Blockchains and Decentralized Applications

Thierry Sans

How Web3 Is Transforming The Future Of Business

Aleksandrs Malins Forbes Councils Member
Forbes Technology Council
COUNCIL POST | Membership (Fee-Based)

Apr 3, 2023, 06:45am EDT

Advantages Of Web3

From my experience implementing blockchain technology in projects, I've found that Web3 offers the following advantages.

• The main advantage is decentralization. This could refer to the networks, finance, identity, storage and more.

• It provides us with more secure and transparent systems because of blockchain implementation. Fewer people are involved in the processes, and they can view the transactions or transfers in real time.

• It offers the possibility to create digital assets such as NFTs to use in the metaverse.

Challenges Of Web3

The challenges I faced while developing Web3 projects included the following.

• The technology is complex, and it can be hard to find the right specialists.

• There's a lack of regulatory clarity (e.g., for game development and tokenization).

crypto.news news feature opinion follow-up markets learn prices Claim 5BTC free bonus

We must bridge the blockchain skills gap in 2024 | Opinion

January 28, 2024 at 12:47 pm

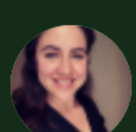
Disclosure: The views and opinions expressed here belong solely to the author and do not represent the views and opinions of crypto.news' editorial.

As we look at how the industry evolved over 2023 and hope glistens for the end of the "crypto winter," the web3 landscape is abuzz with opportunities. Yet, year after year, we address the same elephant in the room: the demand for web3 developers far outweighs the available expertise.

ccn CRYPTO TECHNOLOGY BUSINESS ANALYSIS OPINION EDUCATION

GUIDES 8 MIN READ EASY

Crypto Jobs Are Booming Again: What Skills Are In-Demand for 2025?



PUBLISHED NOVEMBER 29, 2024 9:06 AM
BY LORENA NESSI

WORLD ECONOMIC FORUM

EMERGING TECHNOLOGIES

How tokenization and on-chain capital markets are reshaping global finance

Mar 24, 2025

How $68 Trillion Could Transform Crypto Forever: The Tokenization Revolution You Can't Ignore

Blend Visions Follow 5 min read · Dec 12, 2025

What SEC Chairman Paul Atkins Just Revealed

The SEC's own chairman dropped a bombshell recently. He estimates **$68 trillion could move on-chain soon**. Within just two years, believe it or not.

That's US equities alone going fully tokenized. Think about that number for a second. The current crypto market cap is way smaller. Even 10% of that would double…

Cryptocurrencies

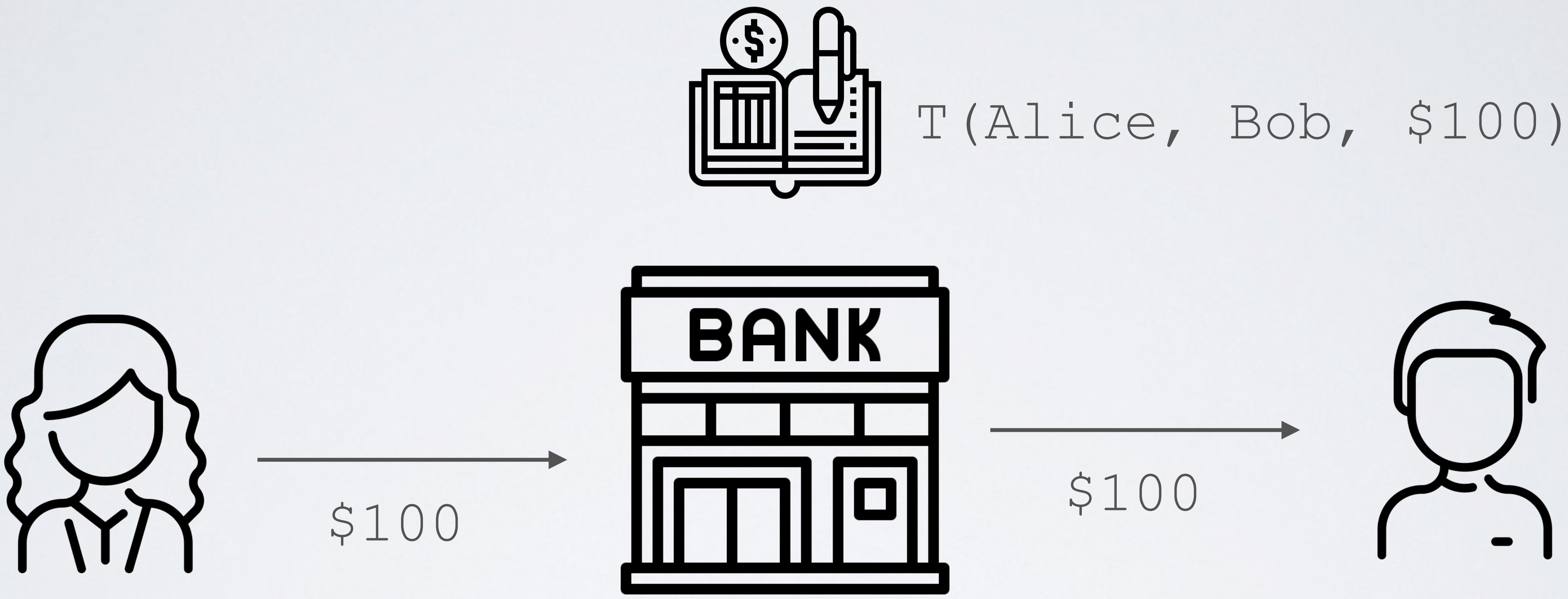
The original Bitcoin paper (2008)

Bitcoin: A Peer-to-Peer Electronic Cash System

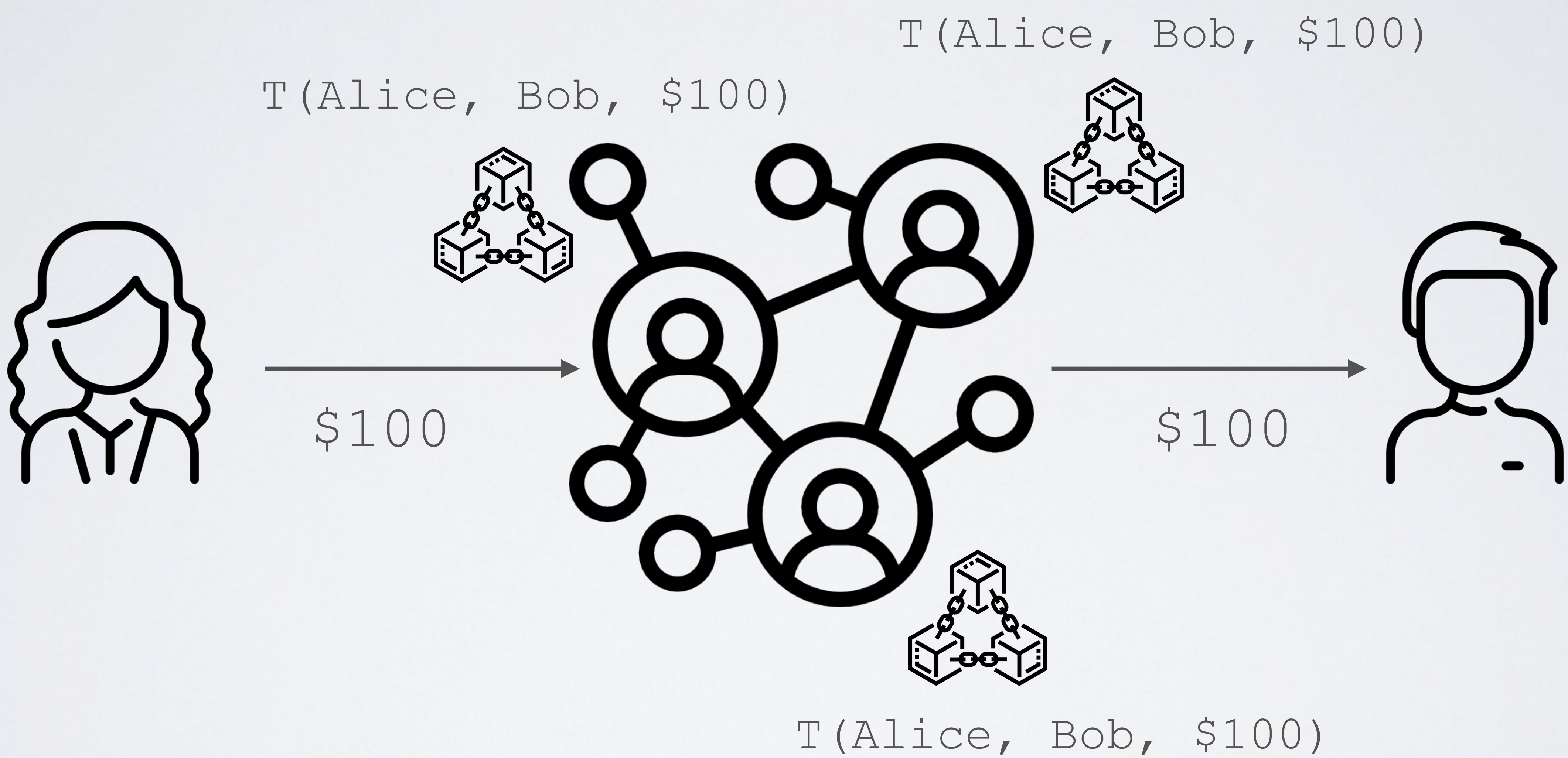
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

A centralized ledger (Trusted Third Party)



A decentralized ledger (Trustless)



Blockchain as a solution to common problems in distributed systems

- Transactions does propagate instantaneously and uniformly through the Network (might not be received in the same order or not even received at all)
- Nodes can join or leave the network dynamically
- Some nodes might be dishonest

➡ How to agree on a common state of the blockchain without any centralized authority and trusted-third party?
(see lecture on "Blockchain Consensus")

Beyond Cryptocurrencies

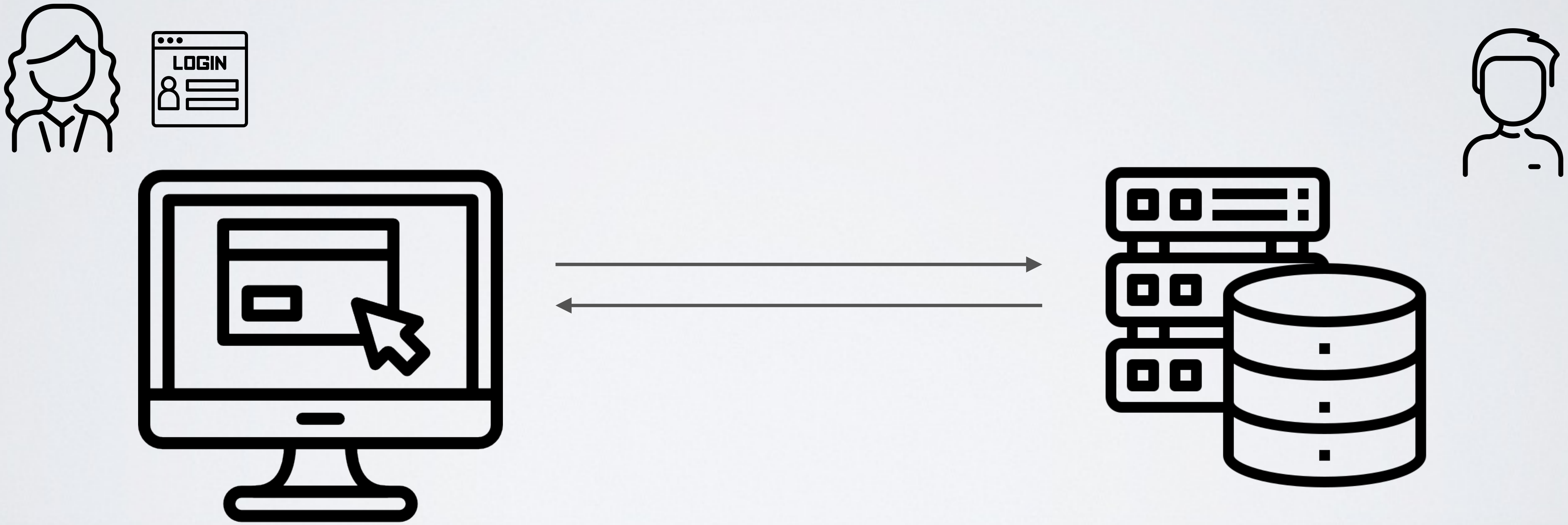
Towards Decentralized Applications

The original Ethereum Paper (2014)

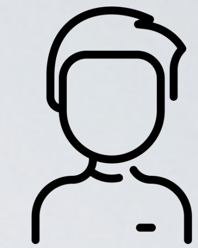
Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
By Vitalik Buterin (2014).

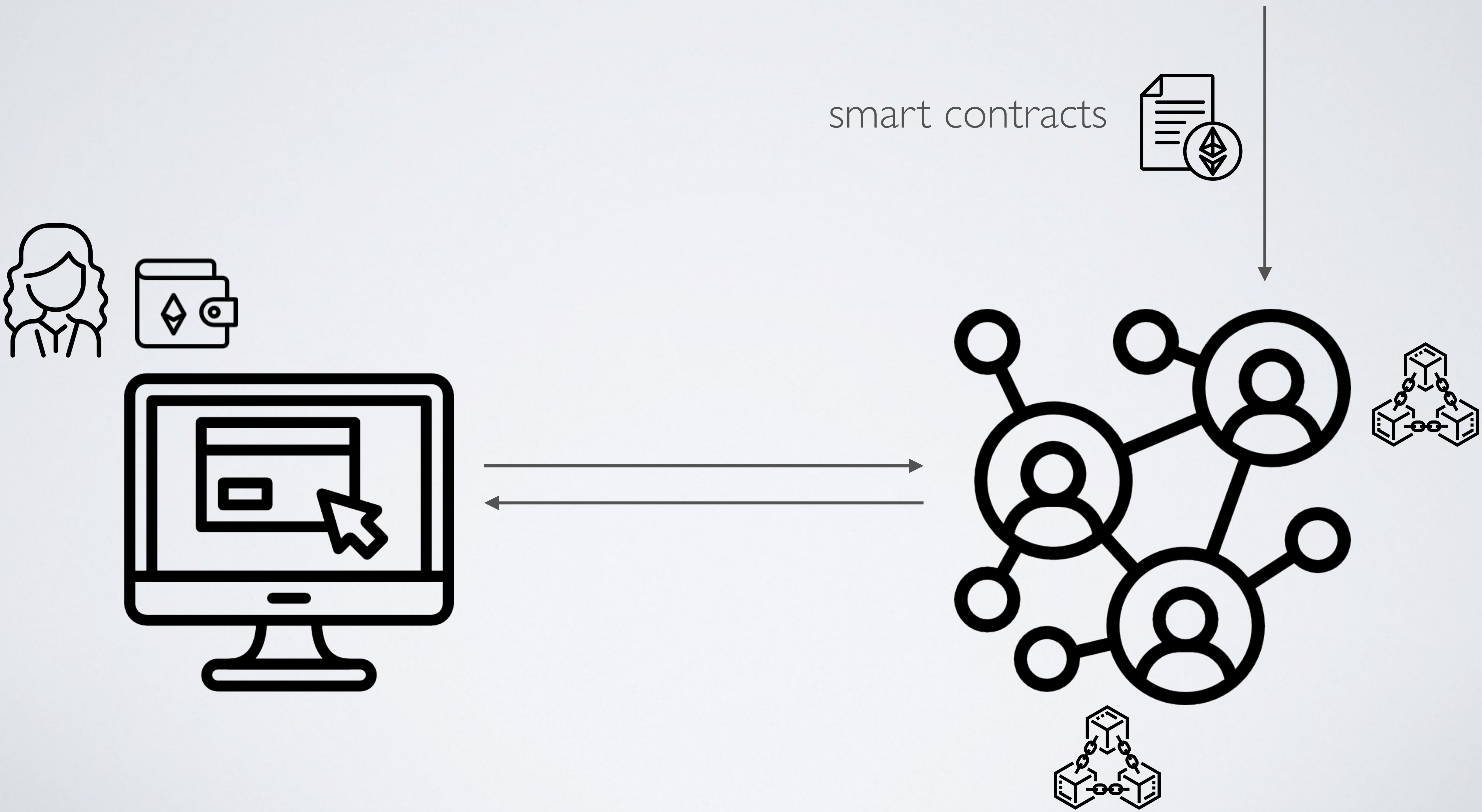
When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was simultaneously introducing two radical and untested concepts. The first is the "bitcoin", a decentralized peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So far, the "bitcoin" as a currency unit has taken up the bulk of the public attention, both in terms of the political aspects of a currency without a central bank and its extreme upward and downward volatility in price. However, there is also another, equally important, part to Satoshi's grand experiment: the concept of a proof of work-based blockchain to allow for public agreement on the order of transactions. Bitcoin as an application can be described as a first-to-file system: if one entity has 50 BTC, and simultaneously sends the same 50 BTC to A and to B, only the transaction that gets confirmed first will process. There is no intrinsic way of determining from two transactions which came earlier, and for decades this stymied the development of decentralized digital currency. Satoshi's blockchain was the first credible decentralized solution. And now, attention is rapidly starting to shift toward this second part of Bitcoin's technology, and how the blockchain concept can be used for more than just money.

Web 2 - The centralized Web



Web 3 - The **decentralized** web





Web3 Decentralized Applications (dApp)

- **DeFi** - enabling financial systems built without intermediaries
- **Asset Management** - enabling creation and exchange of digital assets (art, game assets, domain names, real world assets ...)
- **Decentralized Organizations** - enabling decision making without a centralized authority

Total cryptocurrency market cap

https://www.coingecko.com/en/charts

This course is about

- **Distributed Systems** - how multiples parties can agree on a shared state without centralized control
- **Security** - how to ensure integrity of this shared state without a trusted-third party and in the presence of potential adversaries
- **Economics** - how to incentivize these parties to participate in maintaining this share state in the network

Let's look at the course syllabus

https://thierrysans.me/CSCD71/

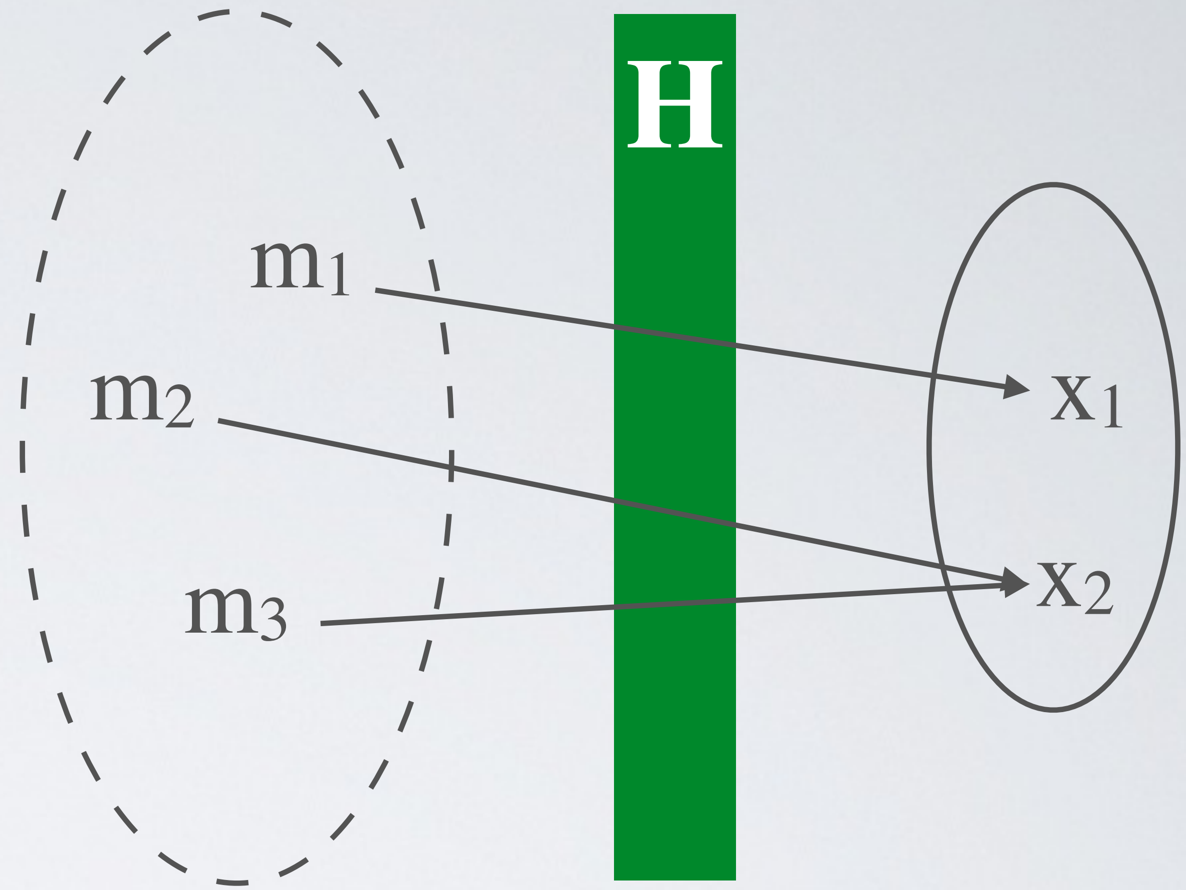
Cryptography Toolbox

The cryptography toolbox has many building blocks …

… but here we only need (for now):

- Hashing (Commitment Scheme and Merkle Tree)
- Digital Signature

Cryptographic Hashing



$H(m) = x$ is a hash function if

- m is a message of any length
- x is a message digest of a fixed length
- H is a non invertible function

➡ H is a lossy compression function
necessarily there exists x, m_1 and m_2 | $H(m_1) = H(m_2) = x$

Computational Properties

- ✓ Given **H** and **m**, computing **x** is **easy** (polynomial or linear)
- ◉ Given **H** and **x**, computing **m** is **hard** (exponential)
- ◉ Given **H**, **m** and **x**, it is hard (exponential) to find **m'** such that **H(m) = H(m') = x**
- ◉ Given **H**, it is hard (exponential) to find **m** and **m'** such that **H(m) = H(m') = x**

Commitment Scheme

A **cryptographic commitment** is a primitive that lets a party fix a value now while keeping it hidden, and reveal it later in a way that is verifiable

➡ Often described as the **digital equivalent of sealing a value in an envelope**

Phase 1 : Commit

```
x = commit(m)
```

$x = H(m)$

✓ The commitment x requires a fixed and minimal storage (32 bytes)

✓ The commitment x alone does not reveal the content of m (non reversible)

Phase 2 : Reveal and Verify

```
verify(x, m) = true
```

$x == H(m)$

✓ There can only be one message that matches (no collision)

(Naive) List Commitment Scheme

Commit several values as one commitment and prove that a value belongs to a collection

Phase 1 : Commit

$\texttt{x = commit(}m_0\texttt{, }m_1\texttt{,...,}m_n\texttt{)}$

$x = H(m_0, m_1, ..., m_n)$

Phase 2 : Reveal $\mathbf{m_i}$ and $\mathbf{p_i}$ to verify that $\mathbf{m_i}$ belongs to $\mathbf{x}$

$\texttt{verify(x, }m_i\texttt{, }p_i\texttt{) = true}$

$x == H(m_0, m_1, ..., m_n)$

- This scheme forces to reveal all messages in the proof $\mathbf{p_i}$

(Better) List Commitment Scheme using a Merkle Tree

Commit several values as one commitment

Phase 1 : Commit

```
x = commit(m₁, m₂, ..., mₙ)
```

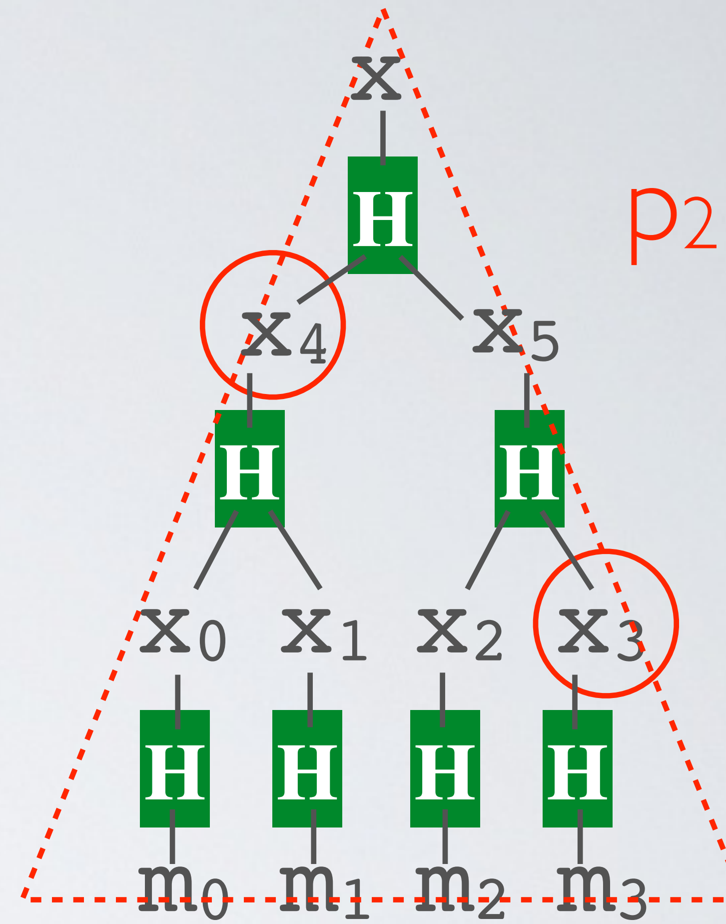
Phase 2 : Reveal m_i and verify that m_i belongs to x

```
verify(x, mᵢ, pᵢ) = true
```

✓ Small proof p_i : $\log_2(n)$

✓ Does not require to reveal the other messages in the proof p_i

Merkle Tree Example (n=3)



Example for m_2

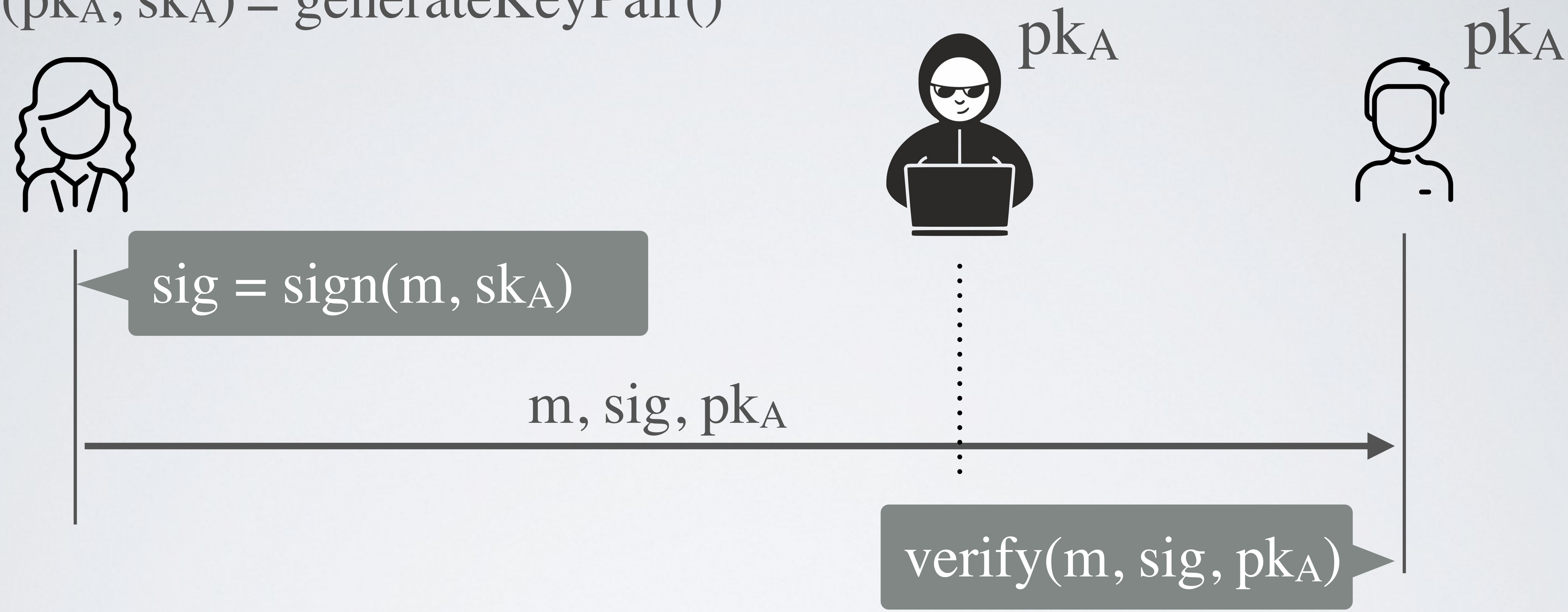
$x_2 = H(m_2)$

$x_5 = H(x_2, \mathbf{x_3})$

$x == H(\mathbf{x_4}, x_5)$

Digital Signatures

$(pk_A, sk_A) = \text{generateKeyPair}()$



Only Alice can sign a message $\mathbf{m}$ with her secret key $\mathbf{sk_A}$

➡ <u>Everybody</u> can verify $\mathbf{m}$ using Alice's public key $\mathbf{pk_A}$

Computational Properties

- ✓ (pk, sk) = generateKeyPair()
  is easy to compute (polynomial)
- ✓ sig = sign(m, sk_A)
  is easy to compute (either polynomial or linear)
- ✓ verify(m, sig, pk_A)
  is easy to compute (either polynomial or linear)
- Finding a matching key **sk**, given **pk** is hard (exponential)
- Forging a valid signature without knowing **sk** is hard (exponential)