11 Digital Cash

11.1 SET

SET (Secure Electronic Transactions)

- Open encryption and security specification to protect Internet credit card transactions.
- Developed in 1996 by Mastercard and Visa.
- Not a payment system, but a set of security protocols and formats.
- Complex, using a PKI, SSL and more.
- Besides authenticity, integrity, and security, SET must also preserve privacy, keeping:
  - Payment Instructions (PI) secret to the merchant
  - Goods and Service Orders (GSO) secret to the bank

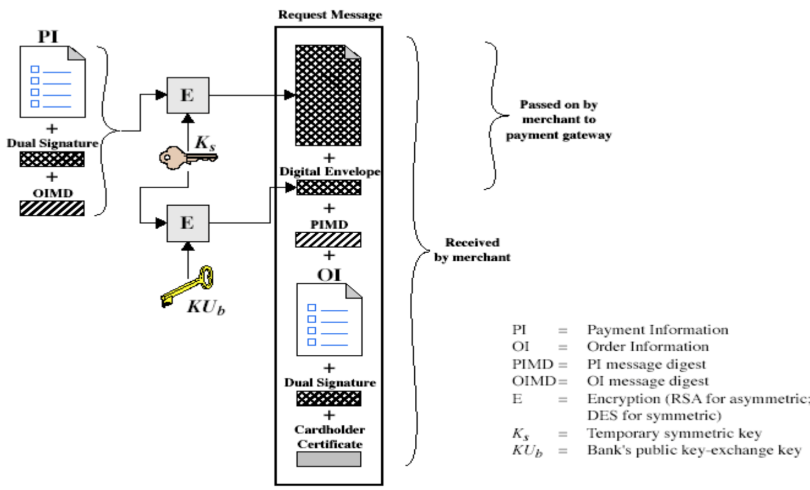
SET
SET Transactions

1. customer opens account
2. customer receives a certificate
3. merchants have their own certificates
4. customer places an order
5. merchant is verified
6. order and payment are sent
7. merchant requests payment authorization
8. merchant confirms order
9. merchant provides goods or service
10. merchant requests payment

SET
Privacy is achieved by dual signatures:

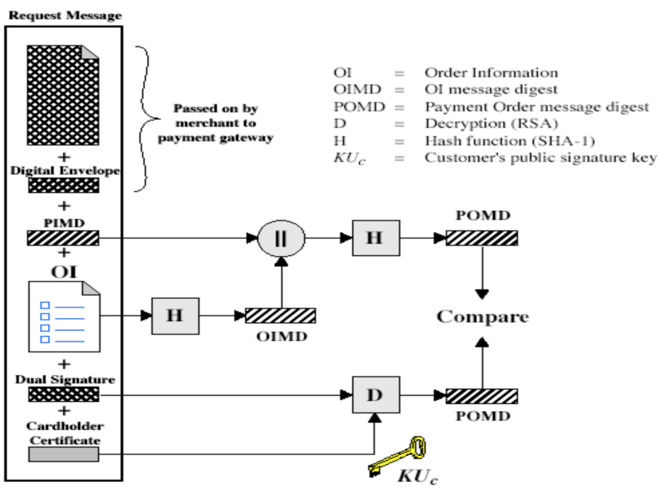
1. cardholder sends merchant: $\{GSO\}_{K_M^+}, \{PI\}_{K_B^+}, H(\{PI\}_{K_B^+})$ and digital signature $DS = \{H(H(\{PI\}_{K_B^+})||H(\{GSO\}_{K_M^+}))\}_{K_C^-}$.
2. merchant checks that $H(H(\{PI\}_{K_B^+})||H(\{GSO\}_{K_M^+})) = \{DS\}_{K_C^+}$, decrypts $\{GSO\}_{K_M^+}$ and sends bank $H(\{GSO\}_{K_M^+}), \{PI\}_{K_B^+}$ and DS.
3. bank checks that $H(H(\{PI\}_{K_B^+})||H(\{GSO\}_{K_M^+})) = \{DS\}_{K_C^+}$, decrypts $\{PI\}_{K_B^+}$ and sends merchant a digitally signed authorization encrypted with K_M^+.
4. merchant checks the signature and gives cardholder a digitally signed receipt encrypted with K_C^+.

SET
Purchase Request: Customer



SET

Purchase Request: Merchant



SET
Purchase Request: Merchant

1. verifies cardholder certificates using CA signatures.
2. verifies dual signature using customer's public signature key to ensure order has not been tampered with in transit and that it was signed using cardholder's private signature key.
3. processes order and forwards the payment information to the payment gateway for authorization.
4. sends a purchase response to cardholder.

SET
Payment Gateway Authorization

1. verifies all certificates.
2. decrypts digital envelope of authorization block to obtain symmetric key and then decrypts authorization block.
3. verifies merchant's signature on authorization block.
4. decrypts digital envelope of payment block to obtain symmetric key and then decrypts payment block.
5. verifies dual signature on payment block.

6. verifies that transaction ID received from merchant matches that in PI received (indirectly) from customer.
7. requests and receives an authorization from issuer.
8. sends authorization response back to merchant.

SET
Payment Capture

1. merchant sends payment gateway a payment capture request.
2. gateway checks request.
3. then causes funds to be transferred to merchants account.
4. notifies merchant using capture response.

11.2 Bitcoin

Digital Cash
There have been many proposals for digital cash.
Until recently, none of the proposals have really taken off.
Requirements:

1. Secure transfer in computer networks
2. Cannot be copied and reused
3. Anonymity
4. Offline transactions
5. Can be transferred to others
6. Can be subdivided

Digital Cash
Most proposals use a centralized system:

- Tied to a traditional currency.
- No real gain over existing systems.

It would be better to create a system with distributed consensus:

- A currency that is peer-to-peer.
- All functions of a bank can be taken over by the network.

Bitcoin
The Bitcoin protocol was proposed by S. Nakamoto in 2009.

- Creation of new currency
- Secure transactions
- Protection against double-spending
- Anybody can be a "merchant" or a "customer"
- Pseudo-anonymity

Bitcoin
We will try to create a peer-to-peer currency step by step.
First attempt: public signed transactions
Alice publishes a signed message: "I, Alice, send one Bitcoin to Bob"
Good points:

- Bob can verify the signature as being from Alice
- The transaction cannot be undone

Bad points:

- No account balances
- Infinite number of Bitcoins
- Very incomplete...

Bitcoin
Second attempt: serial numbers
Alice publishes a signed message: "I, Alice, send Bitcoin number 856034 to Bob"
Duplicate transactions are easily spotted, but how are the serial numbers created?

- The (too) easy solution: a trusted source, like a bank.

We remove the central point of trust:

- Instead, we establish a list of all transactions ever made.
- Computing an account balance is done by summing over all previous transactions for that account.
- This list is called the blockchain and is shared by all users.

Bitcoin
Third attempt: the blockchain
Bob checks his blockchain before accepting the transaction

- If he sees that the Bitcoin in question is owned by Alice, he accepts it.
- After the transaction is complete, Bob broadcasts his acceptance.
- As soon as the other peers hear this broadcast, they will not allow double-spending.

Alice can perform a double-spend before the acceptance broadcast is heard by enough peers

- To solve this problem, we make Bob ask everybody else if a transaction is valid.
- Double-spending will be noticed before payment is accepted.

Bitcoin
How many answers should Bob require? How can the answers be trusted?

- A "majority vote" is impossible, if Alice spams Bob with false confirmations.
- There is no way to perform traditional authentication.
- But Bitcoin won't work if transactions can't be reliably verified...

The finished Bitcoin protocol uses Proof of Work (PoW).

- Basic idea: We only trust solutions that are accompanied by a proof of someone having committed a large amount of resources to a problem.
- That is, we don't authenticate a user, but we authenticate the fact that time/money/energy/etc. has been spent.
- In order for Alice to make a double-spend, she first has to spend energy before Bob trusts her.

Bitcoin
We want a problem with the following properties:

- is difficult to solve
- has solution(s) that are easy to verify
- has scalable difficulty

A cryptographic hash function is pre-image resistant, so finding pre-images is the perfect proof of work.
The verifications are done by miners:

- For transaction message m, a miner selects a random k and computes $h(m+k)$.

- If $h(m+k) > T$ (where T is the threshold), the miner chooses a new k and tries again.
- After a long time we get $h(m+k) < T$ and the miner broadcasts k.
- Bob receives k and checks that $h(m+k) < T$.

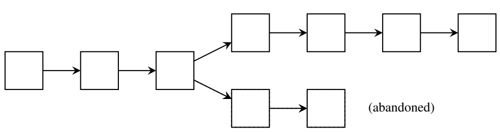
Bitcoin
Let the threshold T be so that the hash value $h(m+k)$ needs five leading zeros and let m ="AAA"

$m+k$	$h(k+m)$
AAA0	802dbe2e69...
AAA1	bbfce0d522...
AAA2	7bb4db476f. .
...	...
AAA770239	00000921ac...
k = 770239 is a valid solution	

Note that in the normal case, k is chosen randomly.
There are several solutions k to the problem $h(m+k) < T$

Bitcoin

- A block is a large number of transactions.
- The process of turning transactions into blocks is mining.
- Mining is a competition to find a solution.
- The blocks are numbered and form a long chain, the blockchain:



If two miners find a valid block simultaneously, the resolution strategy is to randomize and then work on the longest chain.

Bitcoin
The only way for Alice to cheat is the following:

1. Buy a supercomputer
2. Save up money for the electric bill
3. Broadcast an invalid transaction m to Bob
4. Let the supercomputer search for a block containing m.

5. The computer must be faster than everybody else's, combined.

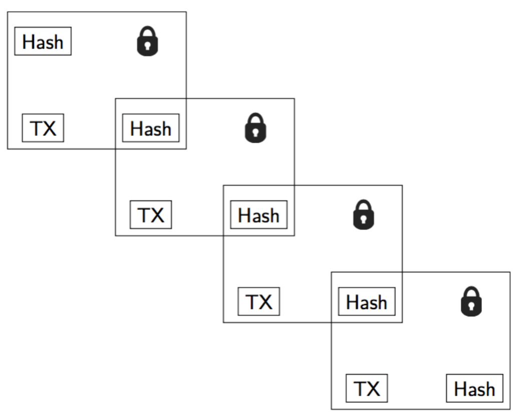
6. Even if she manages to solve an "illegal" block, no other miner will accept it.

Alice has a hard time cheating Bob.
Even if she has 1% of the hashing power, the chance of mining six blocks in a row is $(0.01)^6 = 1 \times 10^{-12}$.

Bitcoin
Bitcoin is quite robust against man-in-the-middle attacks:

- Assume that Alice and Bob have a good copy of the blockchain.
- Eve cannot intercept the transaction and take the money, since Alice and Bob require a proof of work.
- Eve would have to spend a very long time finding a block, so Alice and Bob would notice.

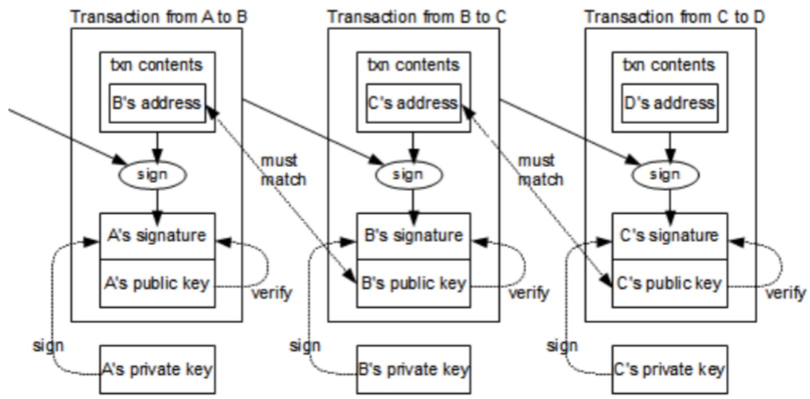
Bitcoin
Each block gives security to the previous ones:



Bob waits a number of blocks before accepting Alice's transaction.

Bitcoin

Detailed view of a transaction:



Bitcoin

- Digital signatures initiate the transaction
- Miners verify the transactions
- Bob accepts the transaction after six successive blocks (takes one hour)
- New currency is created by rewarding miners
- All transactions are in the blockchain
- The threshold T provides a way to adjust the difficulty of the proof of work.
- Bitcoin also has built-in inflation control: every fourth year the mining reward is halved.
- In Bitcoin, the users only need to trust the algorithm, nothing else.
- Transactions are safe, storage is not.