# Groups, elliptic curves and Bitcoin

Felipe Voloch

Talk at ICTP

October 2016

UC
UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

# Abstract

I’ll talk a bit about bitcoin (a form of “digital money”), then I’ll explain what elliptic curves are and how they give us groups and show how these groups are used in the security of bitcoin.

# Cryptography

Public key cryptography (and elliptic curves) are pervasive on the internet. Online shopping, secure connections, software updates, all use similar tech. Bitcoin is another example of how this tech is used.

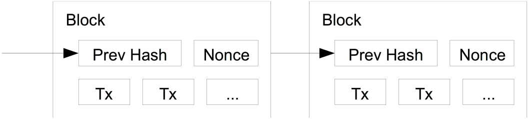
# Bitcoin

Bitcoin is a digital form of currency that tries to exist independently on the Internet. The basic concepts of Bitcoin are:

- Addresses. An address holds a balance denominated in bitcoins (or a fraction thereof).
- Transactions. A transaction is a set of instructions that transfer bitcoins from some addresses to other addresses.
- Blockchain. A ledger listing all valid transactions that have ever occurred, which is organized in blocks placed sequentially in chronological order.

# Blockchain

Bitcoin is also the protocol run as a computer program simultaneously on many computers (“distributed”) online to maintain the ledger (called the “blockchain”) of bitcoin transactions. The computers that participate in maintaining the blockchain get a reward in bitcoin through a lottery of sorts. This process is called mining.



# Transactions

A transaction is like a document in which a user transfer some of her bitcoins to other users. It is digitally signed.

No. ______ Springfield March 21 1860

Springfield Marine & Fire Insurance Company,

Pay to Smith Wickersham Co. or Bearer

One hundred & fifty three 46/100 Dollars,

IN CURRENT BANK NOTES.

$153 46/100

A Lincoln

Richards & Smith, printers.

PSA/DNA
CUT
ABRAHAM LINCOLN
PSA/DNA CERTIFIED
AUTHENTIC
AUTO
83514413

# Addresses

Users have a private key, which they use to sign transactions, a public key, which others can use to verify the signature and an address, which holds a balance.

Private key → Public key → Address

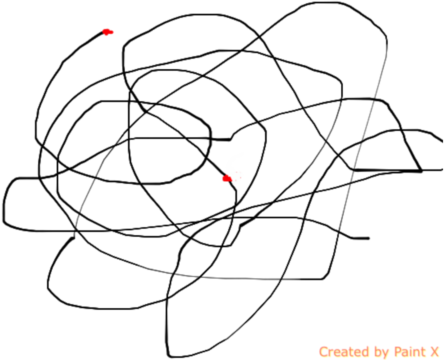
Arrows **cannot** be reversed.

# Address

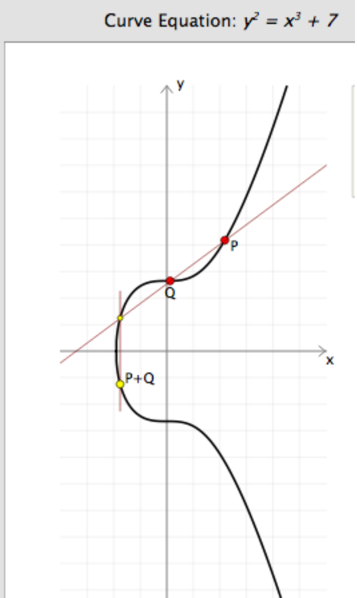
1B9X5Q2v7V4xRcbLdJuGMj9Hw64bhqpy7V

# Curve

Metaphor for public key generation. Start at beginning. Go 123.45 miles (secret number) and use coordinates of final point as public key.



# Elliptic curve



Curve Equation: $y^2 = x^3 + 7$

# Equations for the group law

$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

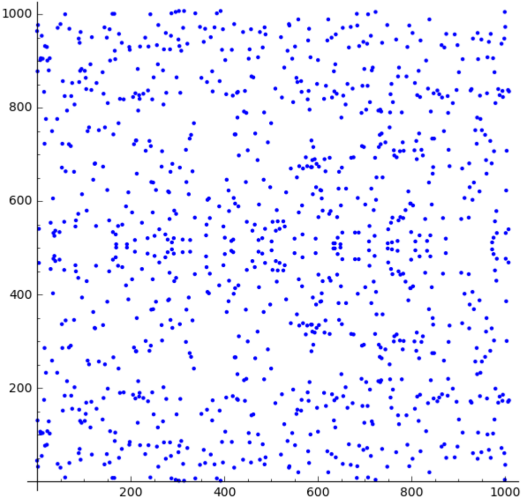
$x_3 = -x_1 - x_2 + \lambda^2, y_3 = -y_1 + \lambda(x_1 - x_3)$

$\lambda = (y_2 - y_1)/(x_2 - x_1)$

Because expressions are algebraic, we can work in other contexts. For our application we work with integers modulo $p$, a large prime. That means we only keep the remainder upon division by $p$ in all calculations.

# Elliptic curve mod 1009

$$y^2 = x^3 + 7 \pmod{1009}$$



# Groups

A group is a set with an operation $+$ where you can do a fragment of algebra. Given $P, Q$, we can compute $P+Q$. We just need associativity: $(P+Q)+R = P+(Q+R)$.

$$2P = P + P, 3P = 2P + P, \dots$$

To compute $nP$ when $n$ is a large number, first compute $2P, 4P = 2(2P), 8P = 2(4P), \dots$ then assemble $nP$ using the binary expansion of $n$. Given the end result $nP$, it should be computationally hard to extract $n$ from it.

# Parameters

$$E : y^2 = x^3 + 7 \pmod{p}$$

$$p = 2^{256} - 2^{32} - 977 =$$

115792089237316195423570985008687907853269984665640564039457584007908834671663

$$\#E \pmod{p} = q =$$

115792089237316195423570985008687907852837564279074904382605163141518161494337

$$G = (55066263022277343669578718895168534326250603453777594175500187360389116729240,$$
$$32670510020758816978083085130507043184471273380659243275938904335757337482424)$$

# ECDSA

Signing a message with elliptic curves.

Let $m$ be the message represented as a number.

Signer secret key $k$, public key $Q = kG$, point on $E$.

Signer also chooses a random number $e$ (the "ephemeral key") and computes $H = eG = (x_1, y_1)$.

Signature $r, s$ where $r = x_1 \pmod{q}, s = e^{-1}(m + rk) \pmod{q}$.

Public info: $m, Q, r, s$.

# Signature verification

Verifier computes $s^{-1}m, s^{-1}r \pmod q$ and $s^{-1}mG + s^{-1}rQ$ on $E$ and if it has $x$-coordinate $r$, the signature validates.

Note:

$$s^{-1}mG + s^{-1}rQ = s^{-1}mG + s^{-1}rkG = s^{-1}(m + rk)G = eG = H$$

# THANK YOU