**Chapter 4. How to store and use Bitcoin**

1. Simple local storage.

* Lưu private key trong file, trong máy tính cá nhân hoặc trên điện thoại.
* Chỉ có sẵn trên thiết bị của bạn nên khi thiết bị bị mất hoặc bị xóa thì key sẽ mất -> mất coins.
* Phụ thuộc vào mức độ bảo mật trên thiết bị. Nên khi thiết bị bị xâm nhập thì key sẽ bị rò rỉ -> mất coins.

1. Wallet software.

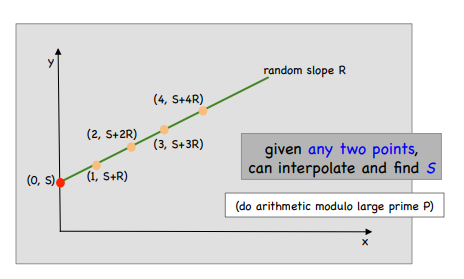
* Theo dõi tiền xu của mình.
* Có giao diện người dùng nên dễ sử dụng.
* Sử dụng từng địa chỉ/khóa cho từng coin.
* Đối với loại ví này, các ứng dụng sẽ không lưu trữ các thống tin khóa bí mật cá nhân của bạn trên các máy chủ và do đó, tiền của bạn nằm dưới sự kiểm soát của bạn chứ không phải của người khác.
* Nhược điểm: khi máy tính bị đánh cắp hoặc ổ cứng bị hư hỏng, thì bạn sẽ bị mất hết toàn bộ số bitcoins đang sở hữu

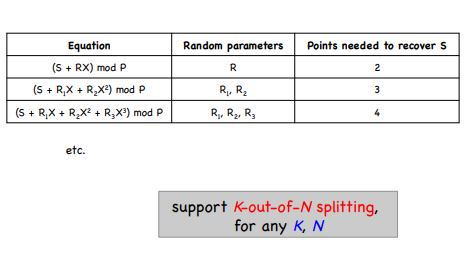
1. Hot wallet and Cold wallet.
   1. Hot wallet.

* Hot wallet là địa chỉ ví (Address) mà người dùng có thể chi tiêu tiền điện tử từ bất kỳ thời điểm nào và hầu như bạn luôn luôn phải kết nối với Internet để có thể duy trì kết nối với mạngBitcoin.
* Hot wallet thường được dùng để tiêu tiền cho bất cứ hoạt động mua bán, giao dịch, ở mọi thời điểm (lưu trữ online).
  1. Cold wallet.
* Cold wallet dùng để lưu trữ bitcoins dưới dạng offline.
* Chỉ sử dụng khi không có sử dụng Bitcoin để chi tiêu thường xuyên, nhưng vẫn có thể nhận được tiền gửi từ những người khác tới bất cứ lúc nào.
* Cold wallet có ưu điểm là không cần kết nối trực tiếp internet, vì nó được sử dụng để lưu trữ Bitcoin ngoại tuyến. Và khi không có kết nối giữa Cold wallet và internet thì Hacker sẽ không thể đánh cắp tiền trong ví của mình được.

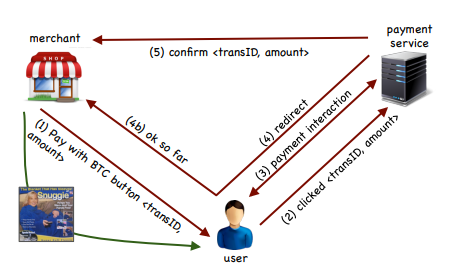
1. Spliting and Sharing keys
   1. Secret Sharing

* Idea: chia private key thành N mảnh, có nghĩa là nếu ta cho K mảnh bất kỳ, ta có thể tái tạo lại private key với số mảnh ít hơn K mảnh.
* Ví dụ: N = 2, K = 2. Có nghĩa là ta chia private key thành 2 mảnh. Và ta cần 2 mảnh này để ghép lại thành 1 private key hoàn chỉnh.
  + P : số nguyên tố lớn.
  + S: secret trong khoảng [0, P-1).
  + R: random trong khoảng [0, P-1).
  + Splitting:
    - X1 = (S+R) mod P
    - X2 = (S+2R) mod P
  + Reconstruct:
    - (2X1 – X2) mod P = S





* 1. The Good and the Bad of Secret Sharing
* The good: lưu trữ các mảnh riêng biệt, nên nếu muốn lấy được private key thì phải thỏa hiệp một số điều kiện thì mới có thể lấy được khóa.
* The bad: nếu muốn thực hiện giao dịch, thì ta phải cần đến các mảnh của khóa và reconstruct lại để thành private key, đây là nhược điểm chủ yếu của việc chia private key thành nhiều mảnh.
  1. MULTI – SIG
* Multi – sig chủ yếu được áp dụng trong doanh nghiệp, nơi mà có sử dụng khái niệm đồng sở hữu. Đây là 1 dạng tài khoản dùng chung mà chỉ khi có đủ chữ ký số tối thiểu cần thiết thì mới có thể rút tiền được ra khỏi tài khoản.
* Cách thức hoạt động của ví Multi – sig.
  + Giả sử một ví đồng sở hữu của 3 người và chúng ta thiết lập điều kiện cho nó là khi có ít nhất 2 người cùng chấp thuận việc chi tiêu trở lên thì việc chi tiêu mới có hiệu lực, thì một người có thể khởi tạo giao dịch, và giao dịch chỉ thực hiện khi có ít nhất một người nữa chấp nhận thì việc chuyển tiền mới có hiệu lực.
  + Còn việc nhận tiền thì không cần phải ai chấp nhận cả. Nó cũng giống như các ví điện tử thông thường, việc nhận tiền thì người nhận không cần online, không cần bật máy, thông tin giao dịch vẫn được ghi nhận trên blockchain và được đồng bộ khắp nơi, và khi bật máy người chủ ví có thể kiểm tra được thông tin về số tiền mình nhận.
  1. Online wallet.
* Cách thức lưu trữ giống local wallet nhưng local wallet lưu trữ ở local còn online wallet lưu trữ trên cloud, chạy trên browser, các website sẽ gửi mã, lưu trữ private key và phải log in thì mới truy cập vào wallet được.
* Ưu điểm: tiện lợi, không cần phải cài đặt để sử dụng, chạy được ở nhiều thiết bị
* Nhược điểm: vì là lưu trên cloud nên độ bảo mật không cao. Có nhiều trang web giả mạo để nhằm lấy Bitcoin của mình.
  1. Bitcoin Exchanges (Sàn giao dịch Bitcoin)
* Cho phép ký gửi Bitcoin và fiat currency
* Cho phép rút ra khi có nhu cầu sử dụng.
* Fiat currency: là loại tiền được chính phủ công nhận nhưng không được bảo chứng bằng giá trị vật chất.
* Cho phép khách hàng:
  + Giao dịch và thanh toán Bitcoin
  + Mua/bán Bitcoin theo các ngoại tệ hiện hành.
  + Thông thường, sẽ liên kết giữa người mua và người bán.

1. Payment Services.
   1. Payment Processing.

Kết quả:

* Customer: tiêu Bitcoin
* Merchant: nhận được tiền (dollars), khấu trừ phần trăm tỉ lệ chuyển đổi.
* Dịch vụ Payment:
  + Nhận Bitcoins
  + Trả tiền mặt (dollars)
  + Tiếp nhận rủi ro: Bảo mật, tỉ giá chuyển đổi.
  + Cần chuyển đổi từ Bitcoin sang tiền mặt (dollars), theo khối lượng.

1. Transaction Fees

Phí cho một giao dịch là tự nguyện, thông thường là 0.0001 BTC. Bạn có thể trả thêm phí để hấp dẫn hơn các miner, giúp giao dịch mau được kiểm chứng hơn.