



Blockchain foundations

Module 1 (part 3)

Part 3

How a blockchain knows that you, and not someone else, initiated a transaction?

Digital Signatures

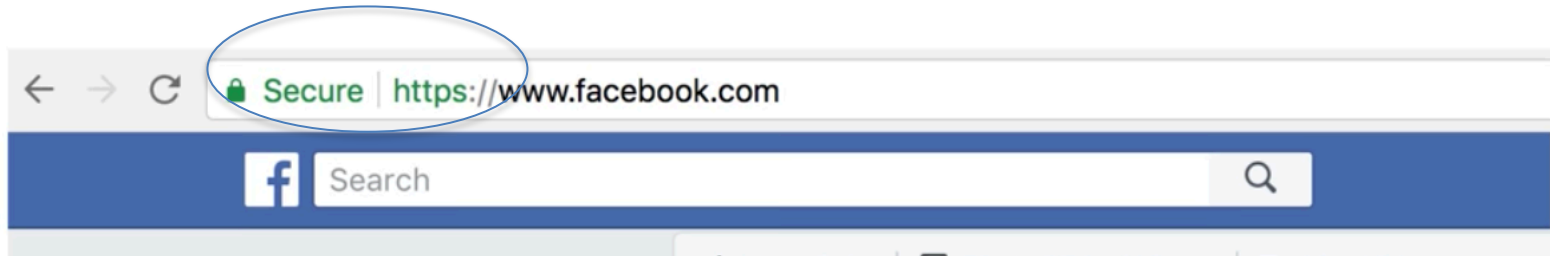
What is a digital signature?

- *A **digital signature** is a mathematical scheme for presenting the authenticity of digital messages or documents.*
- *A valid digital signature gives a recipient reason to believe that the message was created by a claimed sender (**authentication**), that the sender cannot deny having sent the message (**non-repudiation**), and that the message was not altered in transit (**integrity**).*

Where do we see them in read world?

- Digital signatures are used today all over the Internet.

In Browsers: Visit website



United States Government Printing Office (GPO)

- publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures.



- Many more practical applications...

Background

- Digital signatures employ **asymmetric cryptography**.
- Asymmetric cryptography, also known as **public key cryptography/infrastructure (PKI)**, uses public and private keys to *encrypt* and *decrypt* data.



General steps

Digital signature scheme. A digital signature scheme consists of the following three algorithms:

- **(sk, pk) := generateKeys(keysize)** The generateKeys method takes a key size and generates a key pair. The secret key *sk* is kept privately and used to sign messages. *pk* is the public verification key that you give to everybody. Anyone with this key can verify your signature.
- **sig := sign(sk, message)** The sign method takes a message and a secret key, *sk*, as input and outputs a signature for *message* under *sk*
- **isValid := verify(pk, message, sig)** The verify method takes a message, a signature, and a public key as input. It returns a boolean value, *isValid*, that will be **true** if *sig* is a valid signature for *message* under public key *pk*, and **false** otherwise.

We require that the following two properties hold:

- *Valid signatures must verify*
verify(pk, message, sign(sk, message)) == true
- Signatures are **existentially unforgeable**

Some Digital Signature/PKI algorithms

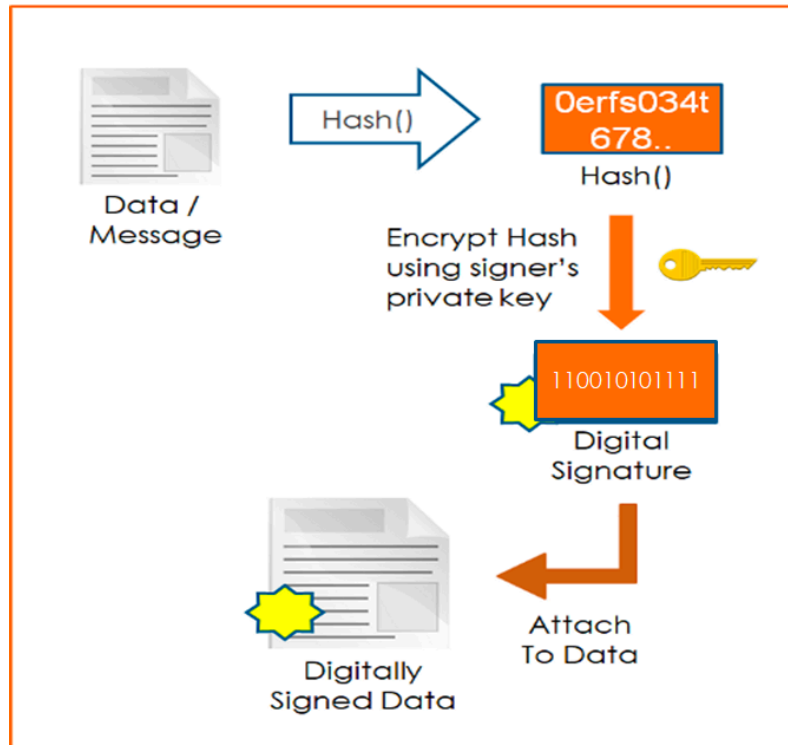
Public key cryptography has algorithms that let you encrypt, decrypt, sign and verify messages using your pair of keys

- [RSA](#)-based signature schemes
- [DSA](#)

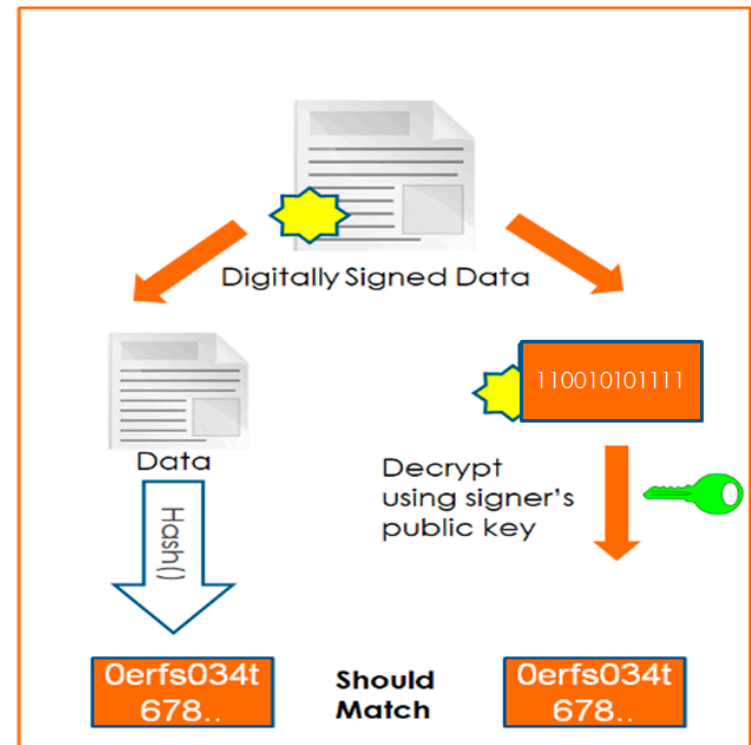
Simplified steps

- **Step 1: Generate a public/private key pair** (This can be done using software such as **Putty** for windows or via the **ssh-keygen** command for Mac or Ubuntu)
- **Step 2: Create a message hash/digest**
- **Step 3: Create the signature** (Encrypt the message digest with the private key to create a signature)
- **Step 4: Append the signature to the document**

1. Signing the message with Private Key

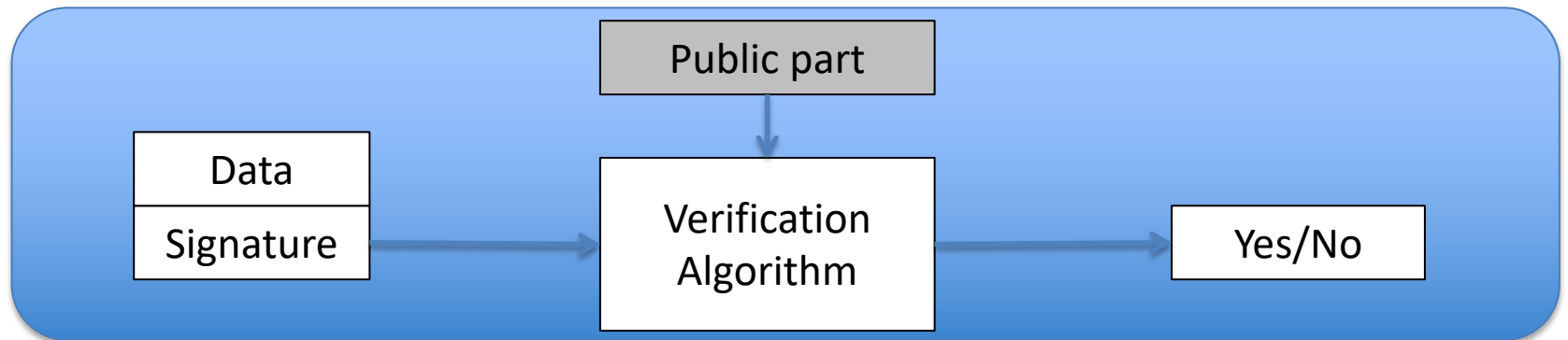
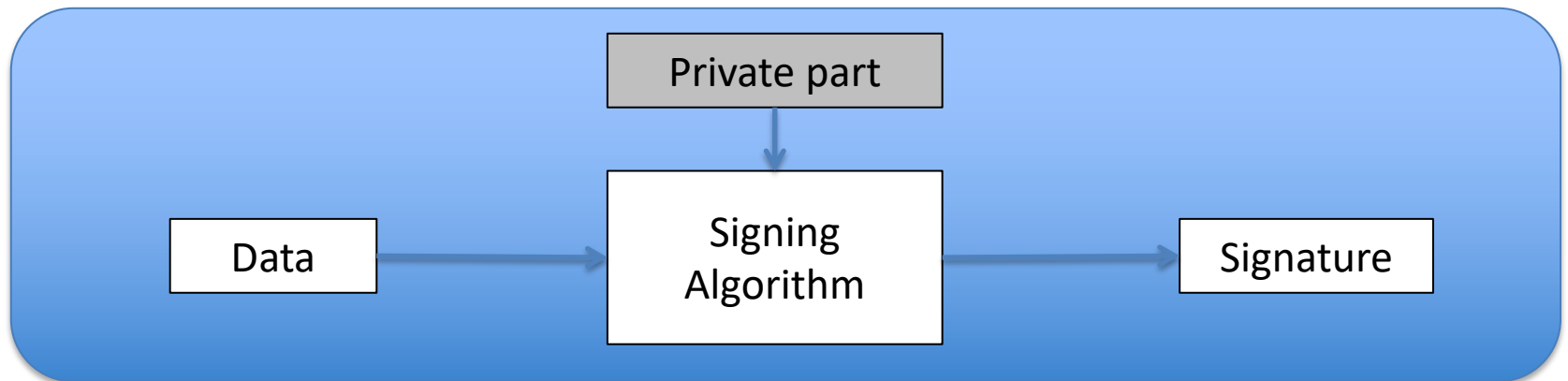


2. Verifying the message with Public Key



Digital Signatures

Signing key	
Public part	454F4D3E1..
Private part	56F23F2D..



Example demo

- <http://cobweb.cs.uga.edu/~dme/csci6300/Encryption/Crypto.html>

On blockchain

- Generating a key pair is analogous to creating an account on blockchain BUT without having to actually register any where. COOL!

How a blockchain knows that you, and not someone else, initiated a transaction?

- Every transaction is executed on the blockchain is digitally signed by the sender using their *private key*
- The signature ensures that the only the rightful owner of the account can move money out of the account...

What is the idea of public keys in blockchains?



- The idea is to take a public key, one of those public verification keys from a digital signature scheme, and equate that to *an identity of a person or an actor* in a system.
- **Decentralized identity management.** This brings us to the idea of decentralized identity management...**what does it mean?**
- **Address: just a hash of a public key**

Public key / private key in bitcoin

- If someone has your public key (i.e. “address”, they can send you money.
- If you lose your private key (i.e., “wallet”), you can’t spend your money.
- If a thief gets your private key, they can steal your money.

Private Key

Front

5K2wewraon7bWgKQDyvde7mit5716wpdNJEc1yDszgyJVEX1rgm



WALLET IMPORT FORMAT



PRIVATE KEY

5K2wewraon7bWgKQDyvde7mit5716wpdNJEc1yDszgyJVEX1rgm

PRIVATE KEY / WITHDRAW



Public Key



Account on Ethereum



LOGIN

Search by Address / Txhash / Block / Token / Ens

GO

Language

HOME

BLOCKCHAIN

TOKENS

RESOURCES

MORE

Top Accounts By ETH Balance

Home / Accounts

A total of > 1999999 Accounts found (104,396,992.811 Ether)

Displaying The Last 10000 Top Accounts Only

First

Prev

Page 1 of 400

Next

Last

Rank	Address		Balance	Percentage	TxCount
1	0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2	WrappedEther	2,026,362.46271148 Ether	1.94101612%	269514
2	0x742d35cc6634c0532925a3b844bc454e4438f44e	Bitfinex_5	1,851,983.23191054 Ether	1.77398140%	3190
3	0x53d284357ec70ce289d6d64134dfac8e511c8a3d		1,378,754.09306818 Ether	1.32068372%	14994
4	0x4e9ce36e442e55ecd9025b9a6e0d88485d628a67	Binance_6	1,207,645.15164206 Ether	1.15678155%	89
5	0x66f820a414680b5bcda5eeca5dea238543f42054		1,200,001.54258381 Ether	1.14945987%	12
6	0x61edcdf5bb737adffe5043706e7c5bb1f1a56eea		1,039,999.00001000 Ether	0.99619632%	138
7	0xab7c74abc0c4d48d1bdad5dcb26153fc8780f83e		1,000,000.01246312 Ether	0.95788201%	413
8	0xbe0eb53f46cd790cd13851d5eff43d12404d33e8		988,887.85544260 Ether	0.94723787%	8
9	0xdc76cd25977e0a5ae17155770273ad58648900d3	Huobi_6	850,860.64184765 Ether	0.81502409%	142
10	0xe853c56864a2ebe4576a807d26fdc4a0ada51919	Kraken_3	801,052.79995972 Ether	0.76731406%	151

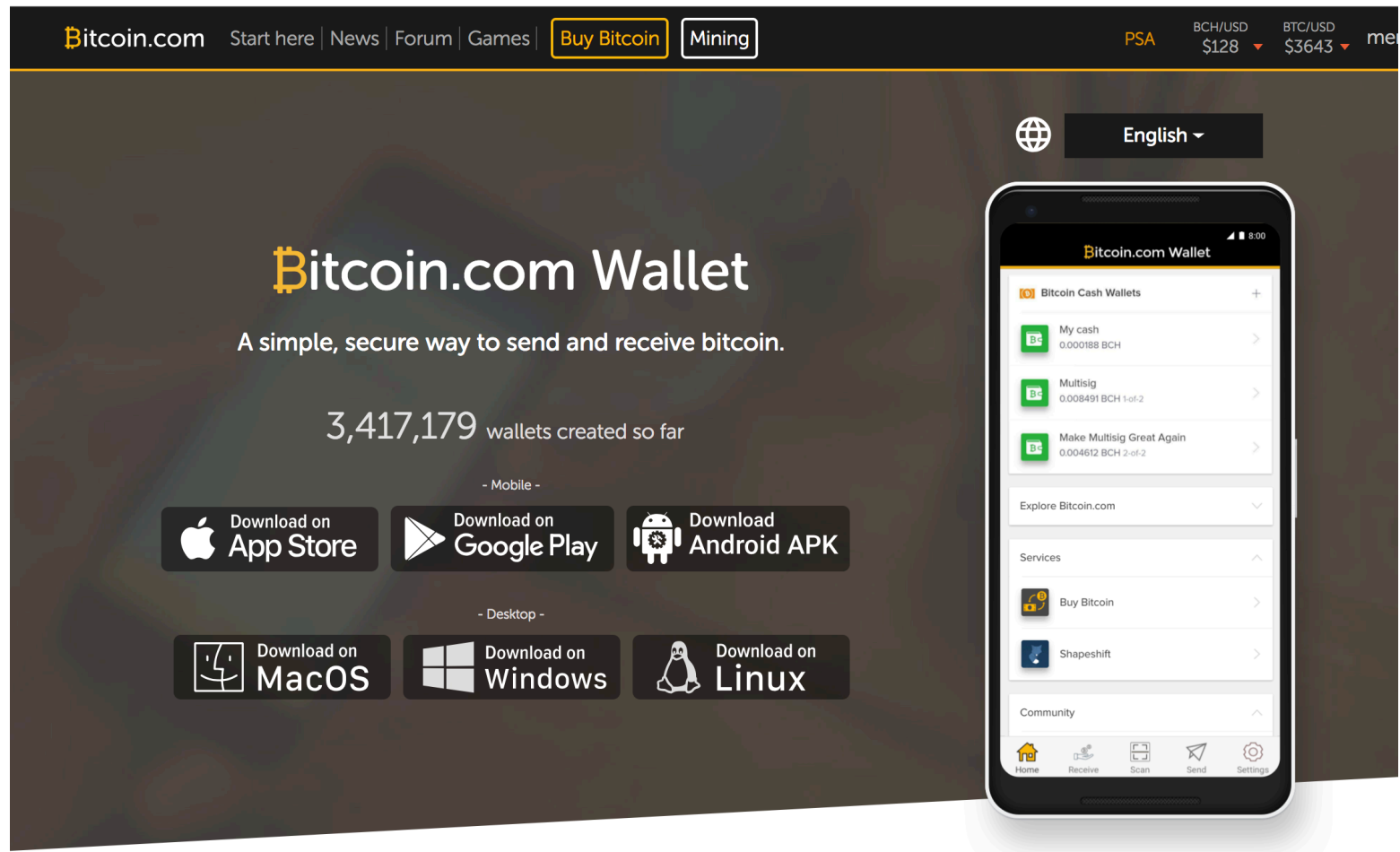
<https://etherscan.io/accounts>

- Your Ethereum address is a public key and your private key is stored either in your browser / mobile / hardware wallet.
- Consider public key like an bank account number, for someone to send you money (Ether), they just need to know your public (account) address. However, only you can access the funds in your account because you are the only one who knows your private key, say similar to your bank account password.

Create an Account on Ethereum

- <https://www.ethereum.org/>

Create an account on Bitcoin



https://wallet.bitcoin.com/?utm_source=get-started&utm_medium=card&utm_content=wallet

Bitcoin Account

Account Number

1Eeq4FM2TTjGqfPx87ZhsGomYpCoh48yy2



$$a = f(p)$$

Private Key

Kyt8y5SrYWPvHEp3dJf65X9LgT
NQavK3D34ru8zqJmFXbyFAzFbi

Transaction Message

From: Bob (1a54..)
To: Eve (14er...)
Amount: 100.0

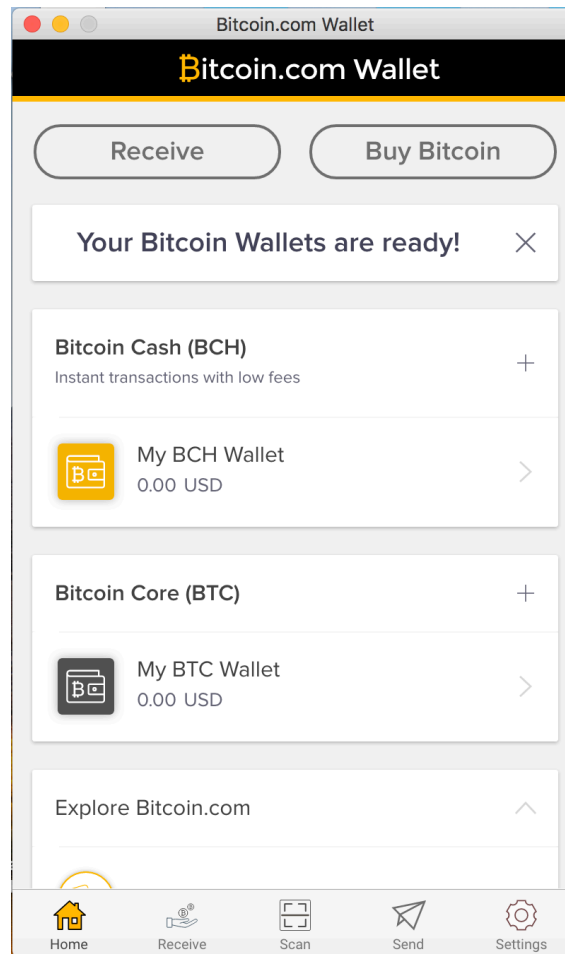
Signature
Checker $f(t,s,a)$

Signature
Creator $f(p,t)$

Signature

3045022100dc50feec13bc11e
4b77a19e34ac903a5413cc1c6
...





Send me some BTC



This how the Bitcoin public address looks (it always starts with **1**)
[Bitcoin private keys always start with **5**]

More reading: ([Ch 1.3](#) digital signatures)

More reading: Need for Public and Private Key
on the Blockchain [link](#)