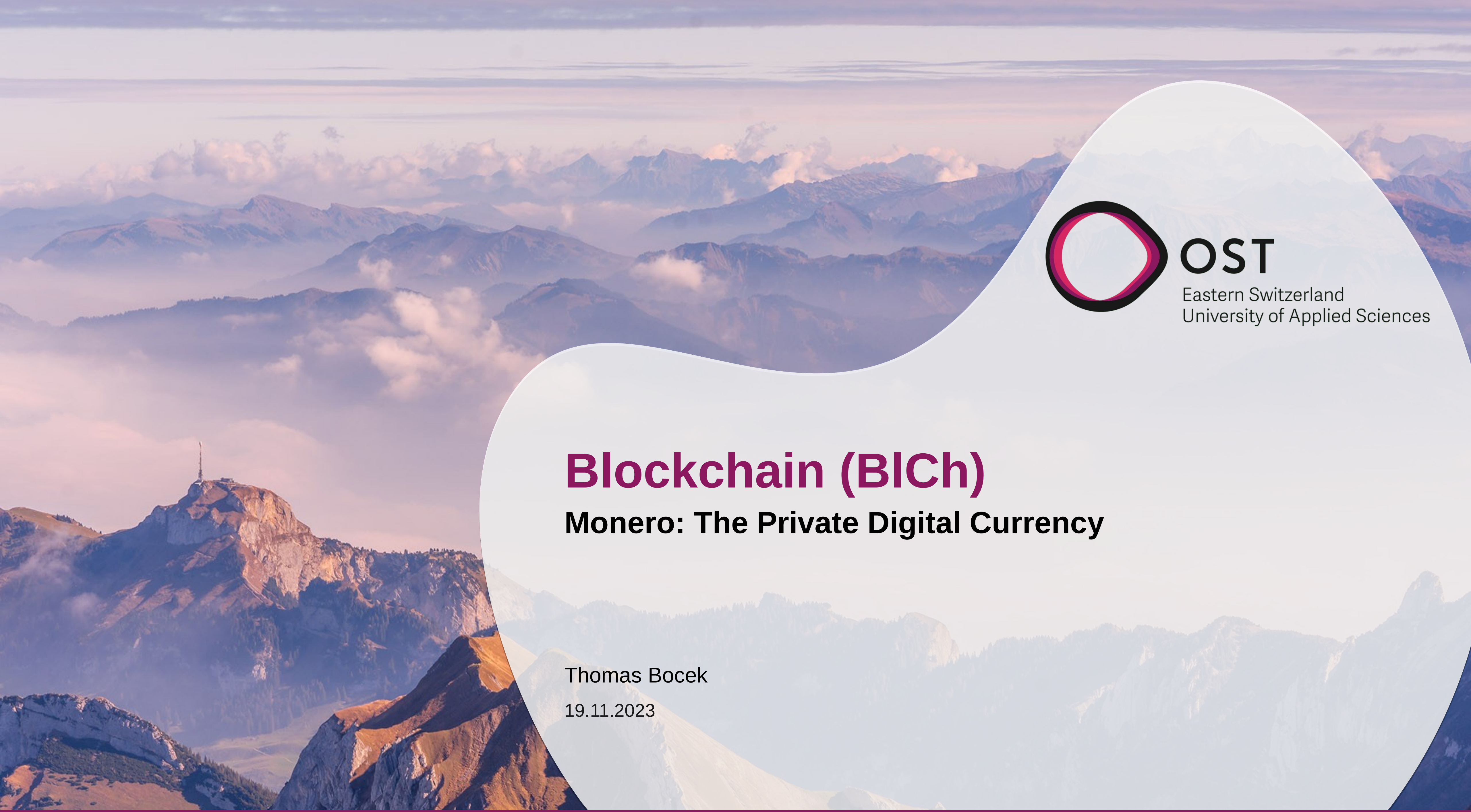


OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

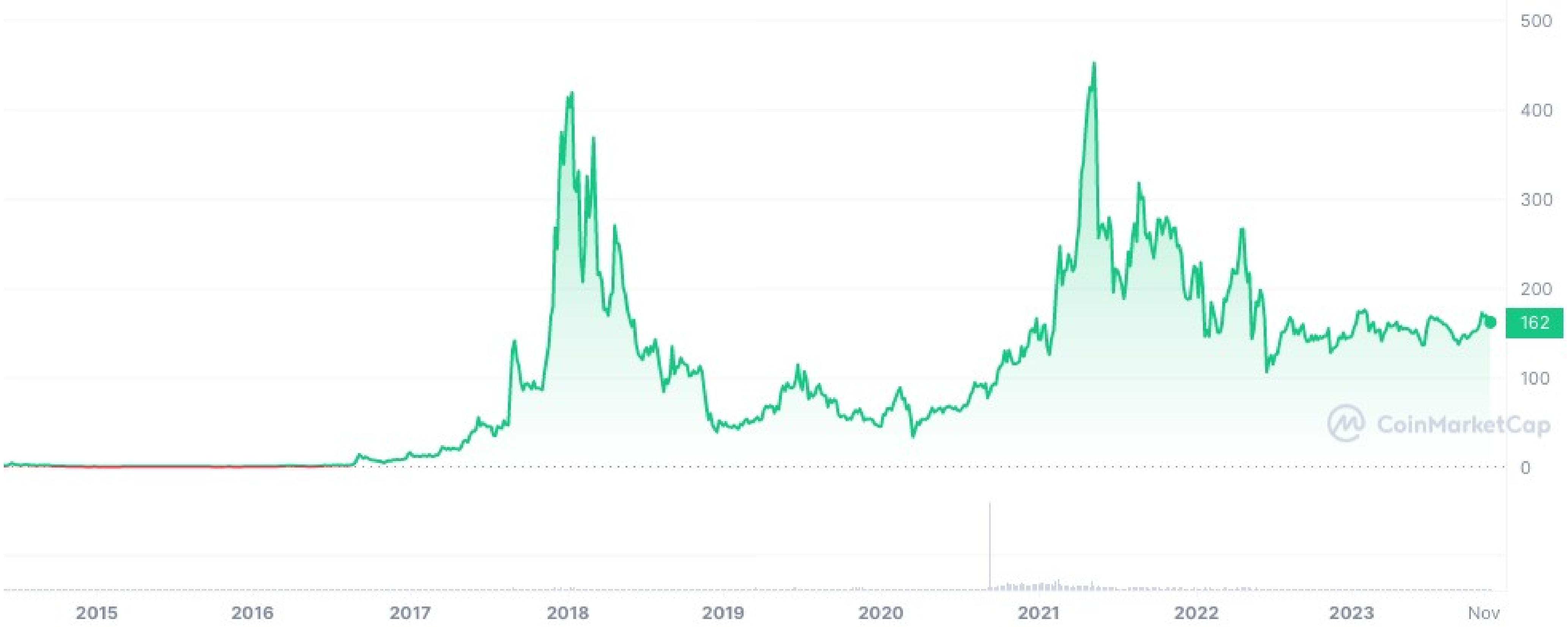
Monero: The Private Digital Currency

Thomas Bocek

19.11.2023

Monero's Market Performance

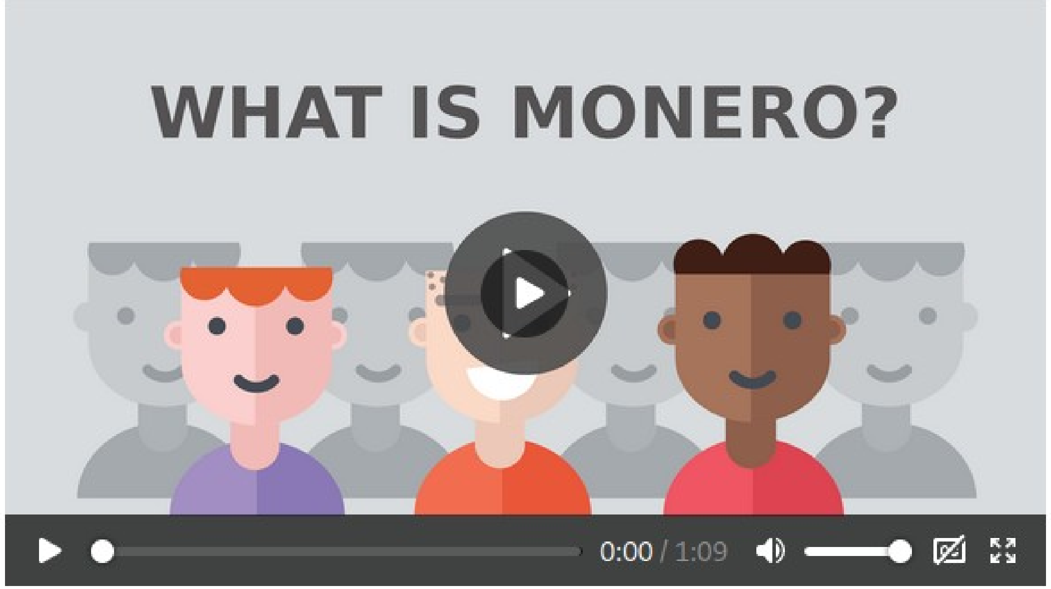
- Historical price trends, 1 XMR = 162 USD



Introduction to Monero (XMR)

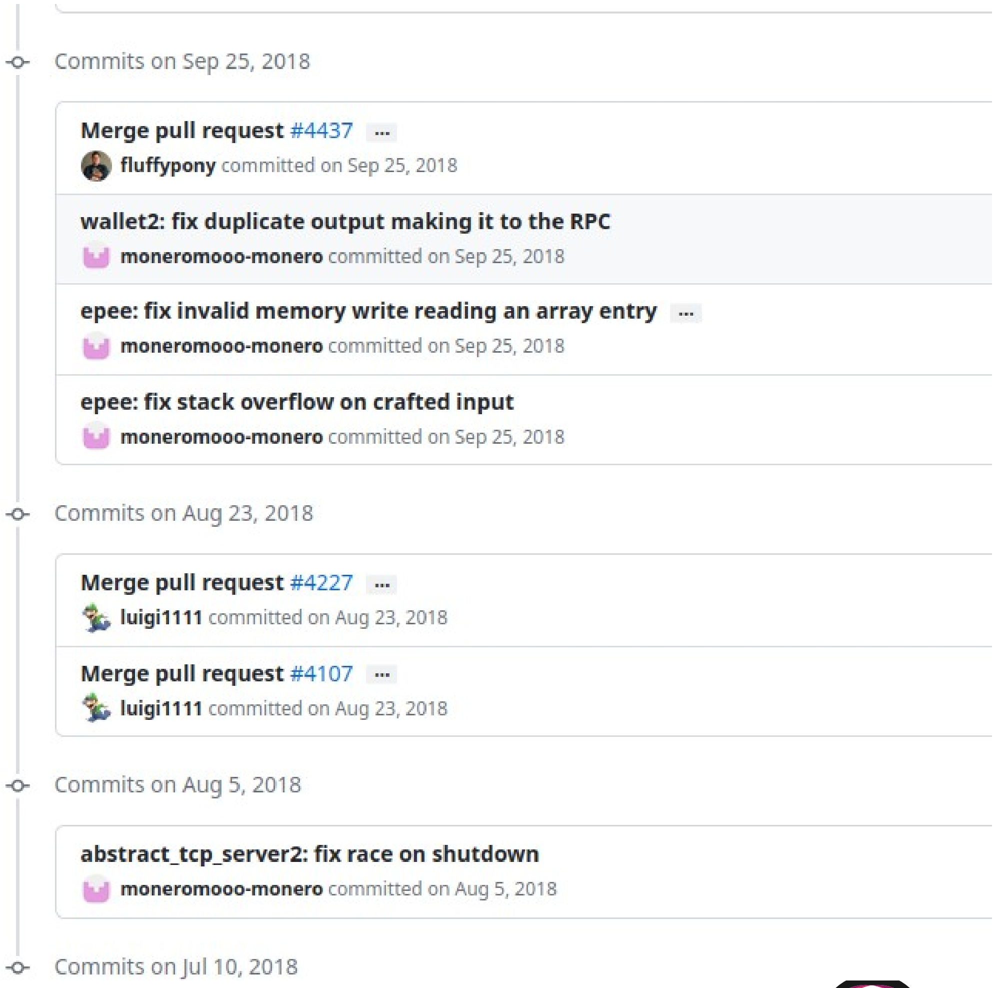
- Definition and Basic Concept
  - Monero (XMR): decentralized cryptocurrency emphasizes privacy, security, and untraceability
  - Monero transactions are confidential and untraceable, thanks to advanced cryptography
- Privacy Focus
  - Privacy by Default: designed to obscure senders, recipients, amount of transaction
  - Utilizes technologies Ring Signatures and Stealth Addresses, protect user identities and transaction details

- Explainer on https://www.getmonero.org/, https://www.getmonero.org/get-started/what-is-monero/



Introduction to Monero (XMR)

- Open Source and Decentralization
  - Monero is open source: code is publicly accessible – transparency, community-driven improvements.
  - Decentralized: no central authority controls Monero, maintained by a community of developers and users.
- Creation and Evolution
  - Monero was launched in April 2014 as a fork of Bytecoin (CryptoNote) -
    - Undergone several updates to enhance its privacy features and network efficiency
    - Bytecoin? Satoshi? Wild speculations



Commits on Sep 25, 2018

Merge pull request #4437 ...
fluffypony committed on Sep 25, 2018

wallet2: fix duplicate output making it to the RPC
moneromooo-monero committed on Sep 25, 2018

epee: fix invalid memory write reading an array entry ...
moneromooo-monero committed on Sep 25, 2018

epee: fix stack overflow on crafted input
moneromooo-monero committed on Sep 25, 2018

Commits on Aug 23, 2018

Merge pull request #4227 ...
luigi1111 committed on Aug 23, 2018

Merge pull request #4107 ...
luigi1111 committed on Aug 23, 2018

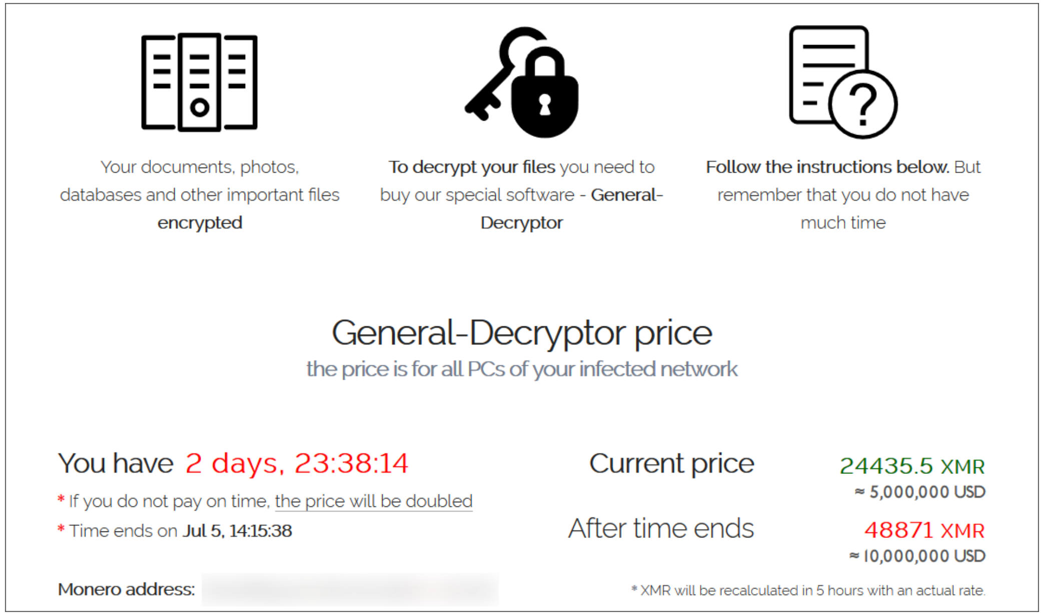
Commits on Aug 5, 2018

abstract_tcp_server2: fix race on shutdown
moneromooo-monero committed on Aug 5, 2018

Commits on Jul 10, 2018

Introduction to Monero (XMR)

- Key Characteristics
  - Untraceability: ring signatures mix a user's account keys with public keys from the blockchain ~impossible to identify sender
  - Fungibility: Monero coin is interchangeable and indistinguishable from another
  - Adaptive Block Size Limit: Unlike Bitcoin, Monero no predefined block size limit
- Challenges and Criticisms
  - Strong privacy features led to controversial discussions regarding illegal activities
  - Regulatory challenges due to its anonymity



Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have 2 days, 23:38:14

* If you do not pay on time, the price will be doubled

* Time ends on **Jul 5, 14:15:38**

Current price 24435.5 XMR ≈ 5,000,000 USD

After time ends 48871 XMR ≈ 10,000,000 USD

Monero address: [redacted]

* XMR will be recalculated in 5 hours with an actual rate

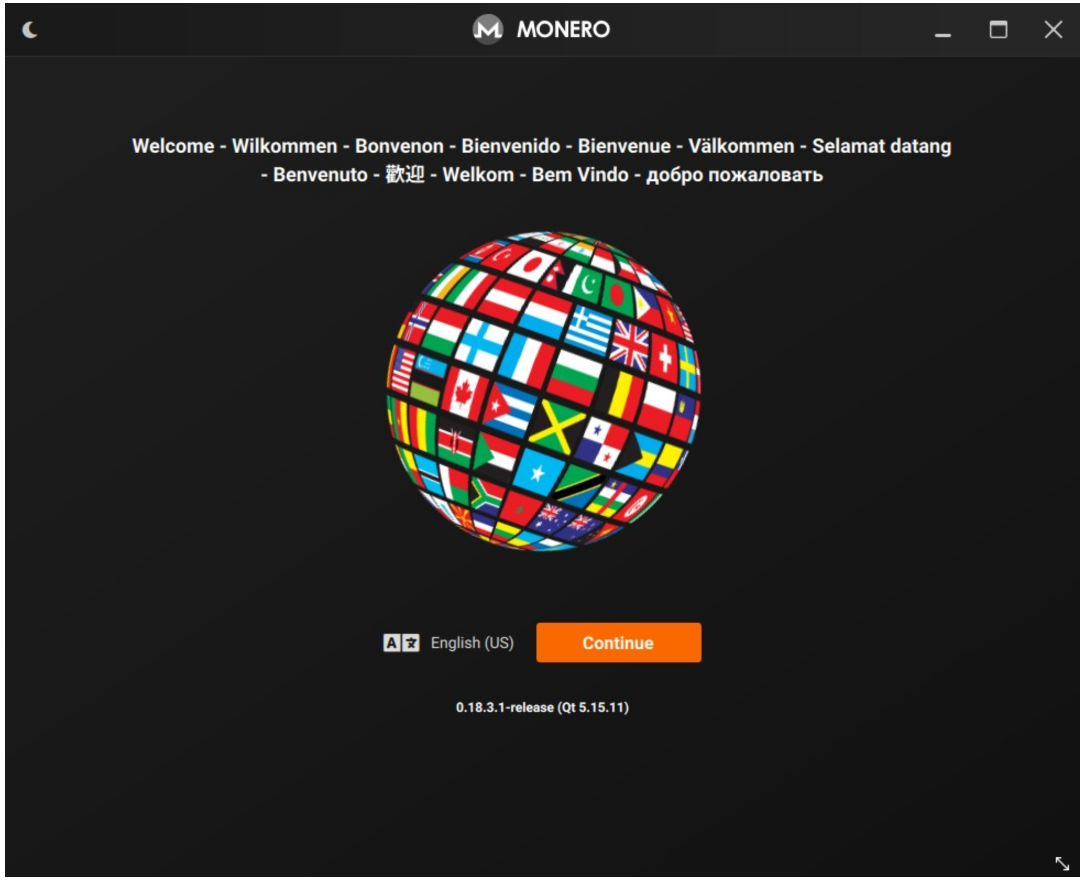
Source: https://en.wikipedia.org/wiki/File:Revil-ransom-demand.png

History and origin of Monero

- Pre-Monero background
  - Traced back to CryptoNote protocol, designed to address several perceived shortcomings in Bitcoin's protocol, particularly around privacy and scalability (chapter 2)
  - CryptoNote introduced innovations like ring signatures and stealth addresses, foundation of Monero
- Fork from Bytecoin
  - Monero was launched in April 2014, fork of Bytecoin, based on the CryptoNote protocol
  - Why fork? Concerns over Bytecoin’s pre-mined coins (>80%), raising questions about fairness and decentralization
- Early development and community involvement
  - Fork by user known as "thankful_for_today" on Bitcointalk forum. However, after disagreements with community regarding the direction, control handed over to community members
  - This group, known as the Monero Core Team, included notable figures like Riccardo Spagni (Fluffypony), Francisco Cabañas (ArticMine), and others
- Name and Symbol
  - The name "Monero" comes from the Esperanto word for "coin" or "currency,"
  - The currency symbol XMR stands for "Monero" and is widely recognized in the cryptocurrency community

History and origin of Monero

- Development Focus
  - Privacy and security
  - Open-source and crowdfunded, relies on donations and community support
- Key Updates and Forks
  - Several scheduled and unscheduled hard forks to improve its privacy, security, and scalability
    - Ring Confidential Transactions (RingCT)
    - Bulletproofs to enhance privacy and efficiency
  - Regular hard forks, ~6 months adapt to emerging technologies



Welcome - Wilkommen - Bonvenon - Bienvenido - Bienvenue - Välkommen - Selamat datang - Benvenuto - 歡迎 - Welkom - Bem Vindo - добро пожаловать

0.18.3.1-release (Qt 5.15.11)

Monero vs. Other Cryptocurrencies

- Foundational Technology
  - Bitcoin: first cryptocurrency, creating decentralized digital currency
  - Ethereum: platform for decentralized applications (dApps) using smart contracts
  - Monero: privacy and security, advanced cryptography to remain confidential and untraceable.
- Mining Algorithm
  - Bitcoin: Uses Proof-of-Work (PoW) with SHA-256 algorithm, high-power mining rigs, leading to centralization concerns
  - Ethereum: Originally PoW, resistance to ASIC mining, now transitioned to Proof-of-Stake, PoS)
  - Monero: Uses RandomX, a PoW algorithm optimized for CPUs, resistance to ASIC mining

Monero vs. Other Cryptocurrencies

- Scalability and Transaction Speed
  - Bitcoin: limited block size leads to slower transaction times and higher fees during peak usage
  - Ethereum: also scalability challenges, upcoming updates aim to address these with sharding
  - Monero: dynamic block size adjusts based on network demand, privacy enhancements can lead to larger transaction
- Fungibility
  - Bitcoin and Ethereum: Lack of fungibility; history of coins traceable, leading to 'tainted' coins
  - Monero: highly fungible, transaction history is untraceable

- Use Cases
  - Bitcoin: Widely used as a digital currency and a store of value ('digital gold')
  - Ethereum: powers many decentralized applications, from DeFi to NFTs, through its smart contract functionality
  - Monero: primarily used for transactions requiring high privacy, popular in regions or use-cases where financial privacy is paramount

The Technology Behind Monero

- Ring Signatures (built-in mixer)
  - Allow a sender to conceal identity by mixing their transaction's digital signature with other users' signatures
  - Outside observers cannot determine which user actually initiated transaction
- Bulletproofs
  - Non-interactive zero-knowledge proof, to prove a number (transaction amount) without revealing it
  - Significantly reduce transaction size (and fees) and improve verification speed
- Stealth Addresses
  - Protect receiver privacy
  - One-time addresses, generated randomly for each transaction on behalf of the recipient
    - Ensures destination of transaction remains hidden
  - Combination of the sender's, the recipient's public keys, and random data
    - Made in a way that only with recipient private key, these transactions can be found
- Kovri (I2P) Integration
  - Similar to TOR, but focus on creating an anonymous internal network