*

In this project we propose to investigate a novative system of payment the BitCoin. After compiling some documentation we decided to investigate three (3) different security problems:

- the first one is the heart of this system : forgery of a proof of work;
- the second is the notion of **anonimity** during a transaction;
- the third issue we choosed to focus on was an anomaly in the transaction record detected by Dorit Ron & Adi Shamir in their 2012 paper [1].

First draft of the article with simple idea and short descriptions.

A traditionnal electronic cash system (via internet or any kind of network) is based on a central authority **the mint**. This mint (or bank) is aware of all transactions, of the balance of each and evry account in his own network and is responsible of security and anonimity of the transactions. To ensure privacy the bank keeps informations only bettween the involved parties. The main advantage is the simplicity of protecting a transaction as the only requiered informations to spend money is a single identification as the bank has access to both balance of accounts and the time of the transaction. The entire intelligence (verification and issuing the keys) is tranfered into the mint so the users only need to know their own key (& id). A real problem of this system is that it relies on a single central mint. If it was to collapse evry history of transactions and evry amount of money would be lost without any chance of recovery. That's why people started to envestigate different solutions like BitCoin (based on a peer-to-peer network) for example. Here is a summary of the specifications of some "<famous"> electronnic currencies.

Table 1: Some Electronic Currencies specifications

	Mint	Public Transactions	Anonimity	PtP
Bank	Yes	No	Yes	No
Ripple	No	Yes	depends	Yes
KARMA	distributed	No	Yes	Yes
PPay	A user = Mint for evry coin he generates	No	Yes	Yes
BitCoin	No	Yes	we'll see	Yes

In the rest of this article we'll focus on one particular currency, the BitCoin.

!!Proof of work!! An attacker with more CPU power than all the other nodes on the network could benefit from it by mining (costs of maintaining such CPU power on electricity connection??) said Nakamoto. Simple verification trust a small number of nodes (security flow?) BitCoin is a peer-to-peer electronic currency system first described by S. Nakamoto in 2008 [2]. It's based on digital signature to prove ownership and an history of transactions publicly available to avoid double-spending. This history is shared using a peer-to-peer network and users agree on it using a proof-of-work system. A BitCoin (or simply coin) is a chain of digital signatures, each owner signs a hash of the prevous transaction and the public key of the next owner and adds this at the end of the coin. To avoid double-spending the system implements a distributed timestamp server based on a proof-of-work system. Each time a node is notified of transactions, it puts them in a block and then hashes a nonce (using SHA-256) and the previous hash in the proof-of-work incrementing it until it start with a predetermine number of zeros.

[1] `www.eprint.iacr.org/2012/584.pdf`

[2] www.bitcoin.org/bitcoin.pdf

Present the theory developped in "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto and deduce the complexity of an attack, based on redoing a full proof of work.

Implement a begenning of redoing a proof of work, then monitor the beginning (the entire history of transactions is available online) and extrapolate to deduce an effective complexity.

The bitcoin system of validation of a transaction allows a user to ask others if the transation is valid. To attack you may not need to redo the proof of work but just give false information. issue we can address:

- who utilise the peer validation;
- how much node is it necessary to have to make this methode of validation unreliable;
- how to detect such attak.

Present (and analyse) the complexity of the attack described in the Ron & Shamir paper. Parse the history of transactions so we can work whith it. Modify it to gain informations (merging public key belonging to the same user). Then see how to gather external information on bitcoin user. Question to answer : is it possible (and by who?) to discover the identity of bitcoin users.

Standart bitcoin transaction are single-signature transaction, however the Bitcoin network allows multi-signatures transaction (M-ofN transaction). We can espect ,in these transaction, multiple input from multiple person. We can adapt the parser to know what is the ratio multiple/single signature tansaction.

several user can provide input and sign the same output(the transaction have now multiple input made by different entity. Sevices as Mtgox might use this feature.

Using the publicly available history of transaction we can analyse anomaly in the transation flow. In this section we can utilise what we will learn about anonymity and security of bitcoin user to better understand these anomaly.