DeFi

AND THE

Future

of Finance

Course II:

DeFi Primitives

4. Joining the World of DeFi

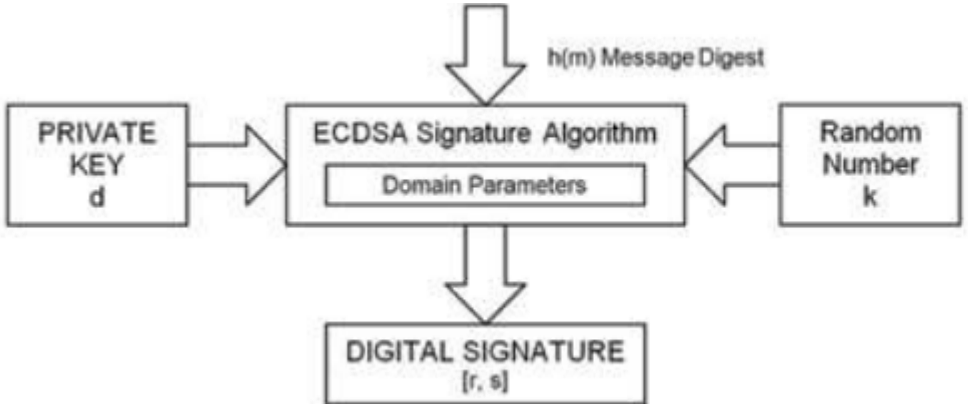
(ii) Blockchain Tech Big Picture

c) Signatures and Transaction Mechanics

Tech Big Picture

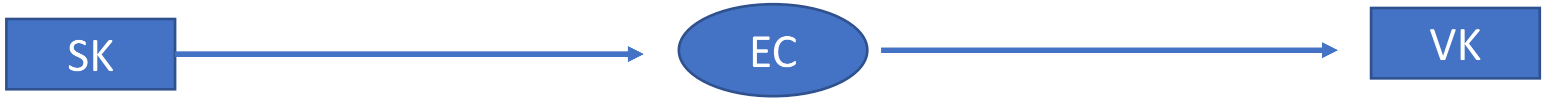
Key ingredients

- **Digital Signatures**: When doing a transaction, you "sign over" your cryptocurrency to someone else using a Digital Signature Algorithm (DSA). The signature proves that you are the owner of the private key. Anyone observing the signature and the public key can verify that you have the private key (without revealing the private key).



Tech Big Picture: ECDSA

- Private key is a number called “signing key” (SK). It is secret.
- Public key is the “verification key” and is mathematically linked to the private key



Private key:
(number)

Elliptic curve operations:
Need base point, modulus, order

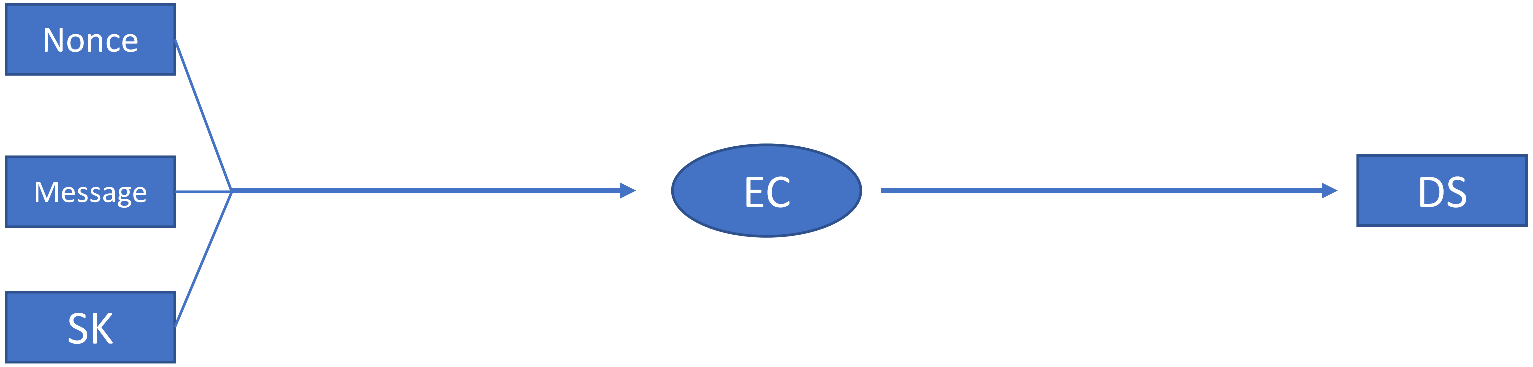
Public key:
coordinate (x, y)

Note: Easy to generate a public key with a private key. Not easy to go the other way.

Tech Big Picture: ECDSA

- Digital signature

Nonce:
(random number)



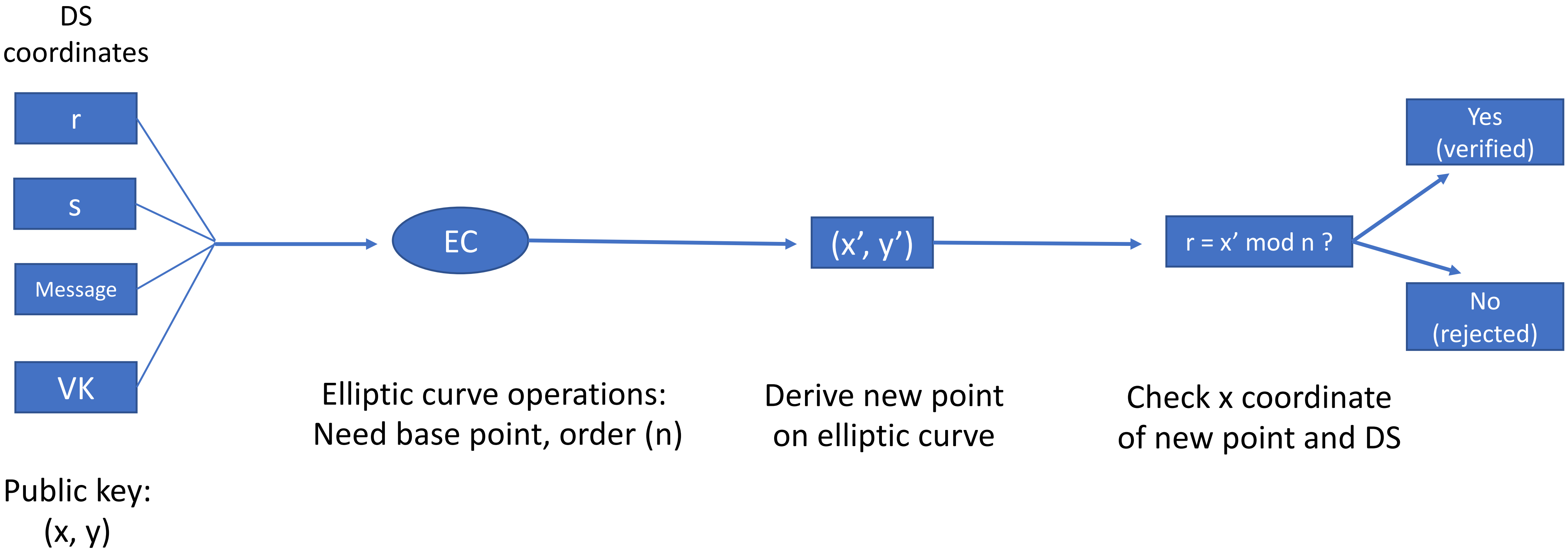
Private key:
(number)

Elliptic curve operations:
Need base point, modulus, order (n)

Digital signature:
coordinate (r, s)

Tech Big Picture: ECDSA

- Verification



Note r not used until verification step

Tech Big Picture: Elliptic Curve Cryptography

Four choices:

- Form of elliptic curve: $y^2 = x^3 + 7$
- Prime modulo: $2^{256} – 2^{32} – 2^9 – 2^8 – 2^7 – 2^6 – 2^4 - 1$ = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F
- Base point: 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8
- Order: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

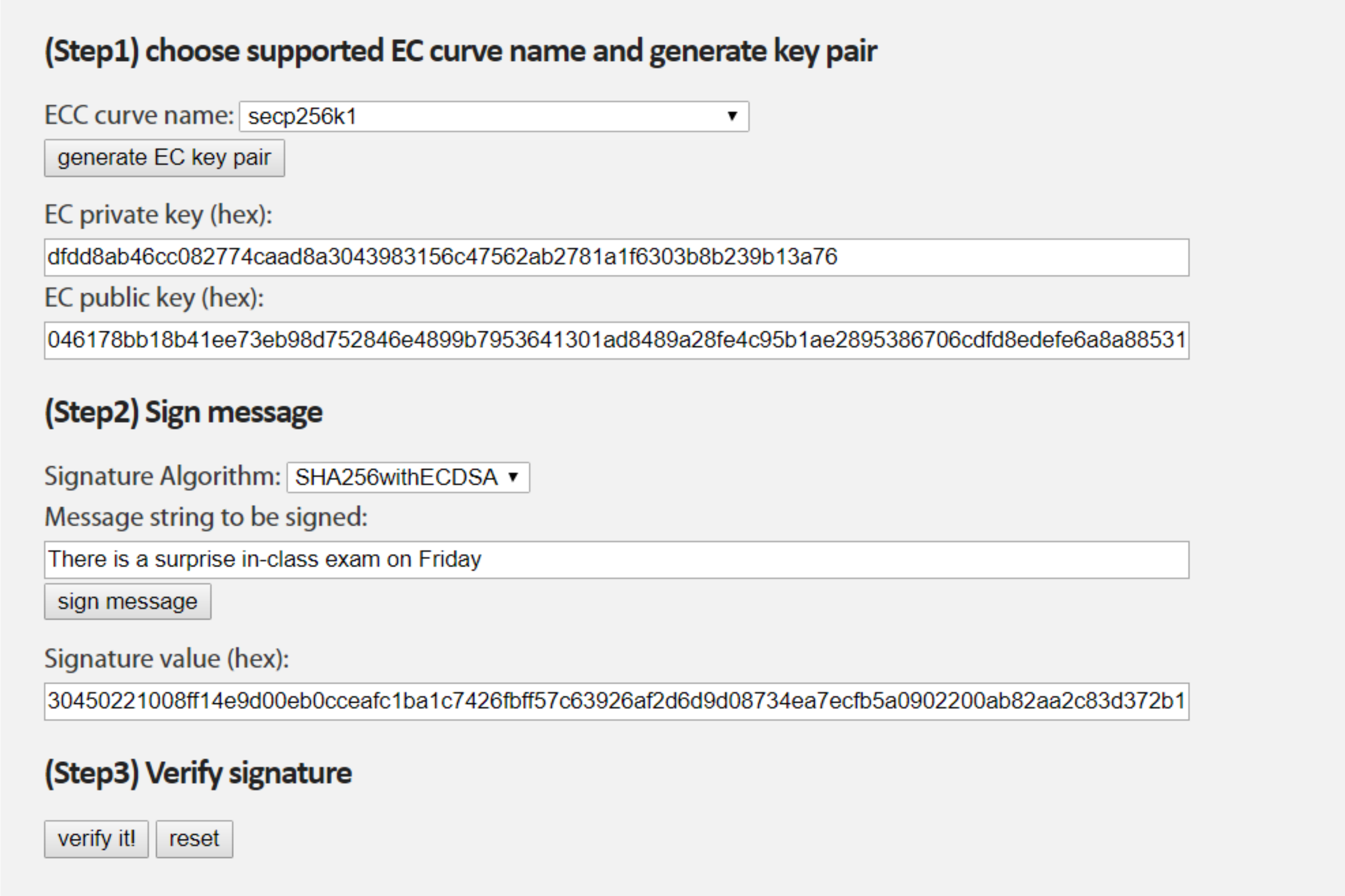
http://www.coindesk.com/math-behind-bitcoin/#

Tech Big Picture: How DSAs Work

Notice

- Proves that the person with the private key (that generated the public key) signed the message.
- Interestingly, digital signature is different from a usual signature in that it depends on the message, i.e., the signature is different for each different message.
- In practice, we do not sign the message, we sign a cryptographic hash of the message. This means that the size of the input is the same no matter how long the message is.

Tech Big Picture: ECDSA in Action



(Step1) choose supported EC curve name and generate key pair

ECC curve name: secp256k1 ▼

EC private key (hex):

dfdd8ab46cc082774caad8a3043983156c47562ab2781a1f6303b8b239b13a76

EC public key (hex):

046178bb18b41ee73eb98d752846e4899b7953641301ad8489a28fe4c95b1ae2895386706cdfd8edefe6a8a88531

(Step2) Sign message

Signature Algorithm: SHA256withECDSA ▼

Message string to be signed:

There is a surprise in-class exam on Friday

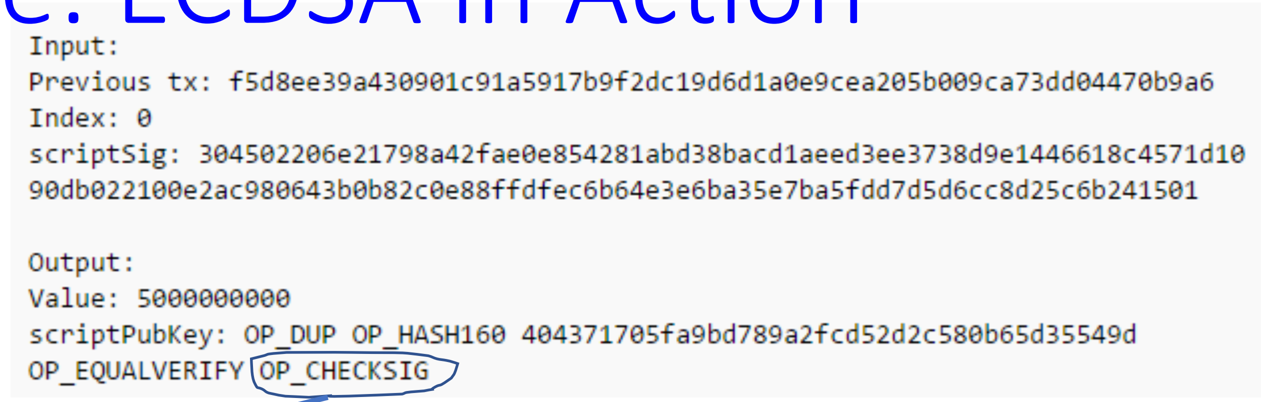
Signature value (hex):

30450221008ff14e9d00eb0cceafc1ba1c7426fbff57c63926af2d6d9d08734ea7ecfb5a0902200ab82aa2c83d372b1

(Step3) Verify signature

https://kjur.github.io/jsrsasign/sample/sample-ecdsa.html

Tech Big Picture: ECDSA in Action



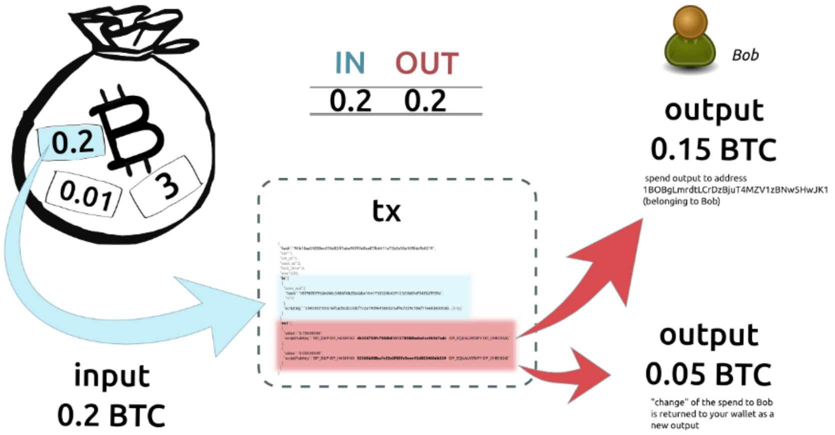
```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

OP_CHECKSIG uses Public Key + Digital Signature + Hash of Transaction

Verifies whether this transaction has been signed by the owner of the Private Key

https://www.youtube.com/watch?v=ir4dDCJhdB4 (advanced by Matt Thomas)

Tech Big Picture


0.2
0.01
3
IN
OUT
0.2
0.2
Bob
output
0.15 BTC
spend output to address 1BOBgLmrdtLCrDzBjuT4MZV1zBNw5HwJK1 (belonging to Bob)
tx
input
0.2 BTC
output
0.05 BTC
"change" of the spend to Bob is returned to your wallet as a new output

Key ingredients

- **Transaction mechanics**: For many cryptocurrencies like bitcoin, we deal with unspent transaction outputs (UTXOs). If I have an UTXO of say 10 units and I want to send 7 to Jenna, Jenna generates a private key (and a public key). I generate a (potentially) new private key (and public key). In a single transaction, I sign over 7 to Jenna and 3 to myself (think of this as “change”). I have a new UTXO of 3 units. The old one resides in a blockchain but has no value. Ethereum uses a different system of account balances.
    - Cryptocurrency doesn’t move anywhere. Everything remains on the associated blockchain.