum, Achieving Electronic Privacy, Scientific American (August 1992), 96-101.
3. David Chaum, Security without Identification: Transaction Systems to make Big Brother Obsolete, ACM 28 no. 10 (Oct 1985), 1030-1044.
4. David Chaum, Amos Fiat, and Moni Naor, Untraceable Electronic Cash, Advances in Cryptology CRYPTO '88, Springer-Verlag, pp. 319-327.
5. David Chaum and Torben Pedersen, Transferred Cash Grows in Size, Advances in Cryptology - EUROCRYPT '92, Springer-Verlag, pp. 390-407.
6. David Chaum and Torben Pedersen, Wallet Databases with Observers, Advances in Cryptology CRYPTO '92, Springer-Verlag, pp. 89-105.
7. Tony Eng and Tatsuaki Okamoto, Single-Term Divisible Electronic Coins, Advances in Cryptology EUROCRYPT '94, Springer-Verlag, pp. 311-323.
8. Niels Ferguson, Extensions of Single-term Coins, Advances in Cryptology - CRYPTO '93, Springer-Verlag, pp. 292-301.
9. Niels Ferguson, Single Term Off-Line Coins, Advances in Cryptology - EUROCRYPT '93, Springer-Verlag, pp. 318-328.
10. Alfred J. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, Boston, 1993.
11. Tatsuaki Okamoto, An Efficient Divisible Electronic Cash Scheme, Advances in Cryptology - CRYPTO '95, Springer-Verlag, pp. 438-451.

I have done my part, now do yours. If you want to learn more, get the Report!

So, who is the inventor, NSA or Satoshi Nakamoto some 12 years later? You may surmise that Satoshi Nakamoto may have been "invented" by the NSA! It is also interesting to note that the Report was first published by an MIT mailing list and the second being much more prominent, The American Law Re*view* (Vol 46, Issue 4). It has also been observed and it is evident that SHA-256, the algorithm Satoshi used to secure Bitcoin, was not available because it came about in 2001. However, SHA-1 would have been available to them, having been published in 1993.

Now, you must research much more on the algorithm SHA-256 and SHA-1!

If you think that I am in a minority, read the below quote from:

https://www.ccn.com/nsa-bitcoin-1996/

Certainly, information security and the National Security Agency are intertwined. The NSA regularly publishes new stable and experimental algorithms. It is up to the public how we implement and use them. If it comes out that the NSA has been behind Bitcoin all along, does that change its value? After all, the NSA is the biggest snoop in town these days, keeping massive logs of metadata on phone calls with many speculating that they are doing a little more than that even…. they are keeping the contents of the phone calls as well. And as for secure e-mail: PGP was declared dead almost a year ago. What do you think? Is Satoshi in fact an NSA agent? What does this imply for the sanctity of Bitcoin? Does this prospect comfort or discomfort you?

Before I finished off the discussion, maybe the observations from Martin Armstrong may shatter your faith and "investments" in Bitcoin and other crypto currencies.

*The general talk has been that the end of the **fiat monetary system** is imminent. Central bank digital currencies allegedly threaten the US dollar, according to some very shallow reasoning*

and a total lack of understanding about why the dollar is even the reserve currency. Beyond that delusion, these people claim that cryptocurrency will end fiat currency. ***However, private crypto-currency is not backed by anything, either.***

Today's transactions are mostly digital,so converting paper dollars to cryptocurrency will not dramatically alter the economy. *The UN and IMF are simply trying to take over the world for a power play. They do not have armies or economies to qualify for the world's financial capital. They are drunk with this delusion of power that they can rule the world by sheer decree. From the very beginning, the elite saw in their vision that they would dominate the world and end democracy.*

Getting knowledge and analysing financial intelligence is hard work, even for the professionals within the Intel Community.