Blockchain and Bitcoin and Crypto, Oh, My:

The Mathematics of Cryptocurrency

Richard W. Beveridge

Clatsop Community College

What this talk is about

- The mathematics that controls most cryptocurrencies and blockchain applications.
- The history of digital cryptography.

What this talk is *not* about

- How to buy and sell bitcoin or other cryptocurrencies.
- The process by which bitcoin "miners" are chosen and how much they receive.

Digital Cryptography

- The two applications of digital cryptography that we will examine are based on simple mathematical ideas.

#1 $(x^a)^b = (x^b)^a = x^{ab}$

#2 $(a + b)G = a * G + b * G$

Digital Cryptography

- Most cryptocurrenices are run from a blockchain which is an encrypted ledger (or database).
- The security of the ledger depends on digital cryptography.

Digital Cryptography

- After World War II the digital computer became a central part of our civilization.
- During the 1960s people realized that codes had to be updated for the digital era because computers made code-breaking faster and easier.

Digital Cryptography

- In the late 1960s an IBM researcher named Horst Feistel developed one of the first digital cryptographic system for Lloyd's Bank Cashpoint ATM system.

- Horst Feistel was born in Germany, but emigrated to the US in 1934 and received US citizenship 1944.

Digital Cryptography

- Feistel's sytem involved a series of "permutation" and "substitution" processes (known as hashing) applied to bit-strings of 0's and 1's.

- This was based on the post-war work of Claude Shannon and the NSA.

Digital Cryptography
Diffie & Hellman

- During the summer of 1974 Whitfield Diffie met with researchers at IBM Watson Research Center in N.Y. to discuss digital cryptography

Digital Cryptography
Diffie & Hellman

- Diffie had been working as a computer programmer for the defense contractor Mitre Coporation in Boston before leaving to pursue his independent research into cryptography.

Digital Cryptography
Diffie & Hellman

- The IBM researchers he met with suggested that he contact Martin Hellman – a former colleague of theirs who was a professor of Electrical Engineering at Stanford.

Digital Cryptography
Diffie & Hellman

- Diffie and Hellman developed what is known as the Diffie-Hellman Key Exchange based on modular arithmetic.

- The particular problem the Diffie-Hellman Key Exchange is based on is called the Discrete Logarithm Problem

Digital Cryptography
Diffie & Hellman

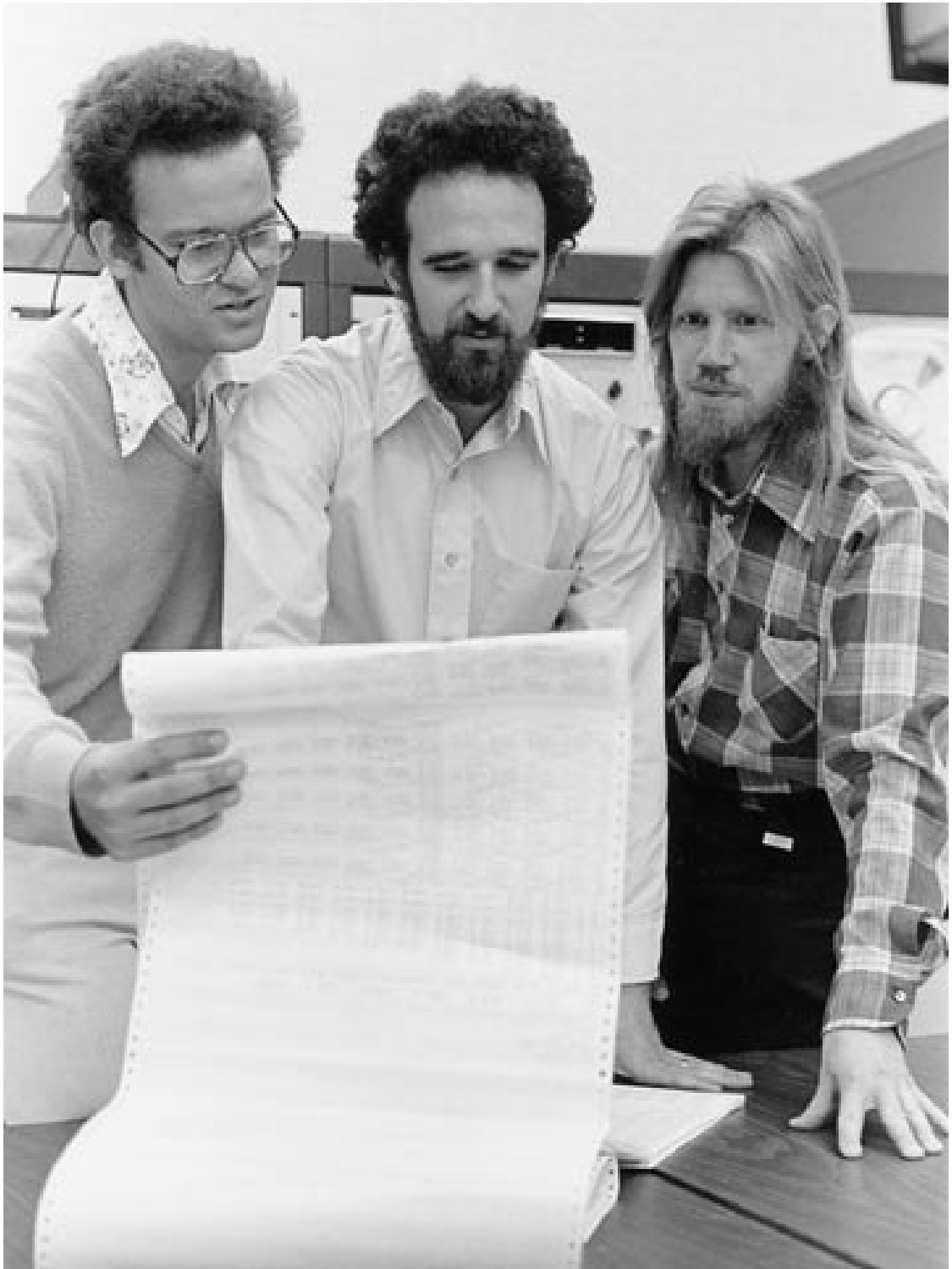
- One major problem in digital cryptography is two parties sending each other the key to decode a message.
- However, if the key itself is not coded then it can be intercepted and used to decode later messages.

Digital Cryptography
Diffie & Hellman

- In the Diffie-Hellman Key Exchange, even though two people may not be in the same place or communicating on a secure channel, the level of difficulty of extracting the key from the information they send is such that present day computers are unable to do this.

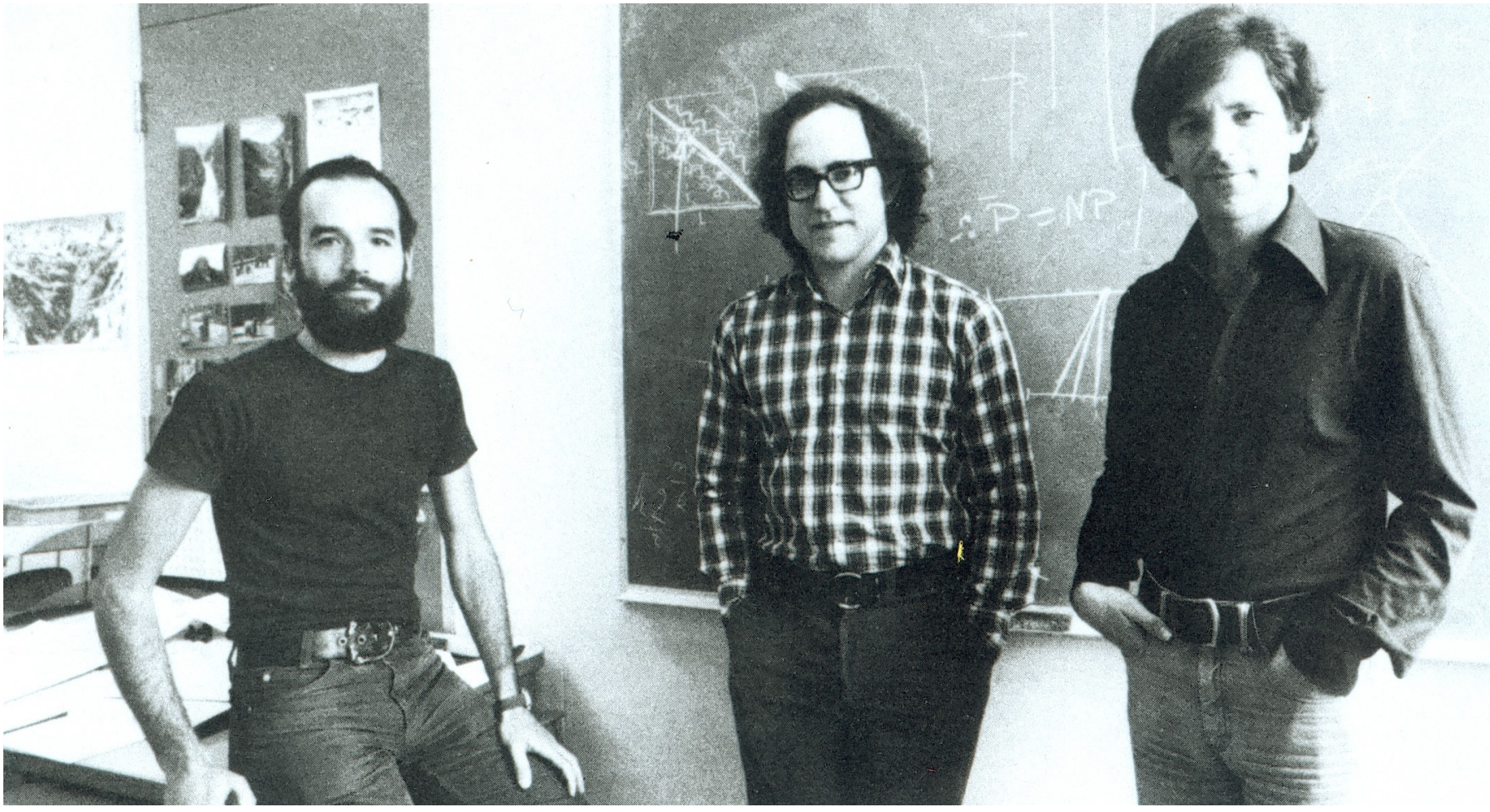
Diffie-Hellman Key Exchange

- A Stanford student named Ralph Merkle had developed a theorectical basis for this type of cryptography in the early 1970's.
- Many contemporary hashing functions are based on Merkle's work from the mid and late 1970s.



Diffie-Hellman Key Exchange

- After Diffie and Hellman published their work in 1976, three MIT professors (Ron Rivest, Adi Shamir, Leonard Adelman) developed the RSA cryptosystem built on the same modular systems as the Diffie-Hellman Key Exchange.


∴P=NP

Diffie-Hellman Key Exchange

- The British GCHQ (equivalent to the American NSA) had also developed a theoretical basis for this type of system in 1970 with specific applications to what became known as RSA cryptography (in 1973) and the Diffie-Hellman Key Exchange (in 1974), but the information was classified until 1997.

Diffie-Hellman Key Exchange

- All of the cryptographic methods we discuss (except for hashing) depend on the mathematics of modular arithmetic.

Modular Arithmetic

- Modular Arithmetic uses only remainders in calculation.
- For example in mod 7 arithmetic, 3*2 = 6 (mod 7), but 3*3=9 $\equiv$ 2 (mod 7) because 9 is 2 more than a multiple of 7.

Modular Arithmetic

ADDITION (MOD 7)

	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

Modular Arithmetic

MULTIPLICATION (MOD 7)

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Modular Arithmetic

EXPONENTS	(MOD 7)					
	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

Modular Arithmetic

- Examples: from Wikipedia – $2^{255} - 19 \approx 5.8 \times 10^{76}$
- Bitcoin uses $2^{256} - 2^{32} - 977 \approx 1.16 \times 10^{77}$

Modular Arithmetic

- The Diffie-Hellman Key Exchange works by publicizing the modular system (we will use MOD 37) and the generator of the system which is chosen.

- A generator returns each value of the system once. In MOD 37, the generators are {2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35 }.

Modular Arithmetic

EXP (MOD 37)																																		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1
3	9	27	7	21	26	4	12	36	34	28	10	30	16	11	33	25	1	3	9	27	7	21	26	4	12	36	34	28	10	30	16	11	33	25	1
4	16	27	34	25	26	30	9	36	33	21	10	3	12	11	7	28	1	4	16	27	34	25	26	30	9	36	33	21	10	3	12	11	7	28	1
5	25	14	33	17	11	18	16	6	30	2	10	13	28	29	34	22	36	32	12	23	4	20	26	19	21	31	7	35	27	24	9	8	3	15	1
6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1
7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1
8	27	31	26	23	36	29	10	6	11	14	1	8	27	31	26	23	36	29	10	6	11	14	1	8	27	31	26	23	36	29	10	6	11	14	1
9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1
10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1
11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1
12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1
13	21	14	34	35	11	32	9	6	4	15	10	19	25	29	7	17	36	24	16	23	3	2	26	5	28	31	33	22	27	18	12	8	30	20	1
14	11	6	10	29	36	23	26	31	27	8	1	14	11	6	10	29	36	23	26	31	27	8	1	14	11	6	10	29	36	23	26	31	27	8	1
15	3	8	9	24	27	35	7	31	21	19	26	20	4	23	12	32	36	22	34	29	28	13	10	2	30	6	16	18	11	17	33	14	25	5	1
16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1
17	30	29	12	19	27	15	33	6	28	32	26	35	3	14	16	13	36	20	7	8	25	18	10	22	4	31	9	5	11	2	34	23	21	24	1
18	28	23	7	15	11	13	12	31	3	17	10	32	21	8	33	2	36	19	9	14	30	22	26	24	25	6	34	20	27	5	16	29	4	35	1
19	28	14	7	22	11	24	12	6	3	20	10	5	21	29	33	35	36	18	9	23	30	15	26	13	25	31	34	17	27	32	16	8	4	2	1
20	30	8	12	18	27	22	33	31	28	5	26	2	3	23	16	24	36	17	7	29	25	19	10	15	4	6	9	32	11	35	34	14	21	13	1
21	34	11	9	4	10	25	7	36	16	3	26	28	33	27	12	30	1	21	34	11	9	4	10	25	7	36	16	3	26	28	33	27	12	30	1
22	3	29	9	13	27	2	7	6	21	18	26	17	4	14	12	5	36	15	34	8	28	24	10	35	30	31	16	19	11	20	33	23	25	32	1
23	11	31	10	8	36	14	26	6	27	29	1	23	11	31	10	8	36	14	26	6	27	29	1	23	11	31	10	8	36	14	26	6	27	29	1
24	21	23	34	2	11	5	9	31	4	22	10	18	25	8	7	20	36	13	16	14	3	35	26	32	28	6	33	15	27	19	12	29	30	17	1

Modular Arithmetic

- If we choose the generator 5, then the modular system (MOD 37) and the generator (5) would be publicized.

- Two individuals wishing to exchange private keys to generate a secret value to encode their message would send each other the following values.

Modular Arithmetic

- If Alice has a private key of 33, she would send Bob the value $5^{33} \bmod 37 \equiv 8 \bmod 37$
- If Bob has a private key of 17, he would send Alice the value $5^{17} \bmod 37 \equiv 22 \bmod 37$

Modular Arithmetic

EXP (MOD 37)																																		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1
3	9	27	7	21	26	4	12	36	34	28	10	30	16	11	33	25	1	3	9	27	7	21	26	4	12	36	34	28	10	30	16	11	33	25	1
4	16	27	34	25	26	30	9	36	33	21	10	3	12	11	7	28	1	4	16	27	34	25	26	30	9	36	33	21	10	3	12	11	7	28	1
5	25	14	33	17	11	18	16	6	30	2	10	13	28	29	34	22	36	32	12	23	4	20	26	19	21	31	7	35	27	24	9	8	3	15	1
6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1	6	36	31	1
7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1	7	12	10	33	9	26	34	16	1
8	27	31	26	23	36	29	10	6	11	14	1	8	27	31	26	23	36	29	10	6	11	14	1	8	27	31	26	23	36	29	10	6	11	14	1
9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1	9	7	26	12	34	10	16	33	1
10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1	10	26	1
11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1	11	10	36	26	27	1
12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1	12	33	26	16	7	10	9	34	1
13	21	14	34	35	11	32	9	6	4	15	10	19	25	29	7	17	36	24	16	23	3	2	26	5	28	31	33	22	27	18	12	8	30	20	1
14	11	6	10	29	36	23	26	31	27	8	1	14	11	6	10	29	36	23	26	31	27	8	1	14	11	6	10	29	36	23	26	31	27	8	1
15	3	8	9	24	27	35	7	31	21	19	26	20	4	23	12	32	36	22	34	29	28	13	10	2	30	6	16	18	11	17	33	14	25	5	1
16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1	16	34	26	9	33	10	12	7	1
17	30	29	12	19	27	15	33	6	28	32	26	35	3	14	16	13	36	20	7	8	25	18	10	22	4	31	9	5	11	2	34	23	21	24	1
18	28	23	7	15	11	13	12	31	3	17	10	32	21	8	33	2	36	19	9	14	30	22	26	24	25	6	34	20	27	5	16	29	4	35	1
19	28	14	7	22	11	24	12	6	3	20	10	5	21	29	33	35	36	18	9	23	30	15	26	13	25	31	34	17	27	32	16	8	4	2	1
20	30	8	12	18	27	22	33	31	28	5	26	2	3	23	16	24	36	17	7	29	25	19	10	15	4	6	9	32	11	35	34	14	21	13	1
21	34	11	9	4	10	25	7	36	16	3	26	28	33	27	12	30	1	21	34	11	9	4	10	25	7	36	16	3	26	28	33	27	12	30	1
22	3	29	9	13	27	2	7	6	21	18	26	17	4	14	12	5	36	15	34	8	28	24	10	35	30	31	16	19	11	20	33	23	25	32	1
23	11	31	10	8	36	14	26	6	27	29	1	23	11	31	10	8	36	14	26	6	27	29	1	23	11	31	10	8	36	14	26	6	27	29	1
24	21	23	34	2	11	5	9	31	4	22	10	18	25	8	7	20	36	13	16	14	3	35	26	32	28	6	33	15	27	19	12	29	30	17	1

Modular Arithmetic

- When Bob receives the value of 8 mod 37 from Alice, he raises this to the power equal to his private key.
  $8^{17} \equiv 23 \bmod 37$

- When Alice receives the value of 22 mod 37 from Bob, she raises this to the power equal to her private key.
  $22^{33} \equiv 23 \bmod 37$

Modular Arithmetic

- This works because:

$$(5^{33})^{17} = (5^{17})^{33}$$

or

$$(x^a)^b = (x^b)^a = x^{ab}$$

Modular Arithmetic

- Now they both have the same code with which to work.
- The actual values that are used in practice involve numbers much larger than 37.

Modular Arithmetic

- Because the numbers used for the public values (in our example 5 and mod 37) are so large, it is functionally impossible to "back-calculate" the power that each person raised the public number to.

Modular Arithmetic

- Examples: from Wikipedia – $2^{255} - 19 \approx 5.8 \times 10^{76}$
- bitcoin uses $2^{256} - 2^{32} - 977 \approx 1.16 \times 10^{77}$

Modular Arithmetic

- This is the "Discrete Logarithm Problem"

Modular Arithmetic

- Even if someone intercepts the 8 mod 37 that Alice sends to Bob, they would not be able to find the power that resulted in the 8 ($5^{?} \equiv 8 \bmod 37$)

- Making a table like the one we have for mod 37 is simply too time-consuming for these very large numbers.

Elliptic Curve Cryptosystems

- The use of Elliptic Cuve Cryptography was proposed independently in 1985 by Neal Koblitz (University of Washington) and Victor Miller (IBM TJ Watson Research Center)

Neal and Ann Koblitz

Victor Miller

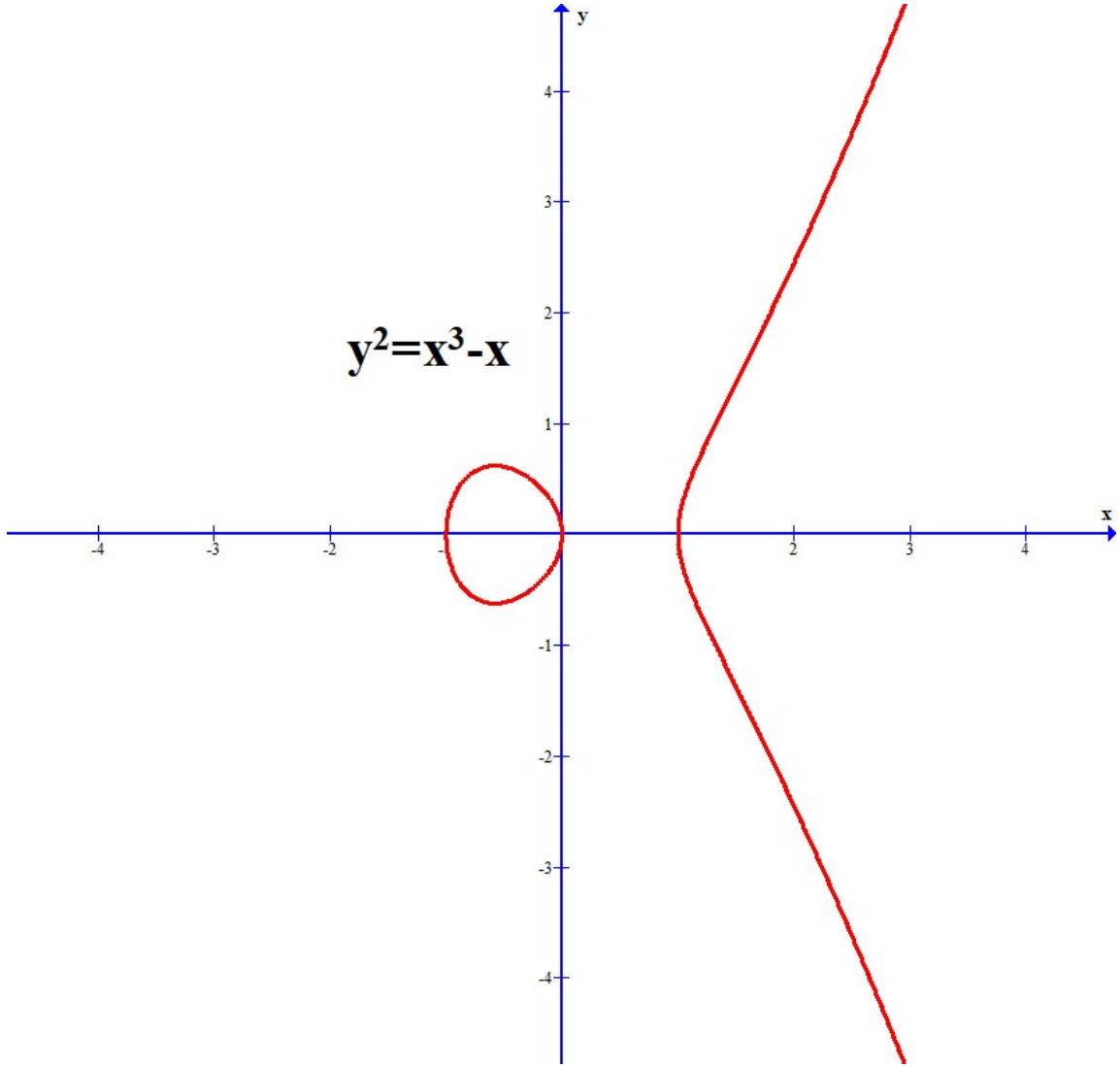
Elliptic Curve Cryptosystems

- ECC uses the graphs and structure of elliptic curves over the same modular systems (finite fields) as the Diffie-Hellman Key Exchange and the RSA cryptosystem.

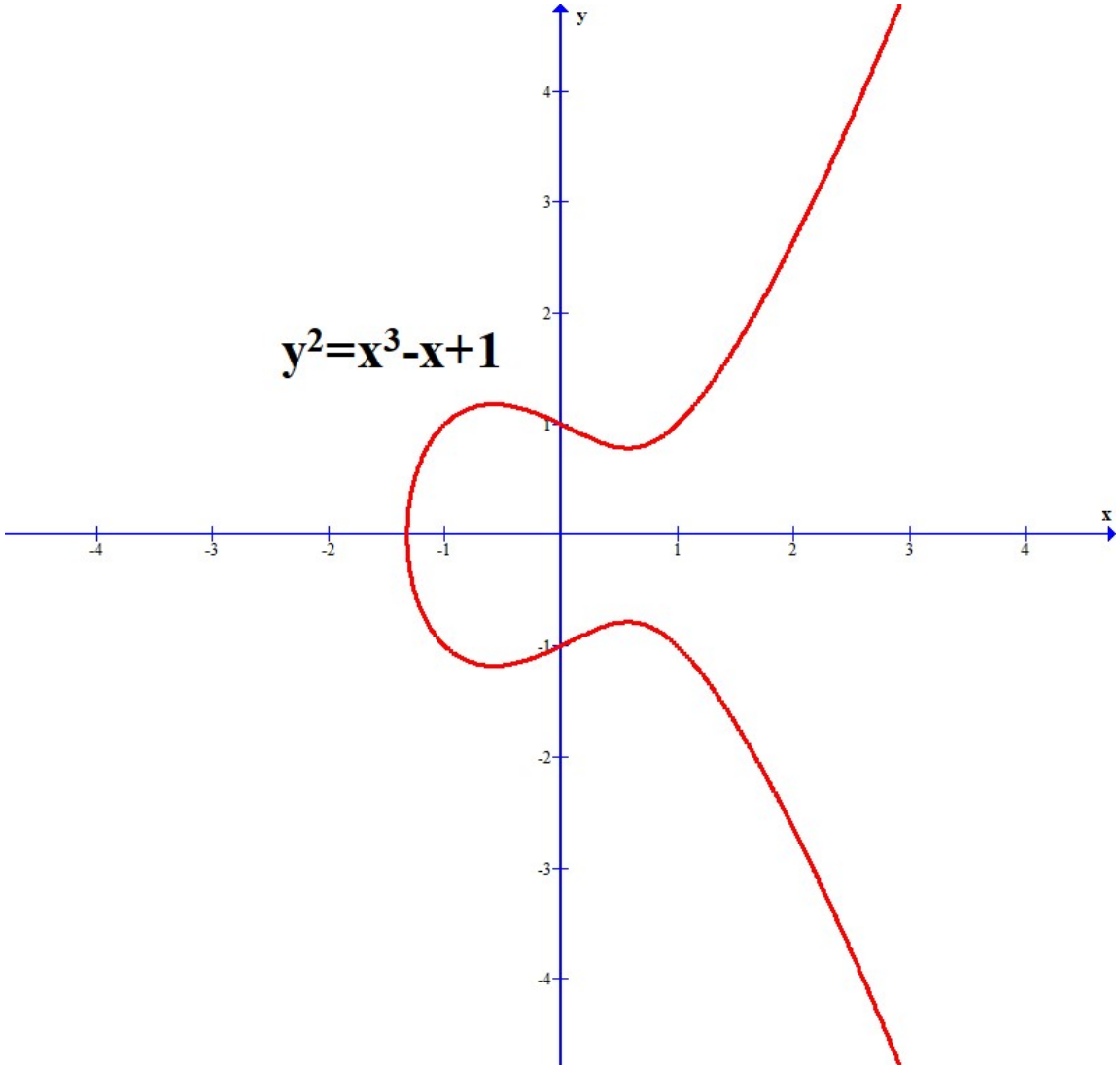
Elliptic Curve Cryptosystems

- Because Elliptic Curve Cryptography has additional levels of complexity, shorter keys can be used without a corresponding loss of security.
- Shorter keys are less memory intensive for computers.

Elliptic Curve Cryptosystems



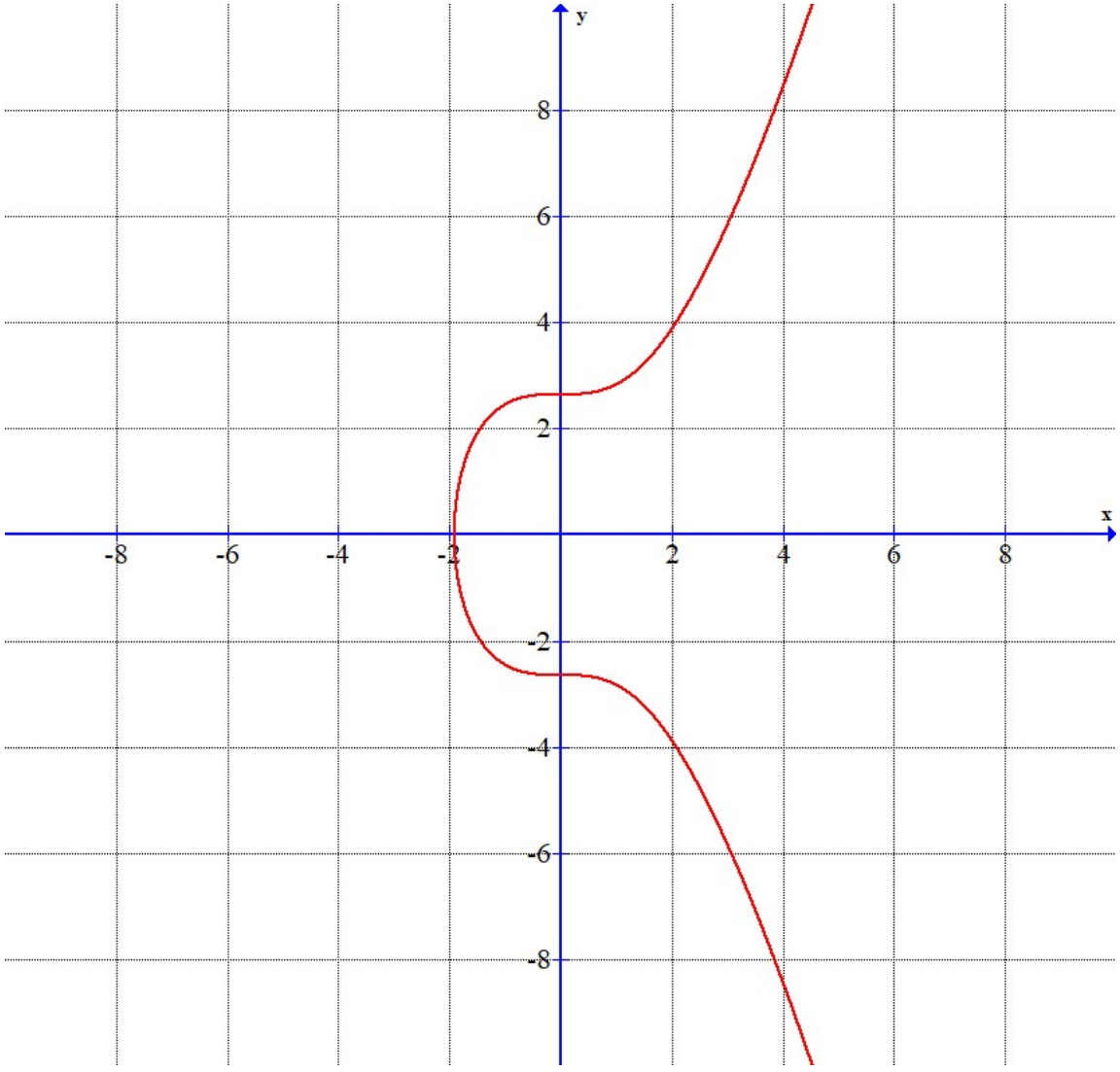
Elliptic Curve Cryptosystems



Elliptic Curve Cryptosystems

- Bitcoin uses the curve $y^2 = x^3 + 7$

Elliptic Curve Cryptosystems



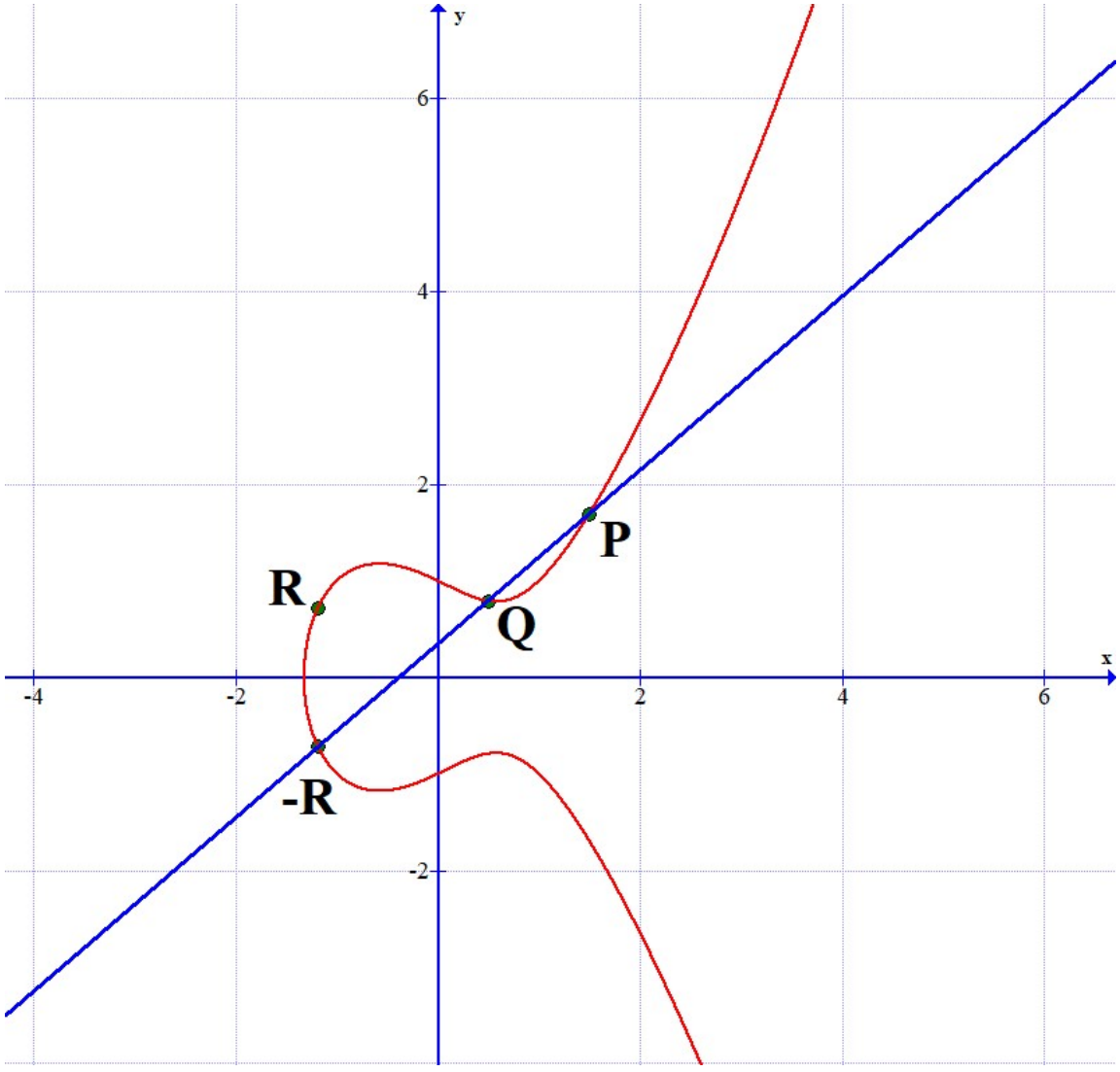
Elliptic Curve Cryptosystems

- The calculation process used in ECC involves addition of points on the curve.
- Using some basic algebraic ideas, a line drawn through any two points on the curve will intersect exactly one additional point on the curve.

Elliptic Curve Cryptosystems

- The y coordinate of this point is negated and the result R is the value of $P + Q$.

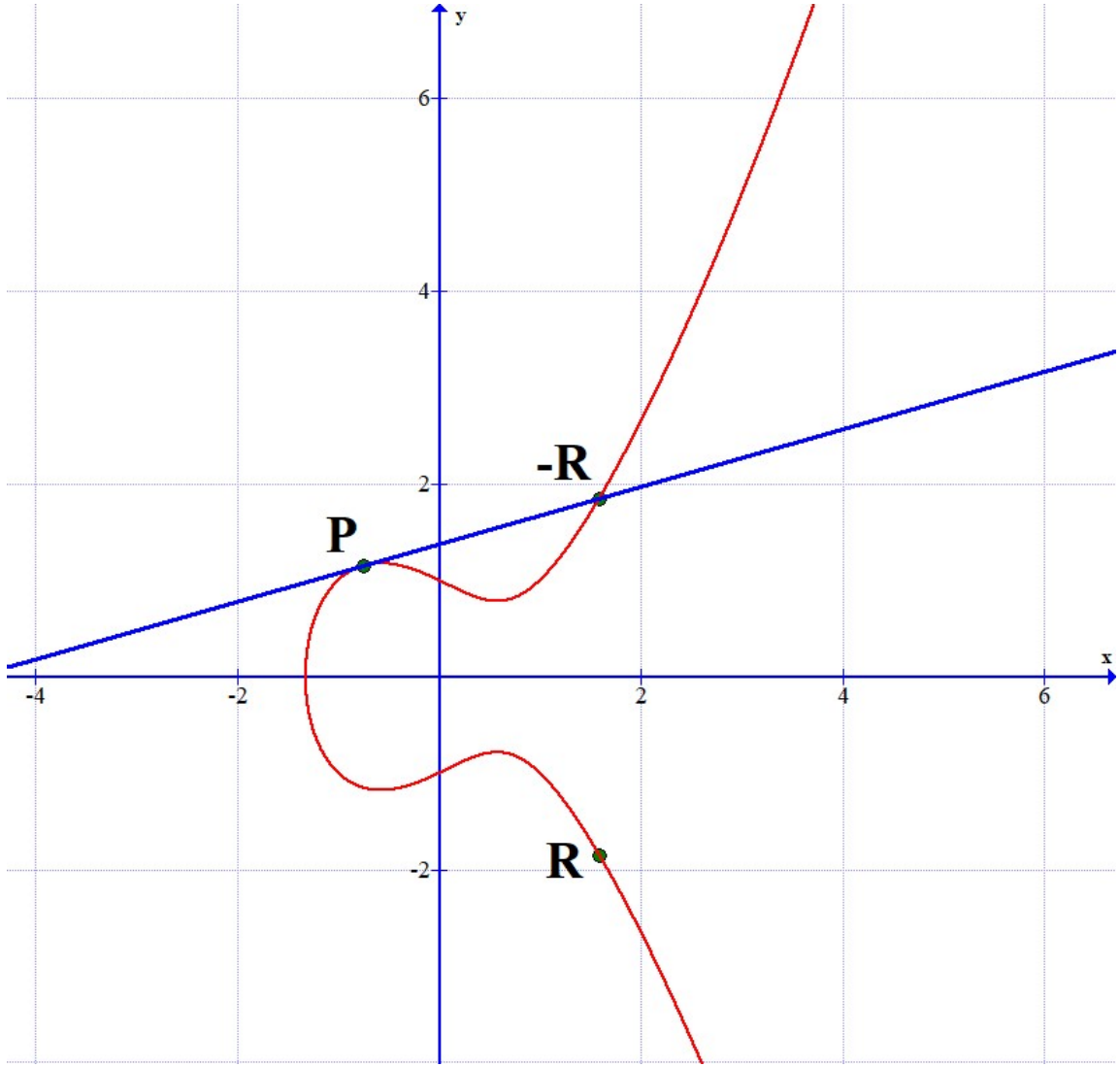
Elliptic Curve Cryptosystems



Elliptic Curve Cryptosystems

- If a point P is added to itself ($P + P$), a line is drawn tangent to the curve at the point P and again this line will intersect the curve in exactly one other point.
- The y coordinate of this point is negated and the result R is the value of $P + P$.

Elliptic Curve Cryptosystems



Elliptic Curve Cryptosystems

- This allows for the creation of a "times table" for a given point.
- As the point is repeatedly added to itself it becomes impossible to know what the point has been multiplied by to get a certain result.

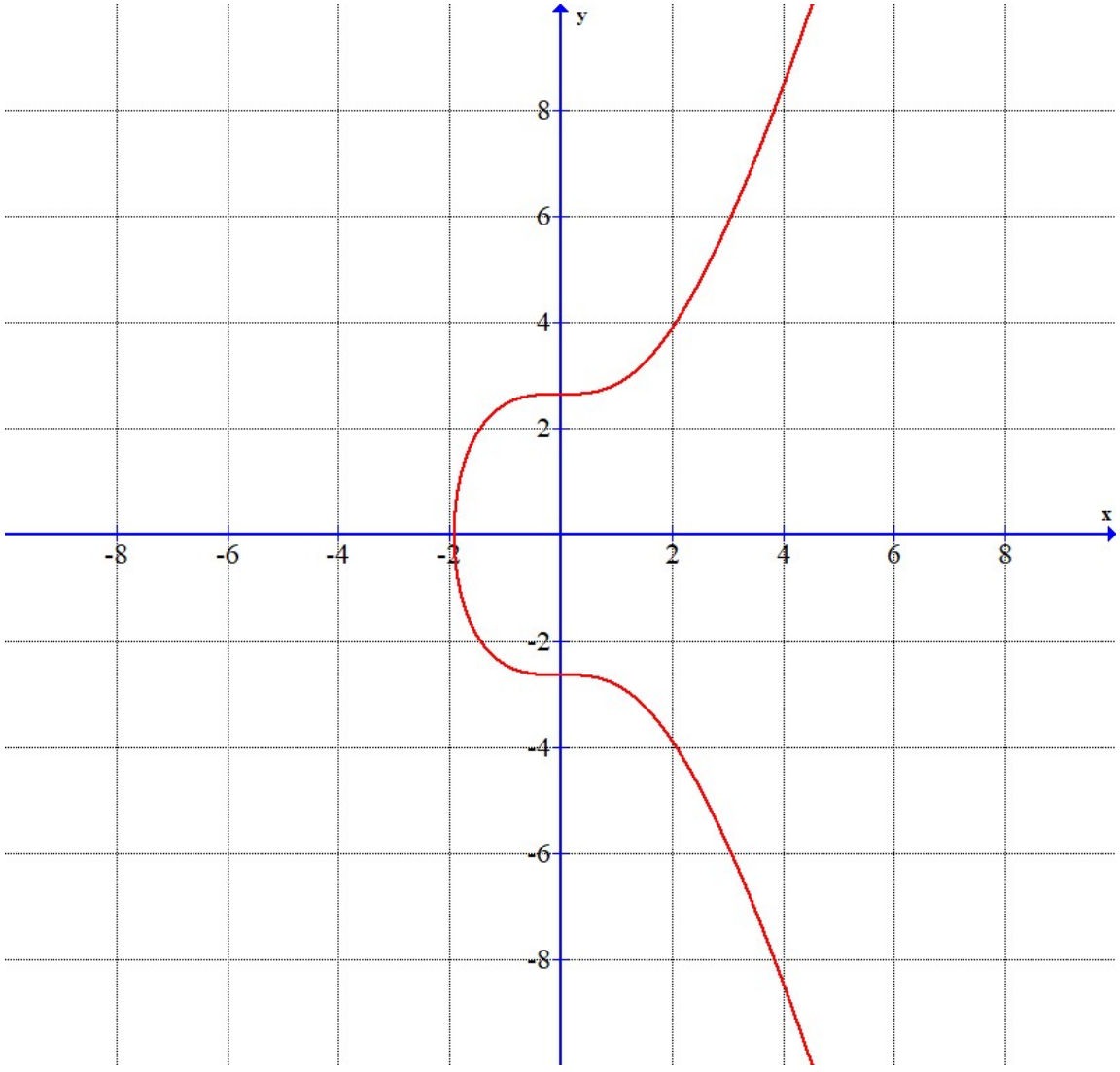
Elliptic Curve Cryptosystems

				x	y			
			1	24	17			
			2	23	36			
			3	18	17			
			4	32	20			
			5	6	36			
			6	8	36			
			7	8	1			
			8	6	1			
			9	32	17			
			10	18	20			
			11	23	1			
			12	24	20			
			13	0	0			

Elliptic Curve Cryptosystems

- Bitcoin uses the curve $y^2 = x^3 + 7$

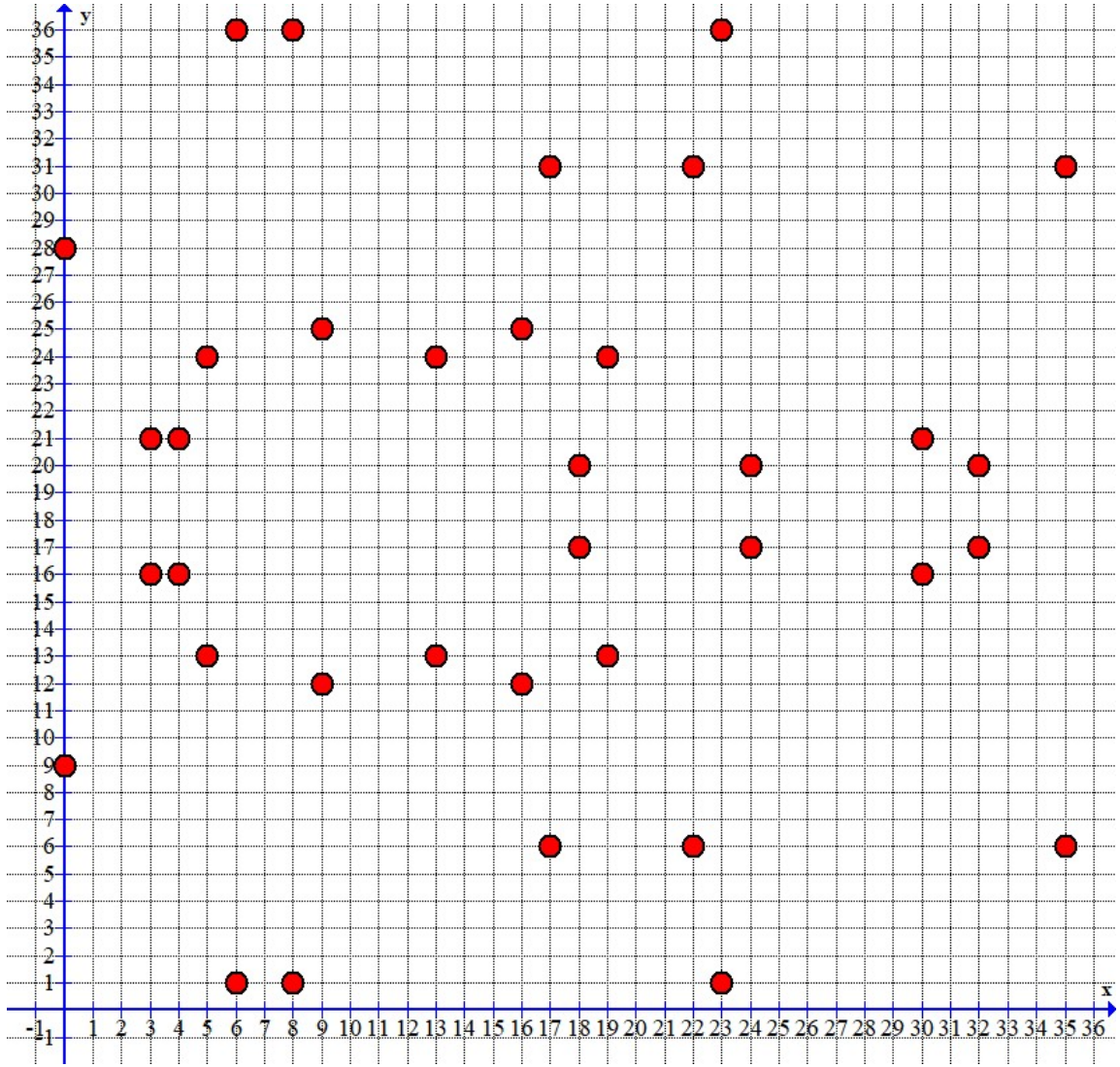
Elliptic Curve Cryptosystems



Elliptic Curve Cryptosystems

- These examples are all showing continuous elliptic curves.
- Elliptic curves over finite fields look different.
- The following slide is the same curve $y^2 = x^3 + 7$ calculated in MOD 37

Elliptic Curve Cryptosystems



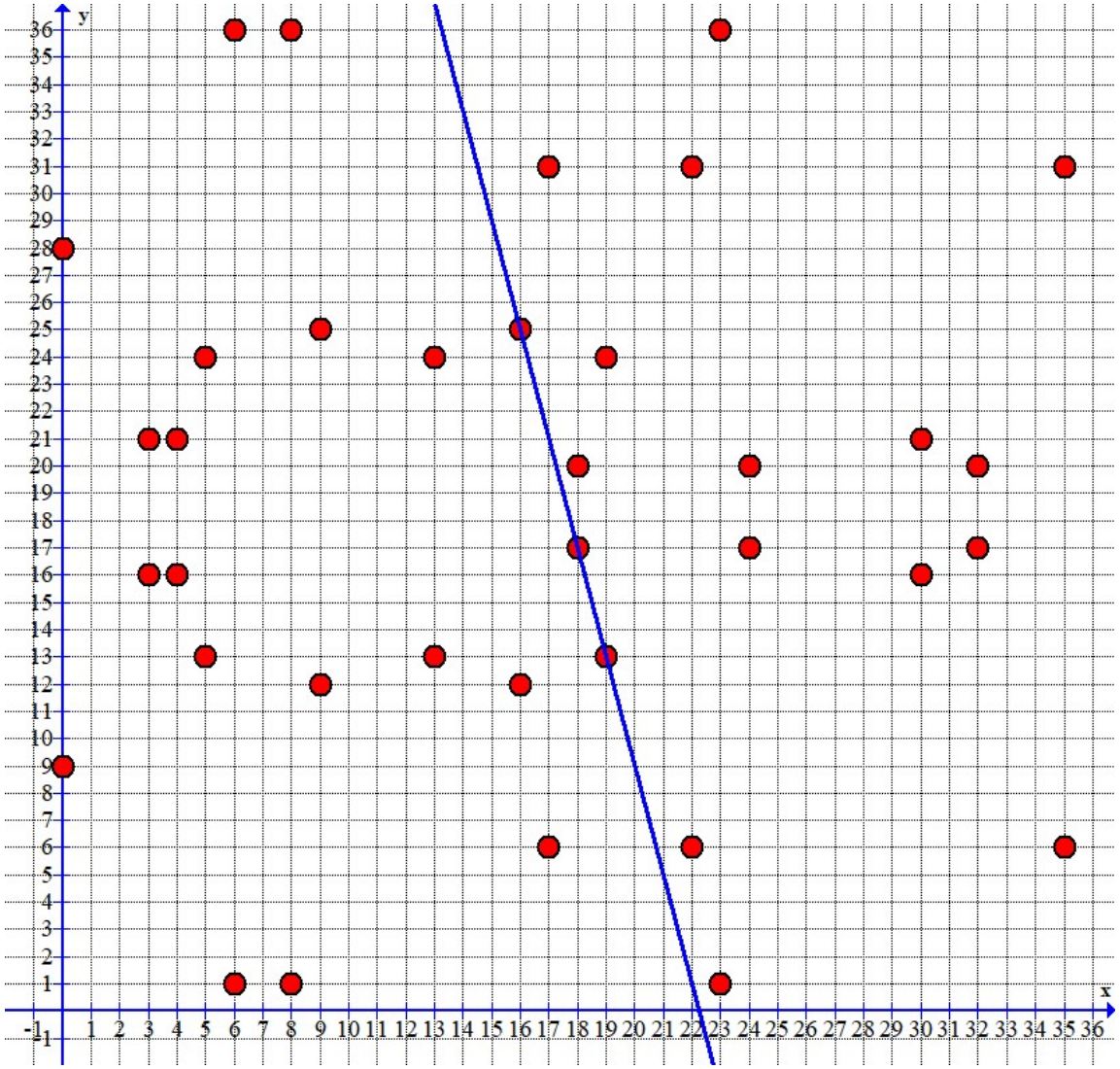
Elliptic Curve Cryptosystems

- The calculation of point addition and point doubling is similar to the same process on a continuous curve.
- A line drawn through two points will intersect exactly one other point on the "curve."

Elliptic Curve Cryptosystems

- A simple example: to add the points $(18, 17)$ and $(19, 13)$ we simply draw a line through them.
- This line intersects $(16, 25)$, so $(18, 17) + (19, 13) = (16, 12)$

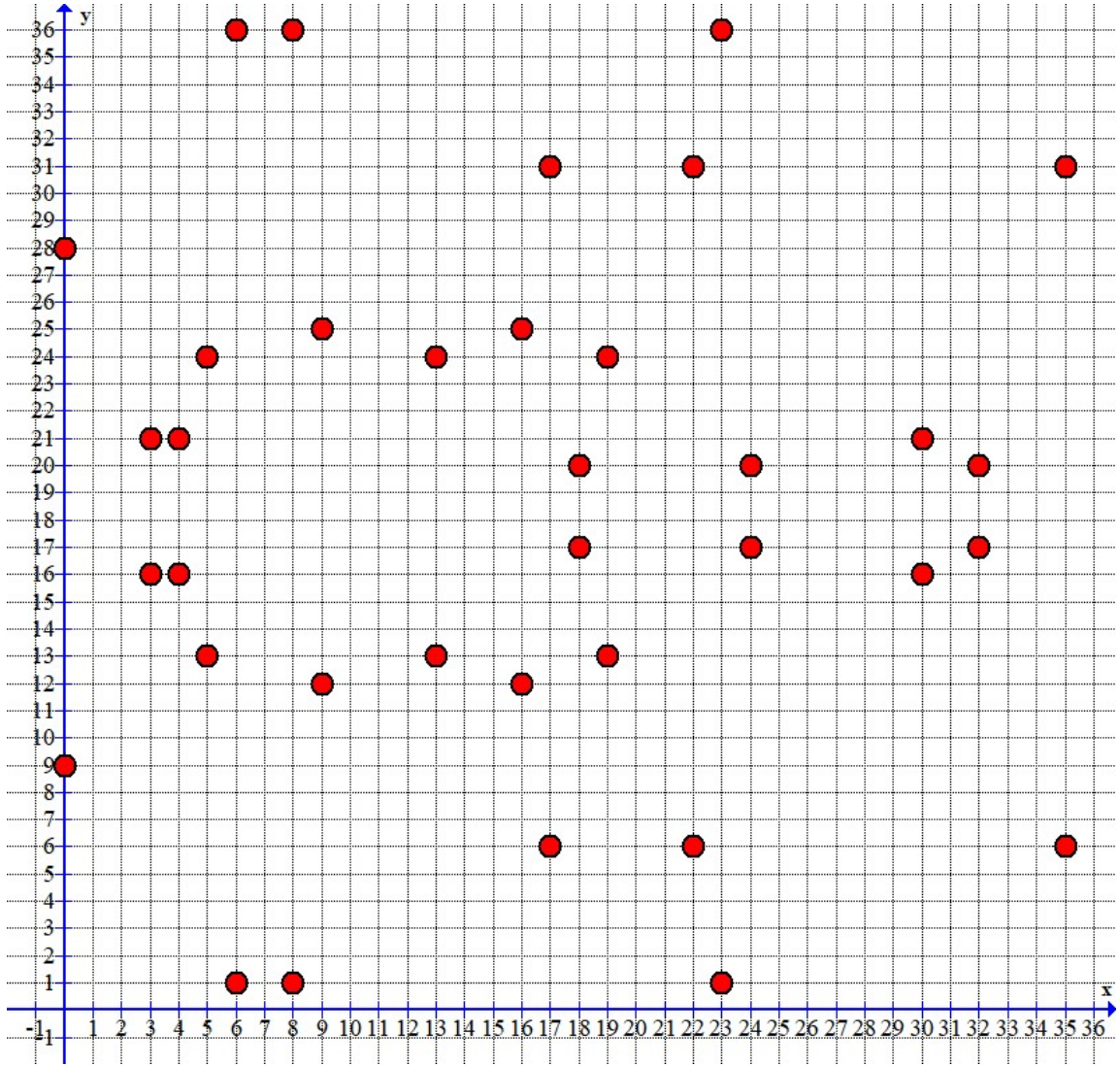
Elliptic Curve Cryptosystems



Elliptic Curve Cryptosystems

- In this system the "negative" will be the number that produces 37 rather than 0, since $37 \equiv 0 \mod 37$.
- The negative of 5 is -5 because $5 + -5 = 0$
- In MOD 37, the negative of 5 is 32 because $5 + 32 = 37 \equiv 0 \mod 37$

Elliptic Curve Cryptosystems



Elliptic Curve Cryptosystems

- To add a point to itself we need calculus to compute the slope, then from there we can calculate the x and y coordinates.
- For $y^2 = x^3 + 7$ $\quad$ $\text{slope}(s) = \dfrac{3x^2}{2y}$

Elliptic Curve Cryptosystems

- The new x coordinate (x_N) will be: $s^2 - 2x$
- The new y coordinate (y_N) will be: $s(x - x_N) - y$

Elliptic Curve Cryptosystems

- So, if we want to double a point like $(24, 17)$, we calculate the slope:

$$\frac{3 * 24^2}{2 * 17} \equiv 16 \bmod 37$$

Elliptic Curve Cryptosystems

- The new x coordinate (x_N) will be: $s^2 - 2x = 16^2 - 2 * 24 = 256 - 48 = 208 \equiv 23 \bmod 37$
- The new y coordinate (y_N) will be: $s(x - x_N) - y = 16(24 - 23) - 17 = 16(1) - 17 = 16 - 17 = -1 \equiv 36 \bmod 37$

Elliptic Curve Cryptosystems

- So

$$2 * (24, 17) = (24, 17) + (24, 17)$$

$$= (23, 36)$$

Elliptic Curve Cryptosystems

				x	y			
			1	24	17			
			2	23	36			
			3	18	17			
			4	32	20			
			5	6	36			
			6	8	36			
			7	8	1			
			8	6	1			
			9	32	17			
			10	18	20			
			11	23	1			
			12	24	20			
			13	0	0			

Elliptic Curve Cryptosystems

- Once these "times tables" are constructed, it becomes computationally impossible to retrace the steps and find what the original point was multiplied by to get the result.

Blockchain

- A Blockchain system uses several of these these concepts together.
- Modular arithmetic, hash functions and elliptic curve systems are all used together to create an unbreakable code.

Blockchain

- A blockchain is a decentralized ledger (or database) system in which information can only be recorded and distributed, but not edited, through the use of private cryptographic keys.

Blockchain

- This can be useful to businesses (and other institutions) that require record keeping by many different individuals or entities.
- Conventional computer businesses are selling blockchain software - IBM, Microsoft, The Linux Foundation and Oracle are several notable examples.

Blockchain

- Companies that are using this technology include Cigna, Anthem, Aetna, Motorola, Renault, UBS, JP Morgan and Visa

Blockchain

- There are many aspects to the blockchain process and most require digital crytpography.
- We will focus on one - the Elliptic Curve Digital Signature Algorithm (ECDSA) used by both Bitcoin and Ethereum.

ECDSA

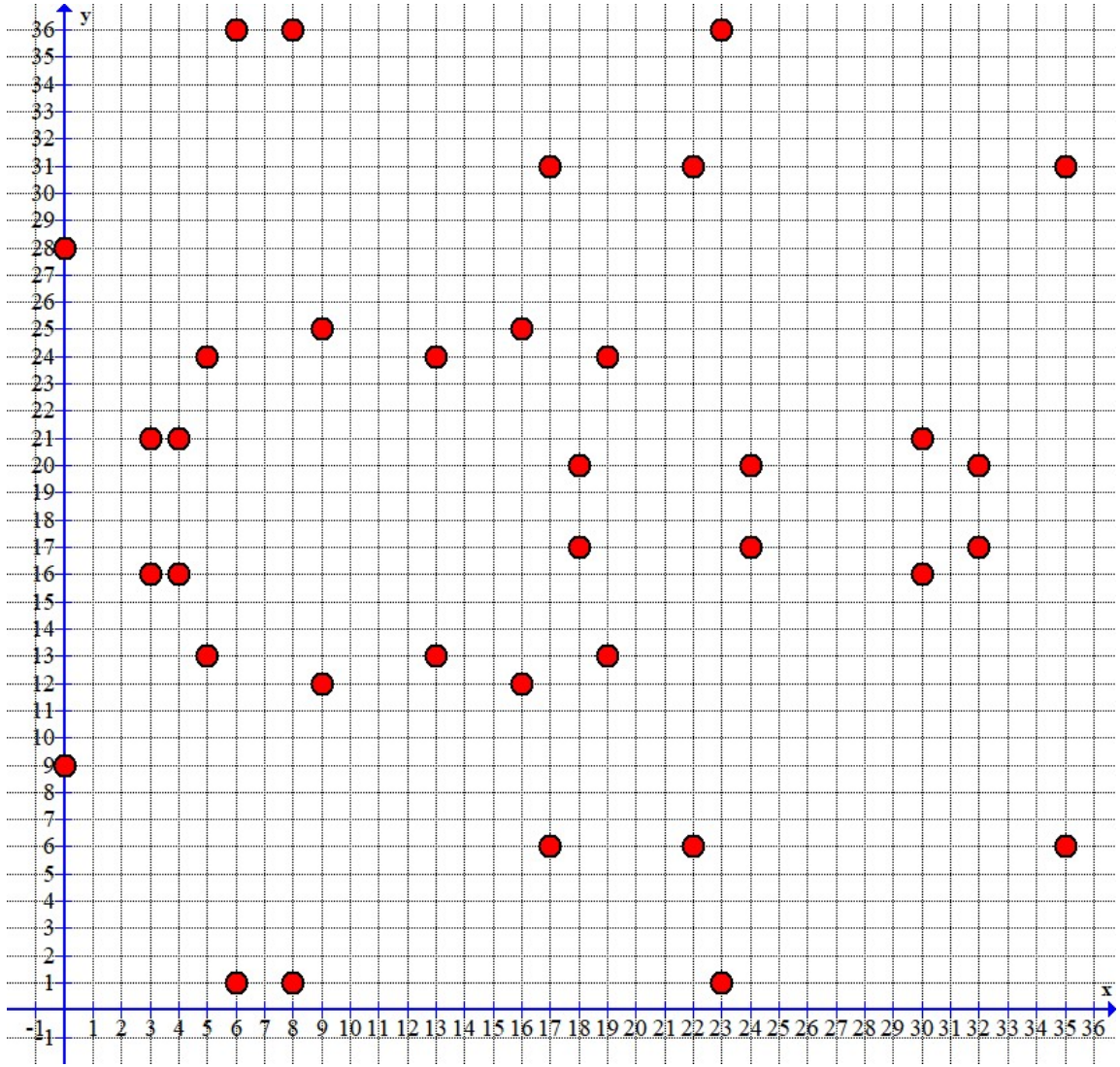
- ECDSA requires an elliptic curve, a modular system and a generating point.

- Bitcoin and Ethereum use $y^2 = x^3 + 7$

ECDSA

- We will use a mod 37 system and the generating point $G = (24, 17)$
- Adding the point $G = (24, 17)$ to itself generates a subset of 13 points from the system of points we saw earlier on the graph.

ECDSA


y
x
36 35 34 33 32 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1
-1
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36

ECDSA

				x	y			
			1	24	17			
			2	23	36			
			3	18	17			
			4	32	20			
			5	6	36			
			6	8	36			
			7	8	1			
			8	6	1			
			9	32	17			
			10	18	20			
			11	23	1			
			12	24	20			
			13	0	0			

ECDSA

PLEASE NOTE

The Elliptic Curve Digital Signature Algorithm is purposefully complex(!!).

ECDSA

- Once we have the curve ($y^2 = x^3 + 7$), modular system (MOD 37) and a generating point (24, 17), an individual needing to digitally "sign" a document or order needs:

ECDSA

- a private key (d) and
- a random number (k)

ECDSA

- The private key (d) and random number (k) must be between 1 and 12.
- For this example, we will use the values of $d = 9$ and $k = 7$.
- The private key ($d = 9$) is used to create a public key (Q):
  $Q = d * G = 9 * (24, 17) = (32, 17)$

ECDSA

- The private key remains secure because of the difficulty of determining $d = 9$ from the generating point $(24, 17)$ and the public key $Q = 9 * G = (32, 17)$

ECDSA

- To sign a document or tranaction, a person calculates two values: r and s.
- r is the x value of $k * G = 7 * (24, 17) = (8, 1)$
- so $r = 8$

ECDSA

				x	y			
			1	24	17			
			2	23	36			
			3	18	17			
			4	32	20			
			5	6	36			
			6	8	36			
			7	8	1			
			8	6	1			
			9	32	17			
			10	18	20			
			11	23	1			
			12	24	20			
			13	0	0			

ECDSA

- $s = k^{-1}(m + dr) \bmod 13$, where m is the message we are sending.
- We will use $m = 1$ in this example for simplicity's sake.

ECDSA

- $s = k^{-1}(m + dr) \bmod 13$
- $s = 2 * (1 + 9 * 8) \bmod 13$
  $\equiv 2 * (1 + 72) \equiv 2 * (1 + 7) \equiv$
  $2 * 8 = 16 \equiv 3 \bmod 13$

ECDSA

- The signature consists of the pair of values:
  $r = 8, \quad s = 3$

ECDSA

- To verify this signature, the receiver computes $m * s^{-1} * G + r * s^{-1} * Q$
- $m * s^{-1} * G + r * s^{-1} * Q =$ $1 * 9 * (24, 17) + 8 * 9 * (32, 17)$
- $= (32, 17) + (23, 1) = (8, 1)$

ECDSA

- $(32, 17) + (23, 1) = (8, 1)$
- The x coordinate of this point should match the value of r, which it does.
- This indicates that a valid signature has been received.

ECDSA

- Why does this work?
- The value of r comes from the calculation of $k * G$.
- When the receiver calculates $m * s^{-1} * G + r * s^{-1} * Q$, they are reproducing this calculation.

ECDSA

- The sender calculates
  $s = k^{-1}(m + dr)$
- This means that:

$$s = k^{-1}(m + dr)$$
$$k * s = k * k^{-1}(m + dr)$$
$$k * s = 1(m + dr)$$
$$k * s * s^{-1} = s^{-1} * 1(m + dr)$$
$$k = s^{-1} * (m + dr) = m * s^{-1} + r * s^{-1} * d$$

ECDSA

- Then,
  $k * G = (m * s^{-1} + r * s^{-1} * d) * G$

- $(m * s^{-1} + r * s^{-1} * d) * G =$
  $m * s^{-1} * G + r * s^{-1} * d * G =$
  $m * s^{-1} * G + r * s^{-1} * Q = k * G$

ECDSA

- The point of all this is that anyone intercepting any of the values that are public would not be able to extract the private keys needed to make fake tranactions.

Bitcoin

- Bitcoin is the best known cryptocurrency and uses the blockchain concept to keep track of the ownership of bitcoin.

Bitcoin

- Bitcoin mining involves the process of verifying the digital signatures for every bitcoin transaction.
- This uses a very large amount of computing power and therefore a very large amount of electricity.

Bitcoin

- One power plant in upstate NY uses enough elctricity to power 35,000 homes in their mining operation.

Bitcoin

- Other issues with bitcoin:
- Banks typically have "know your customer" regulations that make them responsible if they do business with criminals.

Bitcoin

- As a result, bitcoin has become a haven for money made from human misery:
- human trafficking and slavery
- drug addiction
- illegal arms trading
- public corruption.

Bitcoin

Other issues with Bitcoin:

- Many people access bitcoin through a bitcoin exchange, which is a third party entity that maintains an individual's bitcoin ownership.

- In this case people are dependent upon the exchange to handle their business honestly.

Bitcoin

- Largest Bitcoin thefts
- Thodex ($2B) 2021 (Turkey)
- Mt. Gox ($450M) 2014 (Japan)
- QuadrigaCX ($215M) 2020 (Canada)
- Bitfinex($60M) 2016 (Virgin Islands)
- Binance($40M) 2019
  (China/Cayman Islands)
- crypto.com ($15M) 2022 (Singapore)

Bitcoin

- Bitcoin exchanges (like Coinbase and crypto.com) frequently stop trading when prices are volatile

  i.e. the times when the most people want to buy or sell.

Blockchain

- The blockchain concept is distinct from any of its applications.
- Many legitimate businesses use the blockchain concept for inventory (among other uses).

Cryptocurrency

- The best advice when dealing with cryptocurrency is, in fact, close to 500 years old:

Cryptocurrency

CAVEAT EMPTOR

LET THE BUYER BEWARE

Resources

The slides from this talk will be posted at:
https://richbeveridge.wordpress.com

Certicom ECC Tutorial

https://www.certicom.com/content/certicom/en/ecc-tutorial.html

Resources

The slides from this talk will be posted at:
https://richbeveridge.wordpress.com

Certicom ECC Tutorial

https://www.certicom.com/content/certicom/en/ecc-tutorial.html

Resources - websites

https://www.coindesk.com/markets/2014/10/19/the-math-behind-the-bitcoin-protocol/

https://hackernoon.com/what-is-the-math-behind-elliptic-curve-cryptography-f61b25253da3

https://www.johndcook.com/blog/2018/08/14/bitcoin-elliptic-curves/

https://medium.com/@gupta.ayush11786/elliptic-curve-cryptography-over-finite-fields-1d836453fbbe

https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

https://www.allaboutcircuits.com/technical-articles/elliptic-curve-cryptography-in-embedded-systems/

Resources - mathematical papers

Koblitz, Neal, Menezes, Alfred J., (2016), "Cryptocash, Cryptocurrencies, and Cryptocontracts"

Grunspan, Cyril, Perez-Marco, Ricardo, (2020), "The Mathematics of Bitcoin"

Johnson, Don, Menezes, Alfred, Vanstone, Scott, (2001), "The Elliptic Curve Digital Signature Algorithm"