Introduction to Cryptology

1.2 - Cryptography Today and Tomorrow

Federico Pintore

Mathematical Institute, University of Oxford (UK)

Cryptography Today and Tomorrow

The advent of new information technologies has led to advanced cryptographic techniques.

- some techniques have been already deployed
- some are the basis of technologies that have not yet reached the general public or are still under construction

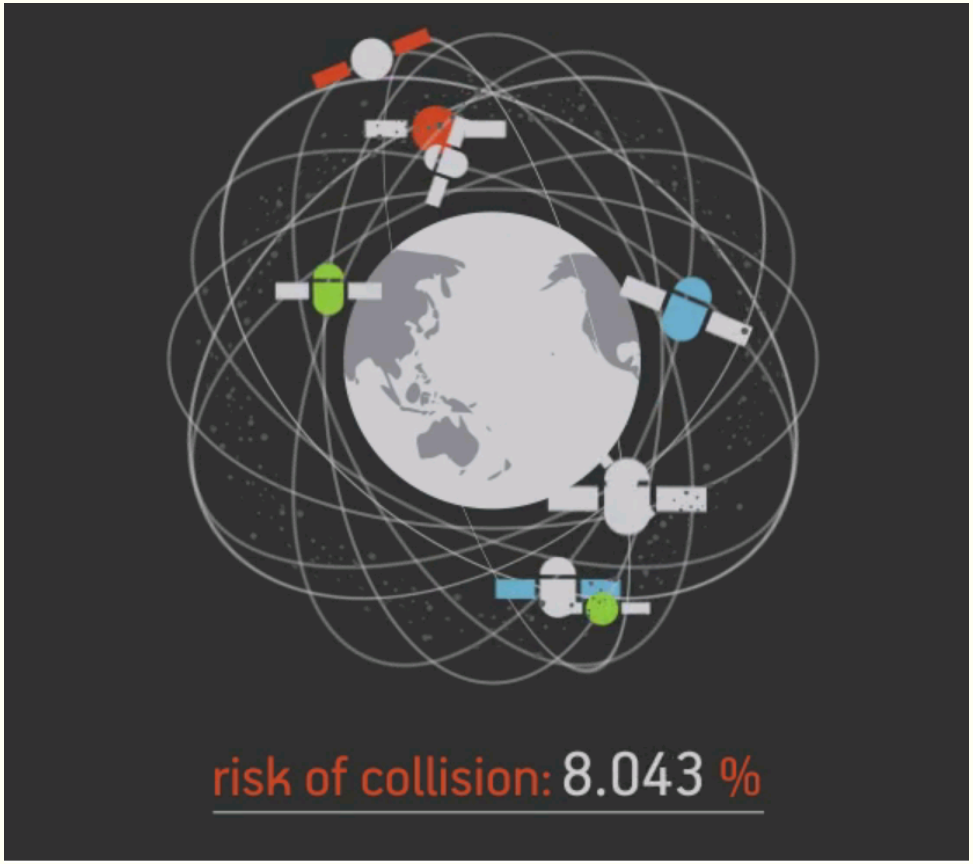
Multi-Party Computation

Context: n parties $P_1, \ldots, P_n$, each having a secret input s_i.

Objective: evaluate a public function f on input $(s_1, \cdots, s_n)$ while keeping each secret input hidden from the other parties.

Technique: Multi-Party Computation.

Multi-Party Computation: an application



https://www.youtube.com/watch?v=bAp_aZgX3B0

Secret Sharing

Context: a dealer distributes a secret s amongst n parties $P_1, \ldots, P_n$, giving to each party a share s_i.

Objective: at least t shares must be combined to reconstruct s (less shares should not provide any information about s).

Technique: Secret Sharing scheme.

Shamir Secret Sharing (1979)

Lagrange Interpolating Polynomial

Given n points $(x_1, y_1), \ldots, (x_n, y_n)$, $P(x) = \sum_{j=1}^{n} y_j P_j(x)$ with

$$P_j(x) = \prod_{\substack{k=1 \\ k \neq j}}^{n} (x - x_k)/(x_j - x_k),$$

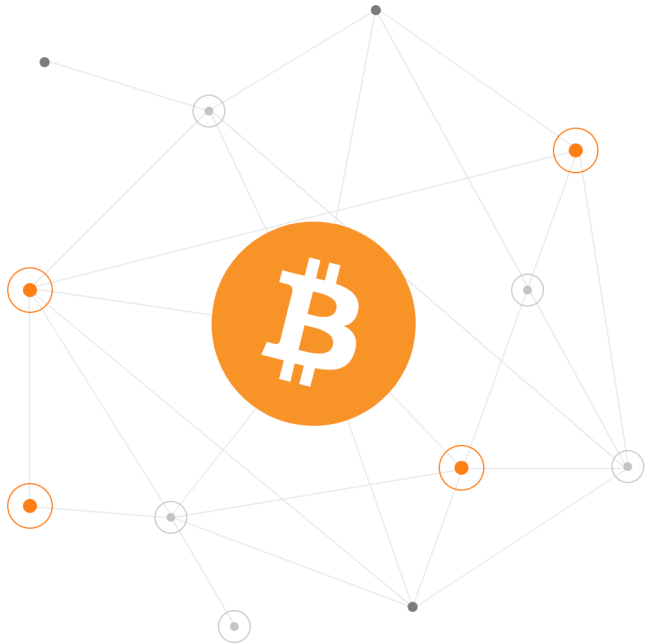
is the unique polynomial of degree $\leq (n-1)$ that passes through all the n points.

- Shares: let $Q(x) \in \mathbb{F}_p[x]$ be a random polynomial of degree $t-1$ s.t. $Q(0) = s$. Then $s_i := Q(i)$.
- Reconstruct the secret: using Lagrange interpolation, any t participants can together compute $Q(0)$.

Bitcoin - the first decentralised digital coin

Get started with Bitcoin

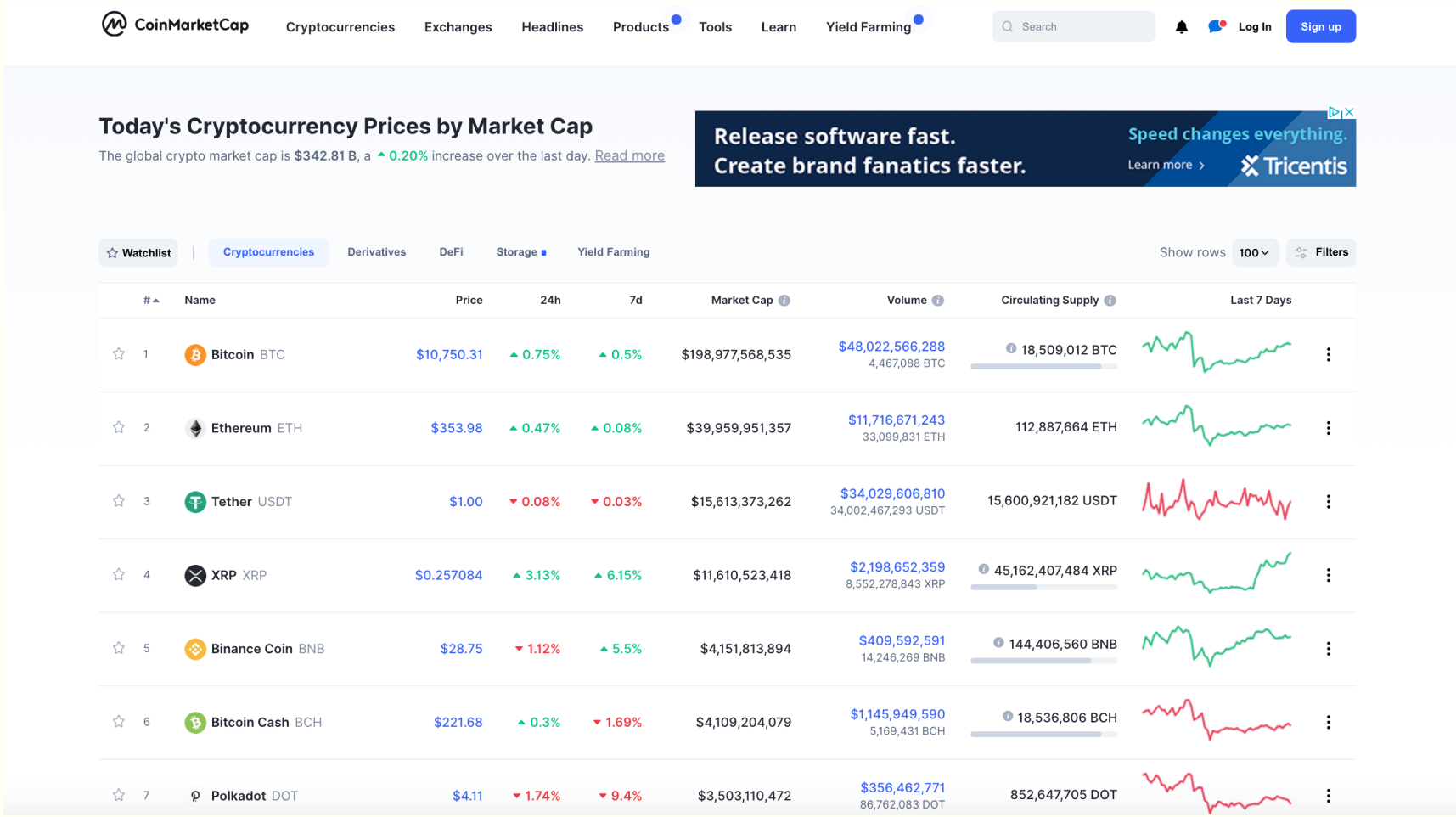
Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. **Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part**. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.



- **Fast peer-to-peer transactions**
- **Worldwide payments**
- **Low processing fees**

https://bitcoin.org/en/

Altcoins



CoinMarketCap Cryptocurrencies Exchanges Headlines Products Tools Learn Yield Farming Search Log In Sign up

Today's Cryptocurrency Prices by Market Cap

The global crypto market cap is **$342.81 B**, a ▲ 0.20% increase over the last day. Read more

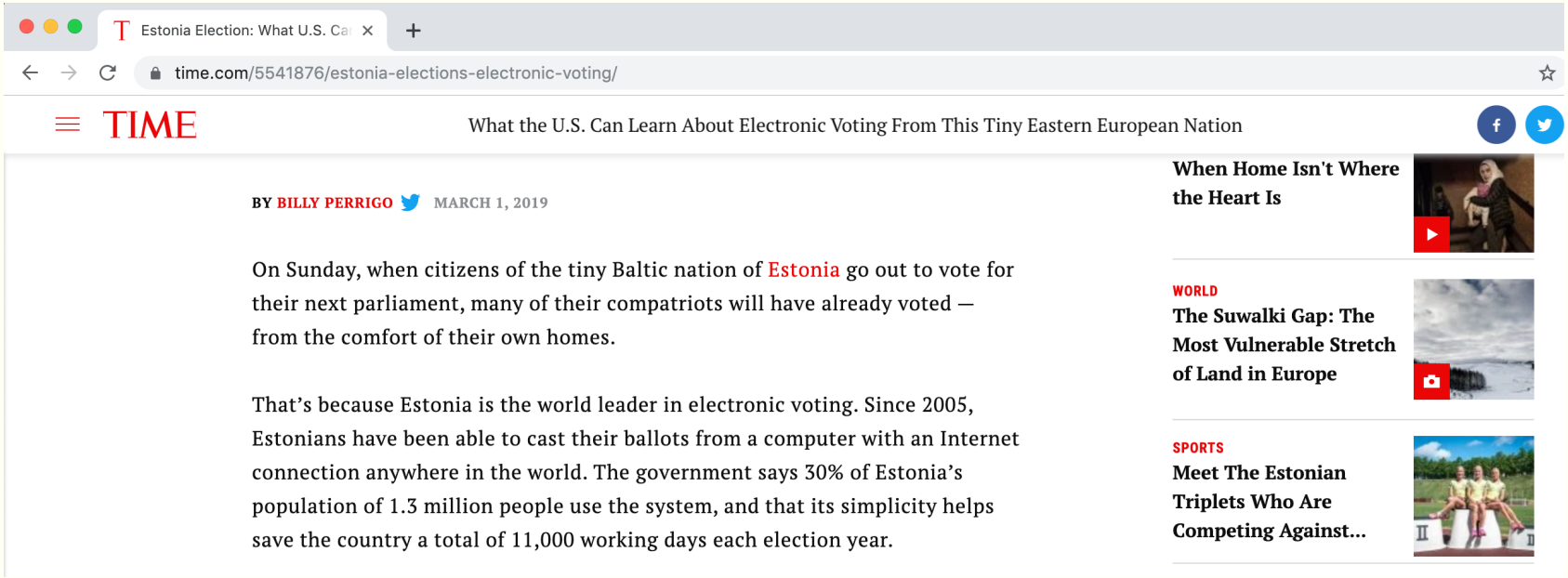
Watchlist | Cryptocurrencies | Derivatives | DeFi | Storage | Yield Farming

Show rows 100 Filters

#	Name	Price	24h	7d	Market Cap	Volume	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$10,750.31	▲ 0.75%	▲ 0.5%	$198,977,568,535	$48,022,566,288 4,467,088 BTC	18,509,012 BTC	
2	Ethereum ETH	$353.98	▲ 0.47%	▲ 0.08%	$39,959,951,357	$11,716,671,243 33,099,831 ETH	112,887,664 ETH	
3	Tether USDT	$1.00	▼ 0.08%	▼ 0.03%	$15,613,373,262	$34,029,606,810 34,002,467,293 USDT	15,600,921,182 USDT	
4	XRP XRP	$0.257084	▲ 3.13%	▲ 6.15%	$11,610,523,418	$2,198,652,359 8,552,278,843 XRP	45,162,407,484 XRP	
5	Binance Coin BNB	$28.75	▼ 1.12%	▲ 5.5%	$4,151,813,894	$409,592,591 14,246,269 BNB	144,406,560 BNB	
6	Bitcoin Cash BCH	$221.68	▲ 0.3%	▼ 1.69%	$4,109,204,079	$1,145,949,590 5,169,431 BCH	18,536,806 BCH	
7	Polkadot DOT	$4.11	▼ 1.74%	▼ 9.4%	$3,503,110,472	$356,462,771 86,762,083 DOT	852,647,705 DOT	

https://coinmarketcap.com/(06/10/2020)

E-voting


Estonia Election: What U.S. Ca
time.com/5541876/estonia-elections-electronic-voting/
TIME
What the U.S. Can Learn About Electronic Voting From This Tiny Eastern European Nation
BY BILLY PERRIGO MARCH 1, 2019
On Sunday, when citizens of the tiny Baltic nation of Estonia go out to vote for their next parliament, many of their compatriots will have already voted — from the comfort of their own homes.
That's because Estonia is the world leader in electronic voting. Since 2005, Estonians have been able to cast their ballots from a computer with an Internet connection anywhere in the world. The government says 30% of Estonia's population of 1.3 million people use the system, and that its simplicity helps save the country a total of 11,000 working days each election year.
When Home Isn't Where the Heart Is
WORLD
The Suwalki Gap: The Most Vulnerable Stretch of Land in Europe
SPORTS
Meet The Estonian Triplets Who Are Competing Against...

Zero-Knowledge Proofs

Context: two parties, P and V, interact over a channel.

Objective: P proves to V that some mathematical statement is true, without revealing anything else.

Zero-Knowledge Proofs

Context: two parties, P and V, interact over a channel.

Objective: P proves to V that some mathematical statement is true, without revealing anything else.

Statements can be about

- *facts* (e.g. the number N is square-free),
- *knowledge* (e.g. I know the factorisation of N).

Zero-Knowledge Proofs

Context: two parties, P and V, interact over a channel.

Objective: P proves to V that some mathematical statement is true, without revealing anything else.

Statements can be about

- *facts* (e.g. the number N is square-free),
- *knowledge* (e.g. I know the factorisation of N).

Technique: Zero-Knowledge Proof.

Zero-Knowledge Proofs - A Definition of Security

- Completeness: If a given mathematical statement is true, P always convinces V.

Zero-Knowledge Proofs - A Definition of Security

- Completeness: If a given mathematical statement is true, P always convinces V.
- Soundness: P cannot convince V if the mathematical statement is false.

Zero-Knowledge Proofs - A Definition of Security

- Completeness: If a given mathematical statement is true, P always convinces V.
- Soundness: P cannot convince V if the mathematical statement is false.
- Zero-Knowledge: The proof does not reveal any extra information beyond the validity of the statement.

Zero-Knowledge Proofs - Gentle introductions

- An informal blog post:

  http://blog.cryptographyengineering.com/2014/11/zero-knowledge-proofs-illustrated-primer.html

- An online demo:

  http://web.mit.edu/~ezyang/Public/graph/svg.html

Fully Homomorphic Encryption

Context: users storing data in a cloud system.

Objective: allow the cloud system to perform computation on encrypted data (no encryption keys given).

Technique: Fully Homomorphic Encryption.

Fully Homomorphic Encryption

- Some encryption schemes are naturally partially homomorphic, e.g. $E_e(m_1) \times E_e(m_2) = E_e(m_1 \times m_2)$.

Fully Homomorphic Encryption

- Some encryption schemes are naturally partially homomorphic, e.g. $E_e(m_1) \times E_e(m_2) = E_e(m_1 \times m_2)$.
- Fully homomorphic encryption allows for arbitrary computation on ciphertexts.

Fully Homomorphic Encryption

- Some encryption schemes are naturally partially homomorphic, e.g. $E_e(m_1) \times E_e(m_2) = E_e(m_1 \times m_2)$.
- Fully homomorphic encryption allows for arbitrary computation on ciphertexts.
- In theory, this was proven possible in 2009. In practice, it is still far away from being practical!

Post-Quantum Cryptography

What would happen to supposed-to-be hard mathematical problems if quantum computers existed?

Post-Quantum Cryptography

What would happen to supposed-to-be hard mathematical problems if quantum computers existed?

Integer factorisation and discrete logarithm problem can be solved *efficiently* with Shor's quantum algorithm.

Post-Quantum Cryptography

What would happen to supposed-to-be hard mathematical problems if quantum computers existed?

Integer factorisation and discrete logarithm problem can be solved *efficiently* with Shor's quantum algorithm.

New hard problems have been proposed and used to construct *quantum − resistant* cryptosystems.

Post-Quantum Cryptography

Different problems have led to different families of cryptographic schemes:

Post-Quantum Cryptography

Different problems have led to different families of cryptographic schemes:

- Lattice-based Cryptography (e.g. fully homomorphic encryption)

Post-Quantum Cryptography

Different problems have led to different families of cryptographic schemes:

- Lattice-based Cryptography (e.g. fully homomorphic encryption)
- Code-based Cryptography (e.g. McEliece cryptosystem)

Post-Quantum Cryptography

Different problems have led to different families of cryptographic schemes:

- Lattice-based Cryptography (e.g. fully homomorphic encryption)
- Code-based Cryptography (e.g. McEliece cryptosystem)
- Hash-based Cryptography (e.g. SPHINCS$^+$ signature)

Post-Quantum Cryptography

Different problems have led to different families of cryptographic schemes:

- Lattice-based Cryptography (e.g. fully homomorphic encryption)
- Code-based Cryptography (e.g. McEliece cryptosystem)
- Hash-based Cryptography (e.g. SPHINCS$^+$ signature)
- Multivariate Cryptography (e.g. Rainbow signature)

Post-Quantum Cryptography

Different problems have led to different families of cryptographic schemes:

- Lattice-based Cryptography (e.g. fully homomorphic encryption)
- Code-based Cryptography (e.g. McEliece cryptosystem)
- Hash-based Cryptography (e.g. SPHINCS$^+$ signature)
- Multivariate Cryptography (e.g. Rainbow signature)
- Isogeny-based Cryptography (e.g. SIKE)

Further Reading I

Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis Guillou, Marie Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, and Soazig Guillou.
How to explain zero-knowledge protocols to your children.
In Advances in Cryptology—CRYPTO'89 Proceedings, pages 628–631. Springer, 1990.

Alice Silverberg.
Mathematics and cryptography: A marriage of convenience?
In Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT 2020, pages 3–9. Springer, Cham., 2020.

Further Reading II


Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov.
The first collision for full sha-1.
In Annual International Cryptology Conference - CRYPTO 2017, pages 570–596. Springer, Cham., 2017.