DeFi AND THE Future of Finance

Course II:

DeFi Primitives

4. Joining the World of DeFi

(ii) Blockchain Tech Big Picture

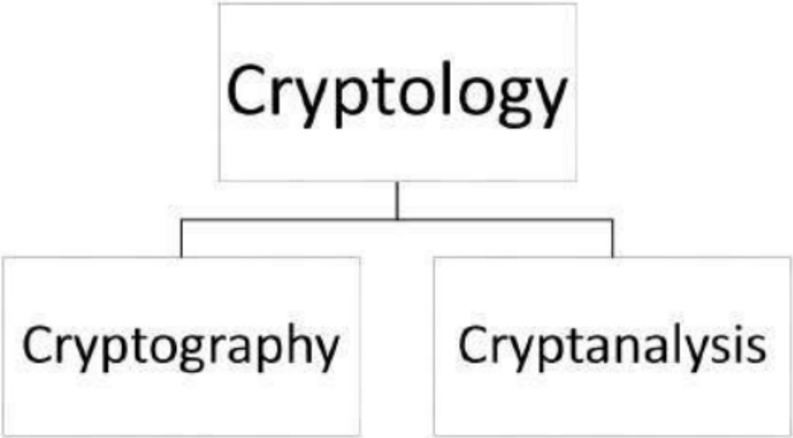
a) Hashes and keys

Tech Big Picture

Key ingredients

- **Hashing function**: provide the chain (the entire last block as the header of the next). Bitcoin SHA-256; Ethereum Keccak-256 (SHA-3). One way cryptographic function (infeasible to go the other way)
- Hashing is a one-way function. It is not encryption – though it is little confusing it is called a cryptographic function

Tech Big Picture



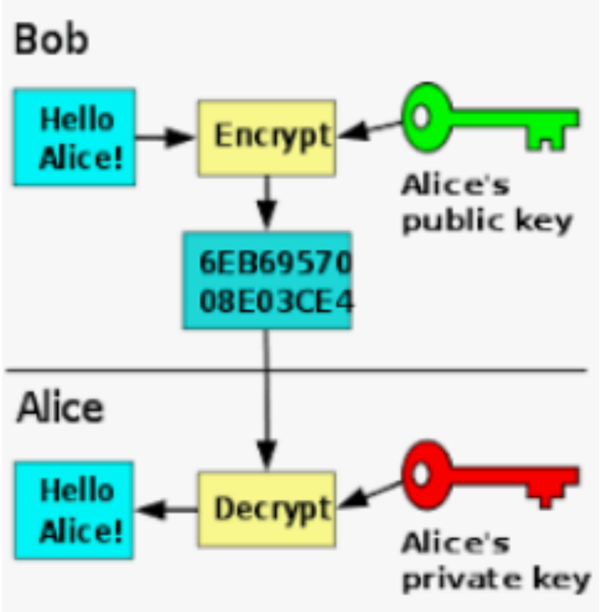
Key ingredients

- **Cryptography**: This is widely used in all aspects of blockchain. It is particularly important in deriving the public key and the DSA. We will also see that other types of cryptography are used in certain blockchain applications (for example, you might find it useful to have a contract codified in a blockchain – but you only want it visible to the contracting parties.

Tech Big Picture

Key ingredients

- **Two types of cryptography:** Symmetric key and asymmetric key
- **Private keys/Public keys**: Private key is just a random number. The public key is mathematically linked to the private key. It is easy to go from the private key to the public key – but very difficult to go from public to private. Current technology uses Elliptic Curve Cryptography (ECC)



Tech Big Picture: Asymmetric keys

Public and private keys

- A message needs to go from Sender to Receiver
- Receiver gives the Sender a lock
- Sender locks the message (ciphertext) and transmits to Receiver
- Only the Receiver can decrypt because they have the key

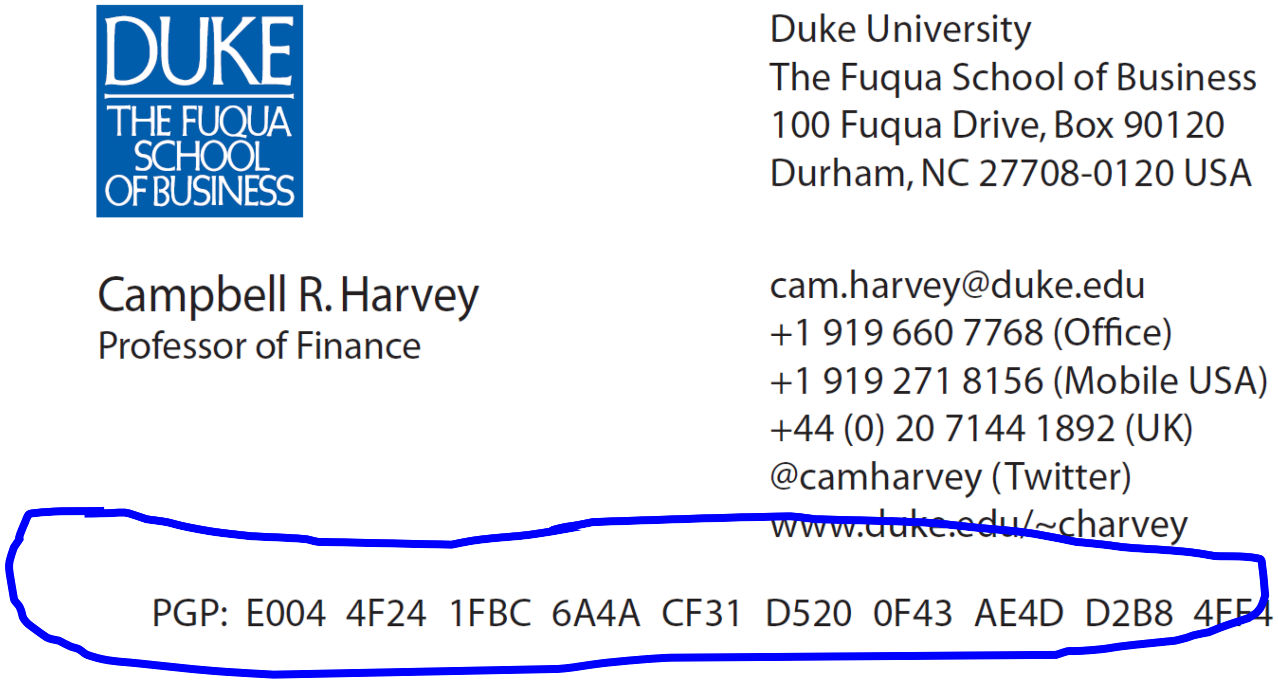
The lock is the public key

The key to open the lock is the private key

Tech Big Picture: Application: PGP Email

My public key for secure email

- You can encrypt an email to me with my public key and only I can decrypt with my private key.
- Notice that both symmetric and asymmetric cryptography is used!



DUKE
THE FUQUA SCHOOL OF BUSINESS

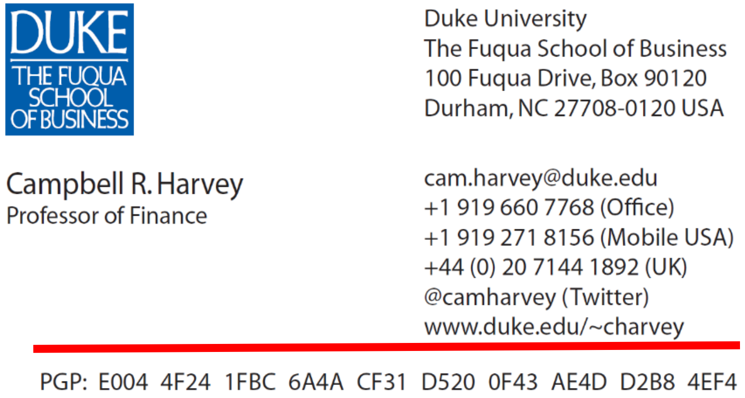
Campbell R. Harvey
Professor of Finance

Duke University
The Fuqua School of Business
100 Fuqua Drive, Box 90120
Durham, NC 27708-0120 USA

cam.harvey@duke.edu
+1 919 660 7768 (Office)
+1 919 271 8156 (Mobile USA)
+44 (0) 20 7144 1892 (UK)
@camharvey (Twitter)
www.duke.edu/~charvey

PGP: E004 4F24 1FBC 6A4A CF31 D520 0F43 AE4D D2B8 4FF4

Tech Big Picture: Application:



DUKE
THE FUQUA SCHOOL OF BUSINESS

Campbell R. Harvey
Professor of Finance

Duke University
The Fuqua School of Business
100 Fuqua Drive, Box 90120
Durham, NC 27708-0120 USA

cam.harvey@duke.edu
+1 919 660 7768 (Office)
+1 919 271 8156 (Mobile USA)
+44 (0) 20 7144 1892 (UK)
@camharvey (Twitter)
www.duke.edu/~charvey

PGP: E004 4F24 1FBC 6A4A CF31 D520 0F43 AE4D D2B8 4EF4

Steps

1. Message compressed
2. Random session key (based on mouse movements and keystrokes) is generated.
3. Message encrypted with session key ← Symmetric key
4. Session key is encrypted with receiver’s public key ← Asymmetric key
5. Encrypted message + encrypted session key sent via email
6. Recipient uses their private key to decrypt the session key
7. Session key is used to decrypt the message
8. Message decompressed

http://www.pgpi.org/doc/pgpintro/