Distributing Trust and Blockchains		Date:	*17 October 2019*
Instructor: *Sujit Prakash Gujar*		Scribes:	Abhigyan Ghosh, Samanvaya Panda

Lecture 11: Bitcoin Storage, Bitcoin and Anonymity

1 Recap

1.1 Bitcoin Storage

1. Storing and managing private keys is sufficient enough for storing bitcoins.
2. Storing and managing keys involves trade-offs between :-
   - Availability :- Able to spend coins whenever you desire.
   - Security :- Others shouldn't be able to spend your coins.
   - Convenience :- Managing keys should be an easy task.

1.2 Local Storage of Bitcoins

1. Storing bitcoins on local machine like on a laptop or smartphone is not advisable because though it may appear to be very convenient, it is not good for security and availability.
2. Your device could get damaged or key file gets corrupted. In that case, your keys may not be available to you. Also, your device could be hacked or stolen. In that case, others can have access to your private keys which violates security principles.
3. However if you still want to store them locally then different techniques used to store bitcoin addresses are :-
   - Wallets :- They provide more convenience and better security(anonymity) by generating multiple private/public key pairs.
   - Base58 encoding :- A number can be encoded as an alphanumeric sequence using base58 encoding. Since, 58 is not a perfect power of 2, so base58 encoding doesn't divide binary data properly. Thus, it can be used only for integer addresses.
     The characters missing in base58 encoding are 0, O, l, 1.

Value	Character	Value	Character	Value	Character	Value	Character
0	1	1	2	2	3	3	4
4	5	5	6	6	7	7	8
8	9	9	A	10	B	11	C
12	D	13	E	14	F	15	G
16	H	17	J	18	K	19	L
20	M	21	N	22	P	23	Q
24	R	25	S	26	T	27	U
28	V	29	W	30	X	31	Y
32	Z	33	a	34	b	35	c
36	d	37	e	38	f	39	g
40	h	41	i	42	j	43	k
44	m	45	n	46	o	47	p
48	q	49	r	50	s	51	t
52	u	53	v	54	w	55	x
56	y	57	z				

Figure 1: Base58 encoding for different characters[1]

[1] https://en.bitcoin.it/wiki/Base58Check_encoding#Base58_symbol_chart

- QR codes :- QR(Quick Response) code converts the private address into a 2-D barcode which can used as an image.
- Vanity address :- Vanity addresses contain a human meaningful string as an prefix in the address.
  Expected no.of trails required to generate a base58 encoded address with a prefix = 58^k where k is length of prefix string

1.3 Hot and cold Storage

1. Hot storage is storing bitcoins in online mode(on laptop or smartphone connected to internet) whereas cold storage is storing bitcoins in offline mode.
2. Both hot and cold storage use different set of addresses to ensure that if one them is compromised other one remains safe.
3. New bitcoins are received at hot storage and transferred later to cold storage.
4. Some examples of cold storage are:-
   - Paper Wallet :- The bitcoin address(base58 encoded or QR code) is printed on physical paper and stored in some safe or vault.
   - Hierarchical wallet :- Private and public key pairs are generated sequentially using key generation information rather than just single pair of key. If (k, y, g) are key generation information then :-
     - i^{th} private key : $x_i = y + H(k||i)$
     - i^{th} public key : $g^{x_i} = g^{H(k||i)} * g^y$
     - i^{th} address: $H(g^{x_i})$
   - Brain Wallet :- Private and public key pairs are generated from a passphrase chosen by the user. It is recommendable to chose a passphrase consisting of 6 words out of 10000 most frequently used words.
   - Tamper-resistance devices :- Using tamper-resistant that either store your keys or generate them. Instead of outputting your key, it will sign your statements when some password is entered. They are also called as hardware wallets.
5. Entropy :- It is the measure of degree of randomness of any particular distribution. It is defined as :-
   $$H(X) = -\sum_{k \geq 1} p_k log(p_k)$$
   where X is discrete random variable.
6. For a passphrase consisting of 6 out 10000 most frequently used words, entropy can be calculated as follows :-
   $$\begin{aligned} H(X) &= -6 \sum_{k=1}^{10000} \frac{1}{10000} log_2(\frac{1}{10000}) \\ &= 6 log_2(10000) \\ &\approx 80 \end{aligned}$$
   So, the passphrase has 80 bits of entropy.

1.4 Splitting and Sharing Keys

1. Instead of storing keys at one place, we could spilt our keys and store them at different locations to avoid any single point failure.
2. But splitting the key would give information about the real key and decrease the computations exponentially for the adversary.
3. So instead of splitting the key, we create N shared components of the key out of which K components are sufficient to construct the key back. With less than k shares, it is not possible to uniquely construct the key.
4. This can be achieved by using polynomial(Lagrange) interpolation. We try to fit a $k-1$ degree polynomial using k different points. But with fewer points than k, a polynomial of degree k can't be uniquely determined. Once the polynomial is fixed, we could choose N different points on the curve out of which k points are sufficient to construct back the polynomial.
5. Multi-signatures :- Instead of trying to split or share the key and store over different devices, we could use multiple signatures required to create a valid transaction. We could use pay to script method in Bitcoin to achieve this.

2 Online Wallets

1. Instead of storing bitcoins ourselves, we could use online services that could that for us. These are called online wallets.
2. They store your keys by encrypting using a password provided by you or have at least access to them.
3. Advantages :-
   - They can be used conveniently used from an online browser on your laptop or as a mobile app on your smartphone.
   - The people maintaining these wallets are security professionals. So, they are better at protecting your keys than you.
4. Disadvantages :-
   - If the site turns out to be malicious, then they could run away with all your bitcoins.
   - If the service provider gets hacked or compromised, then your bitcoins may be at risk.
5. Some of the popular online wallets are Coinbase, Electrum, Mycelinum and blockchain.info.

Figure 2: Some popular online wallets

3 Bitcoin Exchanges

1. To acquire bitcoins, we could start mining. But mining bitcoins requires a lot of computing resources and doesn't guarantee quick returns.
2. Instead we could perform bitcoin exchanges to acquire bitcoins.
3. Bitcoin exchanges may accept bitcoins or fiat currency as deposits and promise to pay them back on demand in either bitcoins or fiat currency or both. These are called as demand deposits.
4. They also convert bitcoins to fiat currency and vice-versa. They usually do this by matching interested parties which are willing to sell bitcoins at a certain price that is acceptable to the party willing to buy.
   Example :- Suppose A had $10000 and 5 bitcoins. Now he wants to buy 3 more bitcoins sold at a price $1000/coin. So, now exchange will promise him to pay $7000 and 8 bitcoins.
5. No actual transaction happens on bitcoin blockchain.
6. Advantages
   - Helps to control flow between price of bitcoin and fiat currency.
   - Makes it easy to exchange bitcoin with fiat currency back and forth.
7. Disadvantages
   - Exchanges may face bankrun when all the people simultaneously come to withdraw their money. In that case, the exchange may not able to fulfill all the promises.
   - The owners of exchanges might turn out to be fraud and run away with all your money.
   - The exchanges may get hacked due to software bugs. In that case, you may lose all your money.
8. 18 out 40 exchanges fail due to their inability to pay their customers back. Mt.Gox is famous example which filed bankruptcy because most of its bitcoins were stolen.

4 Currency Exchange Rate

1. Supply of bitcoins refers to the no.of bitcoins are present in the market for circulation. Most of the calculations regrading supply of bitcoins ignore demand deposits in exchanges.
2. Demand for bitcoins exists in the market because they act an way of mediating fiat currency transactions. Also, bitcoins act as an source of investment.
3. Determining the market price of bitcoin :-
   - Let S = Total supply of bitcoins.
   - Let D = Duration for bitcoin is circulated.
   - Let T = Total transaction value of bitcoin per second($/s)
   - Let P = Price of bitcoin
   - At equilibrium, supply/second = demand/second
     $\implies \frac{S}{D} = \frac{T}{P}$
     $\implies P = \frac{TD}{S}$

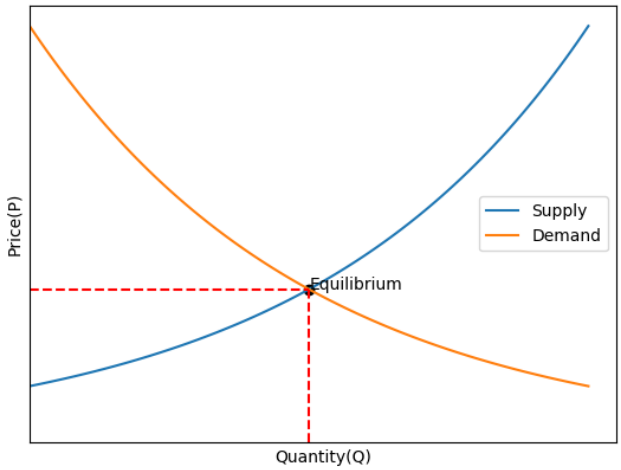

Figure 3: Supply-Demand plot

5 Bitcoin and Anonymity

1. What is Anonymity?

   Definition 1 (Merriam Dictionary)**.** *not named or identified*

   Definition 2 (Oxford Dictionary)**.** *Having no outstanding, individual, or unusual features; unremarkable or impersonal.*

2. Is Bitcoin Anonymous?

   (a) My identity is $RIPEMD160(SHA256(publickey))$

   (b) Can anyone know my real world identity from my address?

   (c) Two meanings of anonymity

      i. Without your real identity

      ii. Without any identity

   (d) Is Bitcoin anonymous? - It is pseudo-anonymous

3. What is the requirement?

   - Privacy
   - Why?
     (a) Competitors of a production company may know how much I am producing by looking at amount I credit at vendors
     (b) It is more dangerous than centralized currency if an adversary can link my real life identity to my Bitcoin transactions
   - Thus, $Anonymity = PseudoIdentity + Unlinkability$

4. Unlinkability

   – Hard to link different addresses of same user

   – Hard to link different transactions made by the same user

- Hard to link the sender of payment to its recipient
- Isn't the last one obvious not to be satisfied?

5. Anonymity Set
   - It is difficult to have complete unlinkability
   - Instead:
     - Given a set of transactions, adversary should not be able to detect which one belongs to you
     - This set is called anonymity set
     - Bigger the anonymity set, the more desirable
6. Different Addresses: Every time you receive money at a different account
7. Ethics
   - There is always an ethical question: Can technology help in having anonymity for good use cases and bad use cases are prohibited?
   - Current answer is *NO*
8. Stealth Address
   (a) Mohit publishes g, y such that $y = g^x \pmod{p}$
   (b) Amit selects a random r and sends money to $H(y^r)$
   (c) Communicates r securely to Mohit
   (d) Private key to redeem these coins: xr
   - Dark Wallet
   - Cryptonote
9. Side Channel Attacks
   - Try to observe activity on Bitcoin network and other social media networks. There is a high probability that I am active on BTC network, I am also active on some social media during that period
   - *Netflix Challenge*
     - They published anonymised datasets and you need to predict user's ratings on movies
     - Winning team gets $10 million
     - Was conducted in 2007,2008 and 2009
     - 2010 had to be canceled
     - University of Austin, Texas linked identities of users by linking them with IMDB ratings

Definition 3 (def)**.** *Any important definitions will go here*

Theorem 1. *Theorems should go in this environment*

References