Investing in your future
OPERATION PART FINANCED BY THE EUROPEAN UNION
European Regional Development Fund

# SMART CITIES Conference

## What is Bitcoin and how does it work?

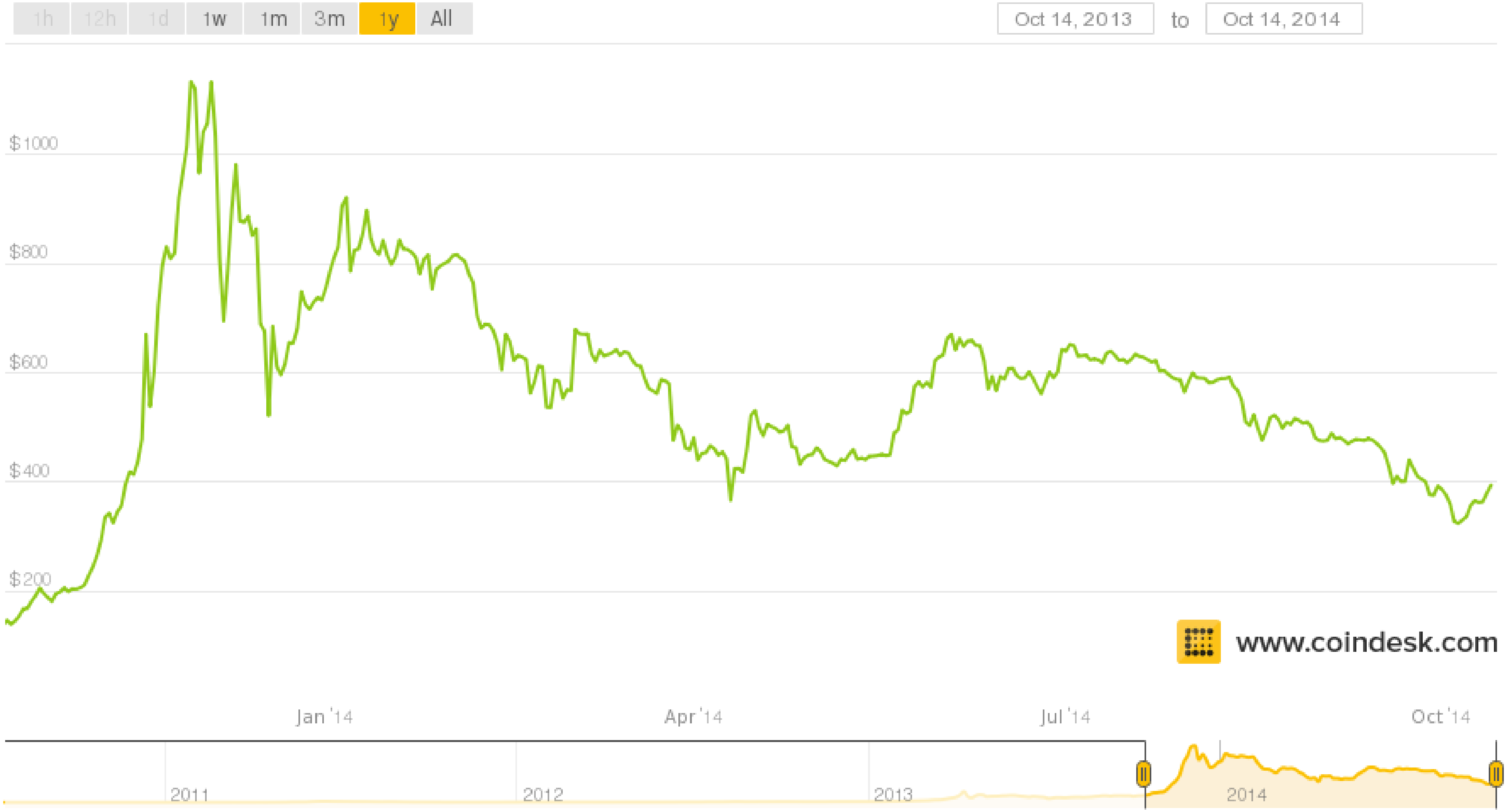
Matej Petković
Abelium

# Introduction

- Bitcoin is a cryptocurrency
- Advantages:
  - Aanonymity
  - No provisions
  - Peer-to-peer system
- Disadvantages:
  - High volatility
  - Small number of places where bitcoins can be spent

# Value of bitcoin

ABELIUM
Research & Development



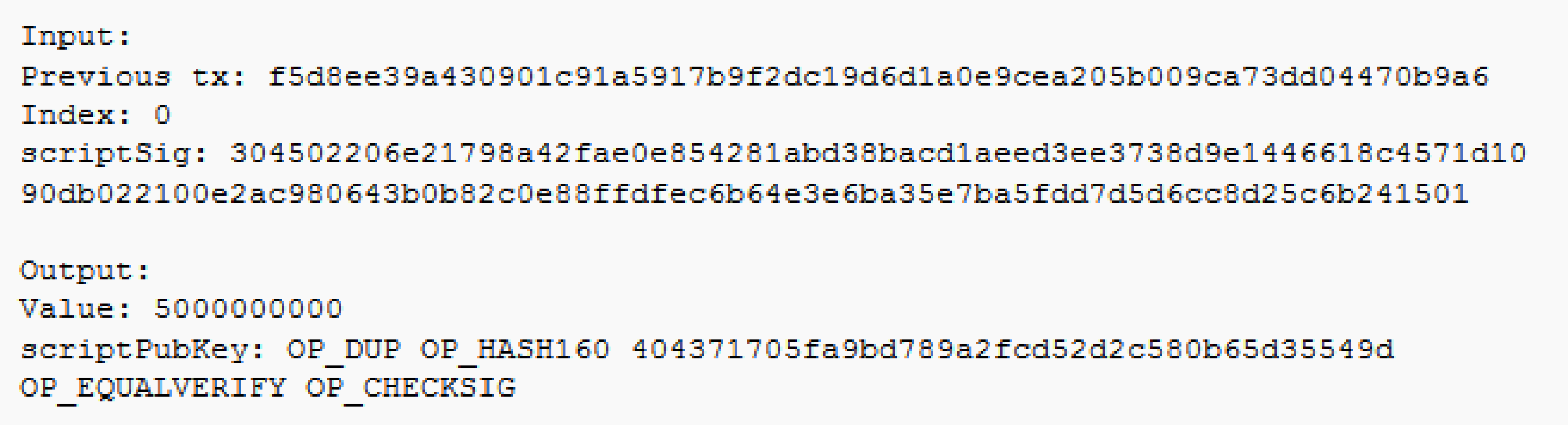
REPUBLIC OF SLOVENIA
**MINISTRY OF EDUCATION, SCIENCE AND SPORT**

UNIVERZA NA PRIMORSKEM
UNIVERSITÀ DEL LITORALE

*Investing in your future*
OPERATION PART FINANCED BY THE EUROPEAN UNION
European Social Fund

# Transactions in the system of Bitcoin

- Every transaction is a text file
- These files contain:
  - Data about bitcoins we are paying with
  - Receiver’s  Addresses to which our bitcoins are sent
  - Additional flags



```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

# Mining

- The heart of the system of Bitcoin
- Work of a miner:
  - Validation of transacitons
  - Grouping transactions into blocks

- Reword for creating a block:
  - 25 BTC
  - Fees, offered by creators of transactions

# Hash function

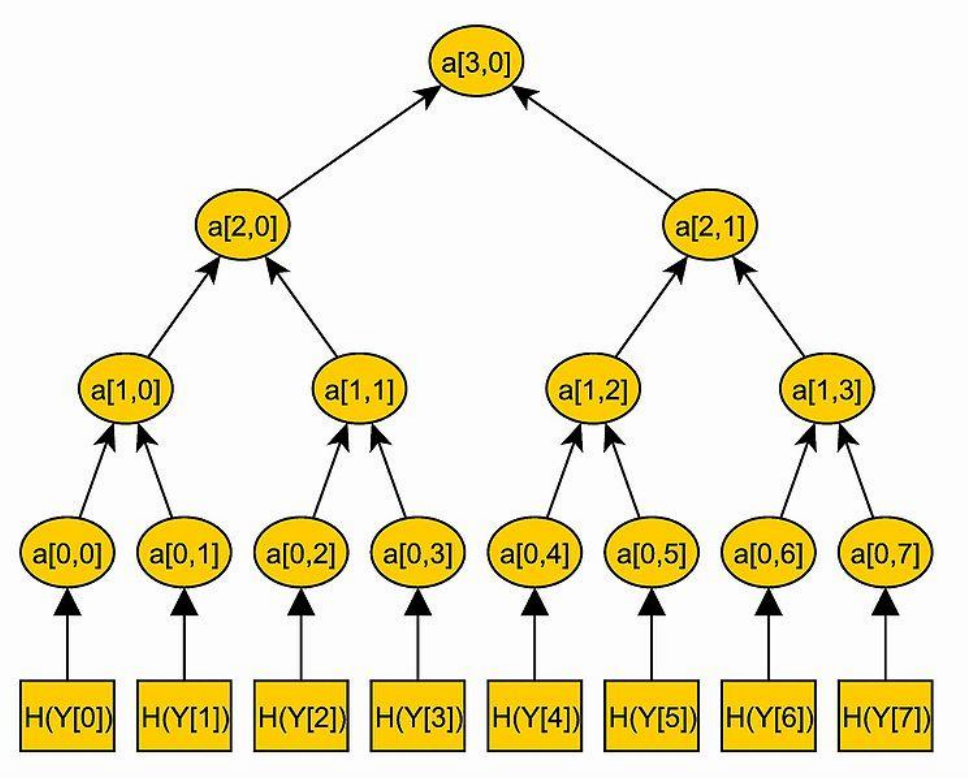
- any function that can be used to map digital data of arbitrary size to digital data of fixed size in a such way that it is practically impossible to find input if output is given
- In the system of Bitcoin, SHA256 is used

# Structure of a block

- Header:
  - hash value of this blok’s predecessor
  - Merkel root, derived from transactions included in the block
  - Time stamp
  - target
  - nonce
- List of transactions

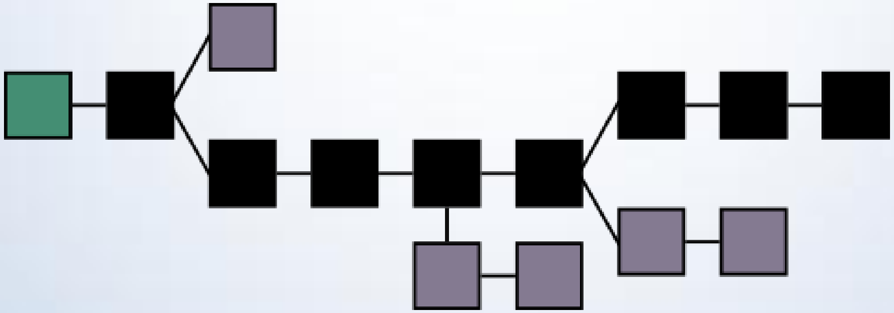
# Merkle tree

- Hash value H(Y)  of transaction Y is defined as SHA256(SHA256(Y))



# How to mine

- If SHA256(SHA256(header)) ≥ target,
  change the nonce (nonce = nonce + 1)
- Else: the block is completed
- If a new transaction occurs while mining, add it to the  block
- new block is appended to a *block chain*, which contains all valid transactions that were made in the system



# Theoretical possible ways of cheating

- Double spending
- 51% attack
- Spamming transactions

JAVNI SKLAD REPUBLIKE SLOVENIJE
ZA RAZVOJ KADROV IN ŠTIPENDIJE

# Thank You

Matej Petković
Abelium

*»Projekt delno financira Evropska unija, in sicer iz Evropskega socialnega sklada. Projekt se izvaja v okviru Operativnega programa razvoja človeških virov za obdobje 2007–2013, 1. razvojne prioritete »Spodbujanje podjetništva in prilagodljivosti« ter prednostne usmeritve 1.3. »Štipendijske sheme«, v okviru potrjene operacije »Po kreativni poti do praktičnega znanja«.*

REPUBLIC OF SLOVENIA
**MINISTRY OF EDUCATION, SCIENCE AND SPORT**

UNIVERZA NA PRIMORSKEM
UNIVERSITÀ DEL LITORALE

*Investing in your future*
OPERATION PART FINANCED BY THE EUROPEAN UNION
European Social Fund