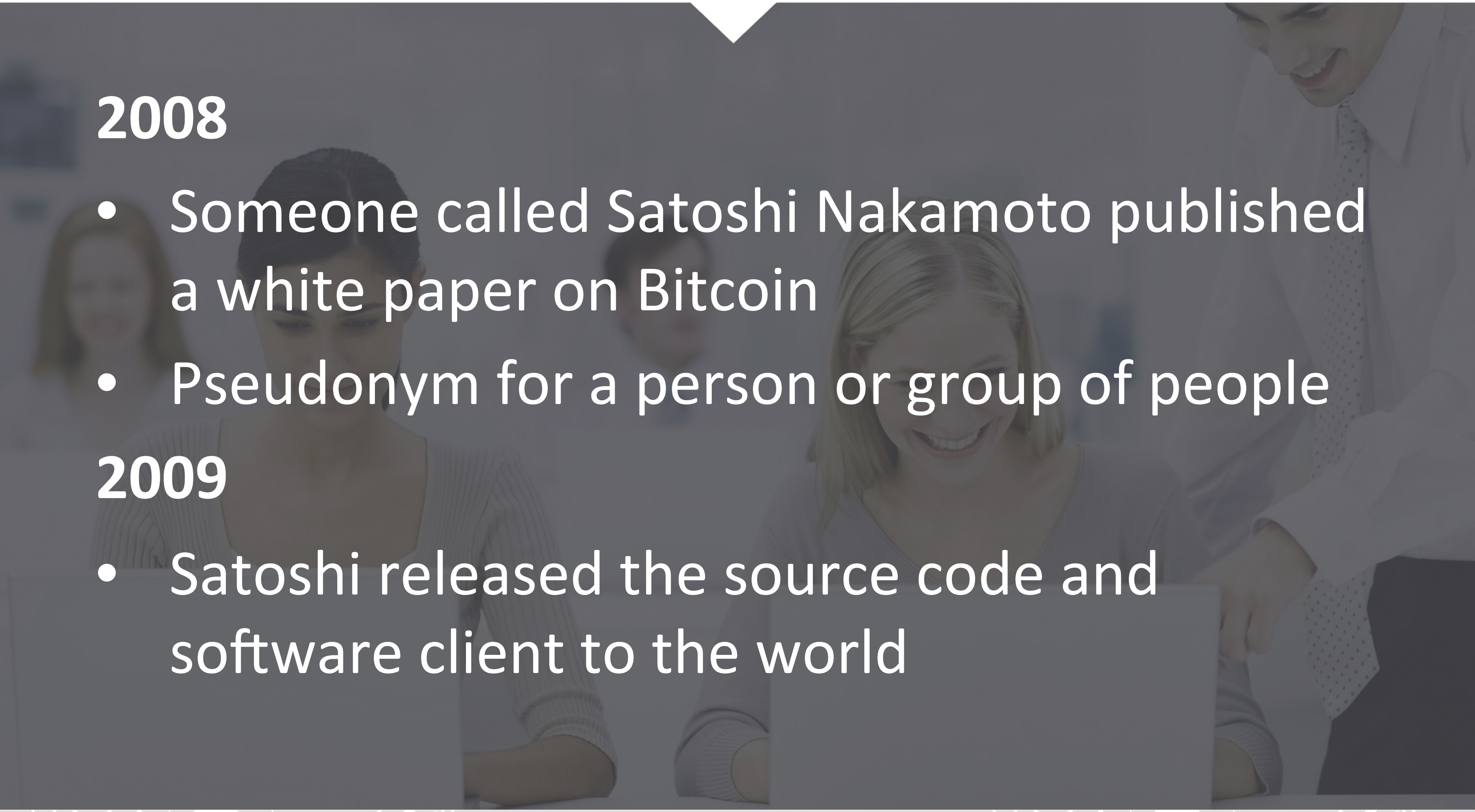
An Introduction to Bitcoin and Blockchain Technology

BITCOIN ACADEMY

Sonya Kuhnel, Managing Director

The History of Bitcoin



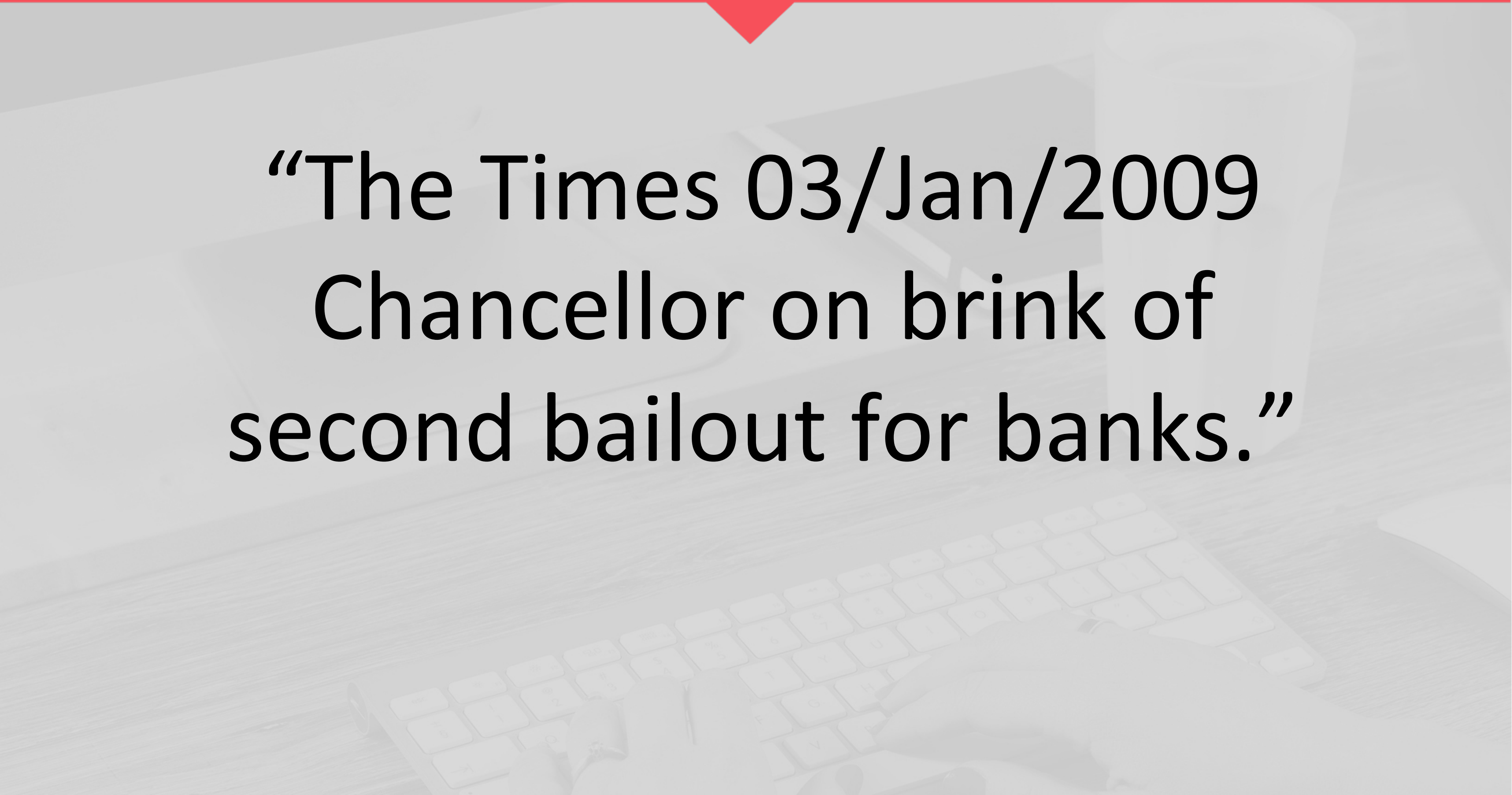
2008

- Someone called Satoshi Nakamoto published a white paper on Bitcoin
- Pseudonym for a person or group of people

2009

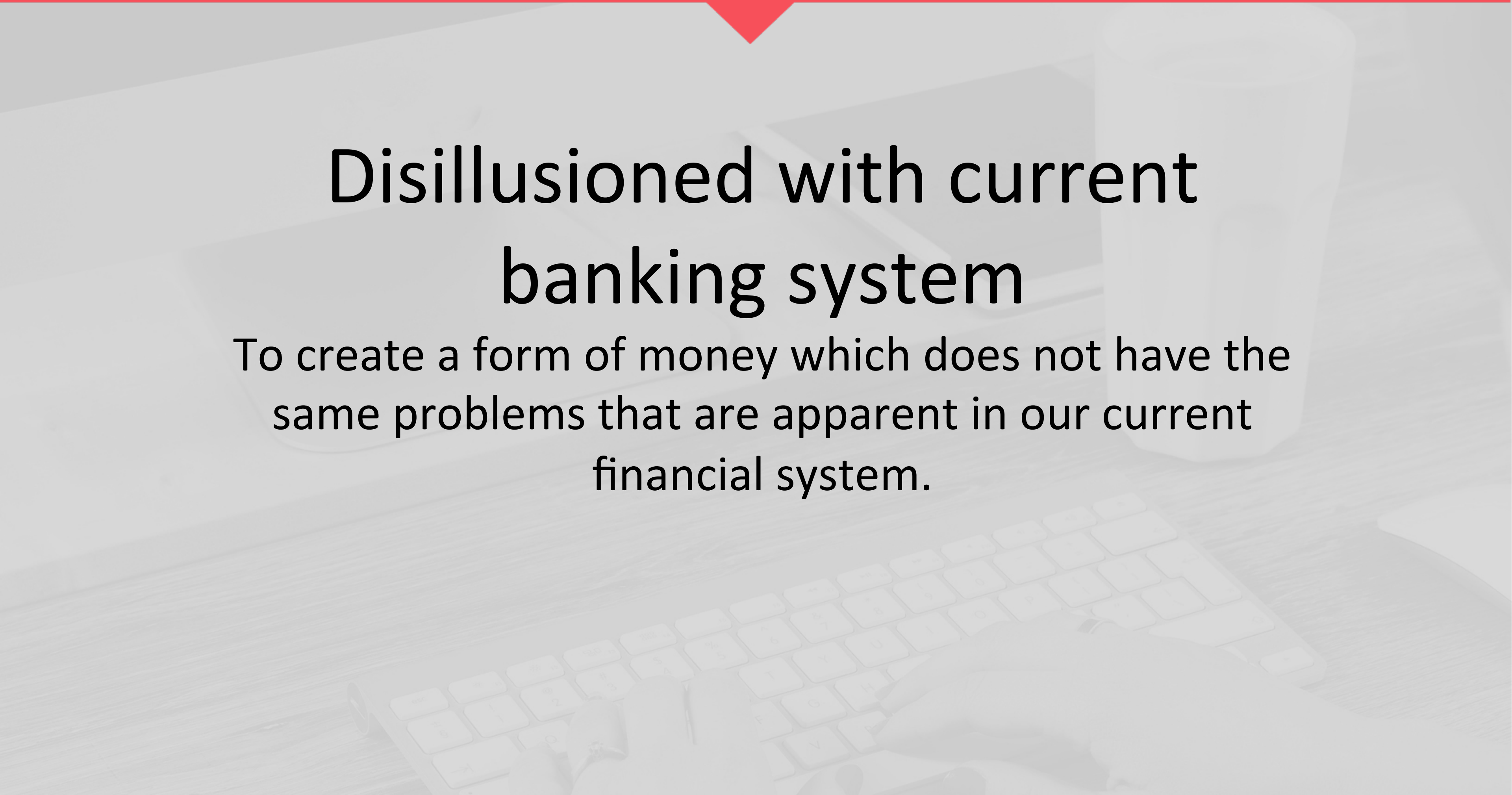
- Satoshi released the source code and software client to the world

Comment by Satoshi in first block



"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

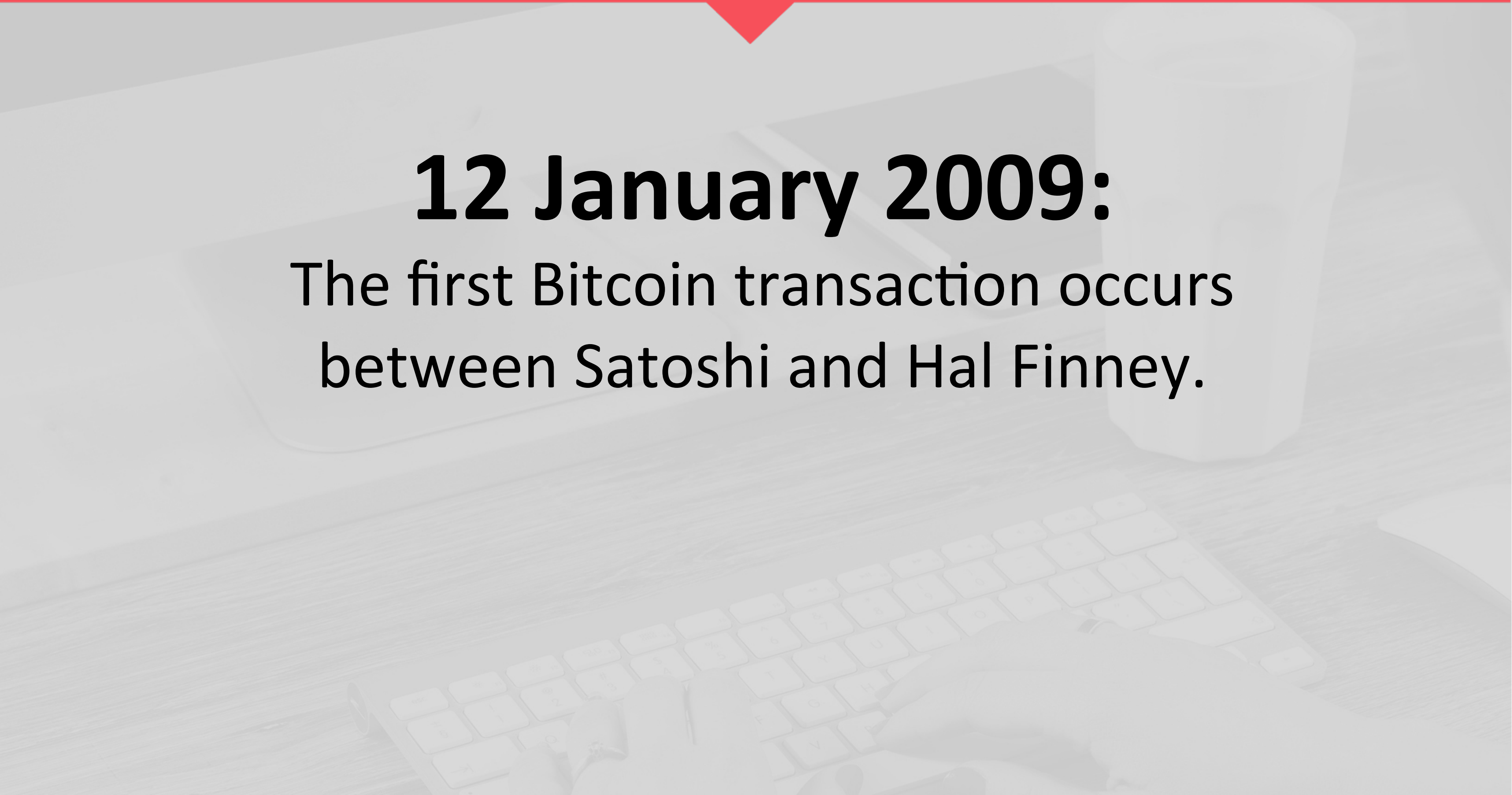
Possible Motive



Disillusioned with current banking system

To create a form of money which does not have the same problems that are apparent in our current financial system.

The First Bitcoin Transaction



12 January 2009:

The first Bitcoin transaction occurs between Satoshi and Hal Finney.

Pizza is bought using bitcoin

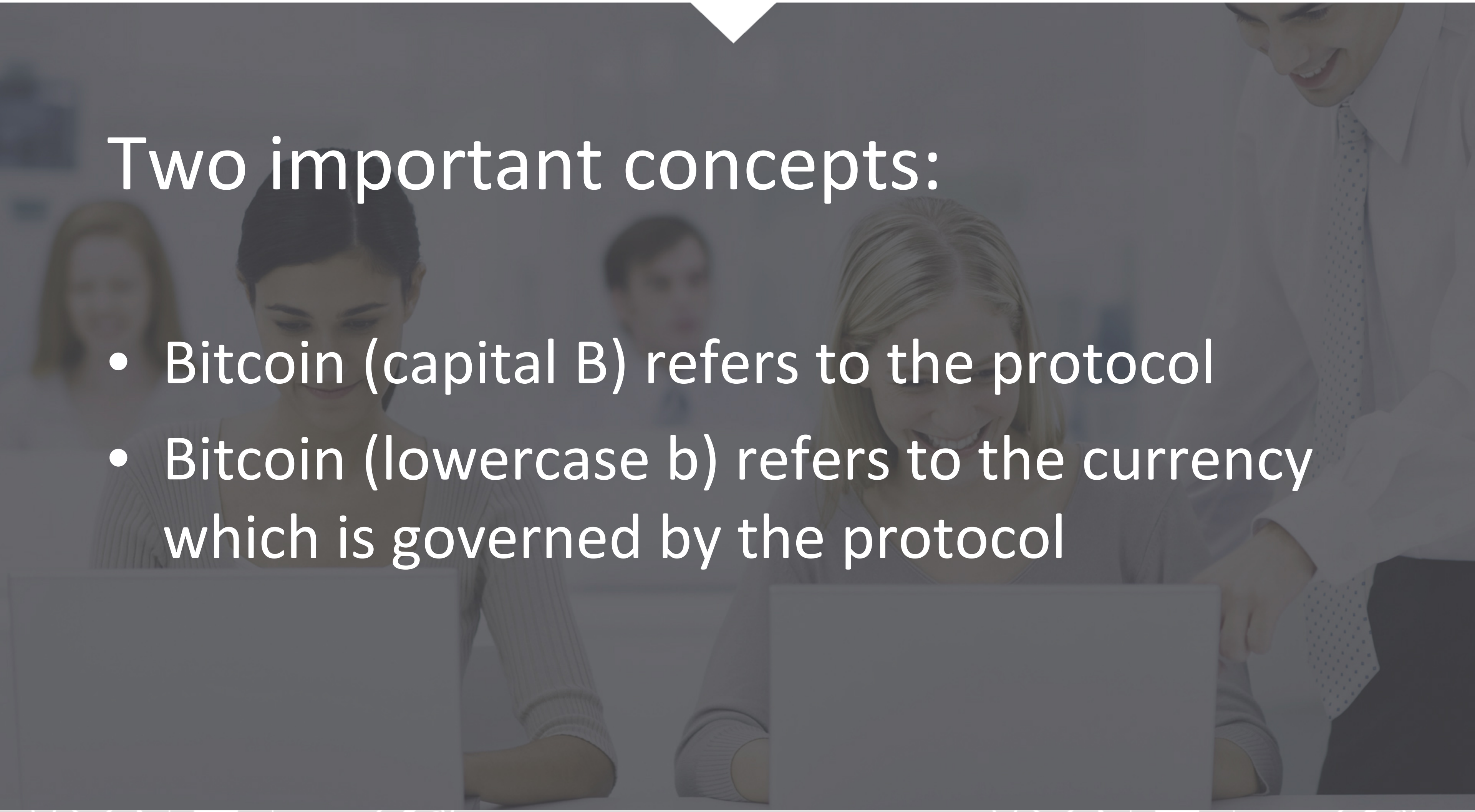
22 May 2010:

The first, real-world transaction occurs when a developer in the US pays **10,000 bitcoin** for a pizza. At the time, the exchange rate put the purchase price for the pizza at around US$25.

At todays BTC price = R95 million

What is Bitcoin?

Bitcoin vs. bitcoin



Two important concepts:

- Bitcoin (capital B) refers to the protocol
- Bitcoin (lowercase b) refers to the currency which is governed by the protocol

What is Bitcoin?

- **Digital currency**: created and held electronically
- **Not printed**
- **Decentralised**
- A **peer-to-peer payment network**
- Created through **mining**
- Underlying technology: the **blockchain**
- **Technology and a protocol**

The Bitcoin Protocol

Internet
TCP/IP

Web Pages
HTTP

Email
SMTP / IMAP

Bitcoin
MOIP
Money Over Internet **Protocol**

Applications built on TCP/IP Protocol

What can it be used for?

As a currency:
People can use bitcoin to pay for goods and services online or in a retail environment.

As a technology
The blockchain, bitcoin's underlying technology, can be used to store data and rules to execute smart contracts; for example, title deeds.

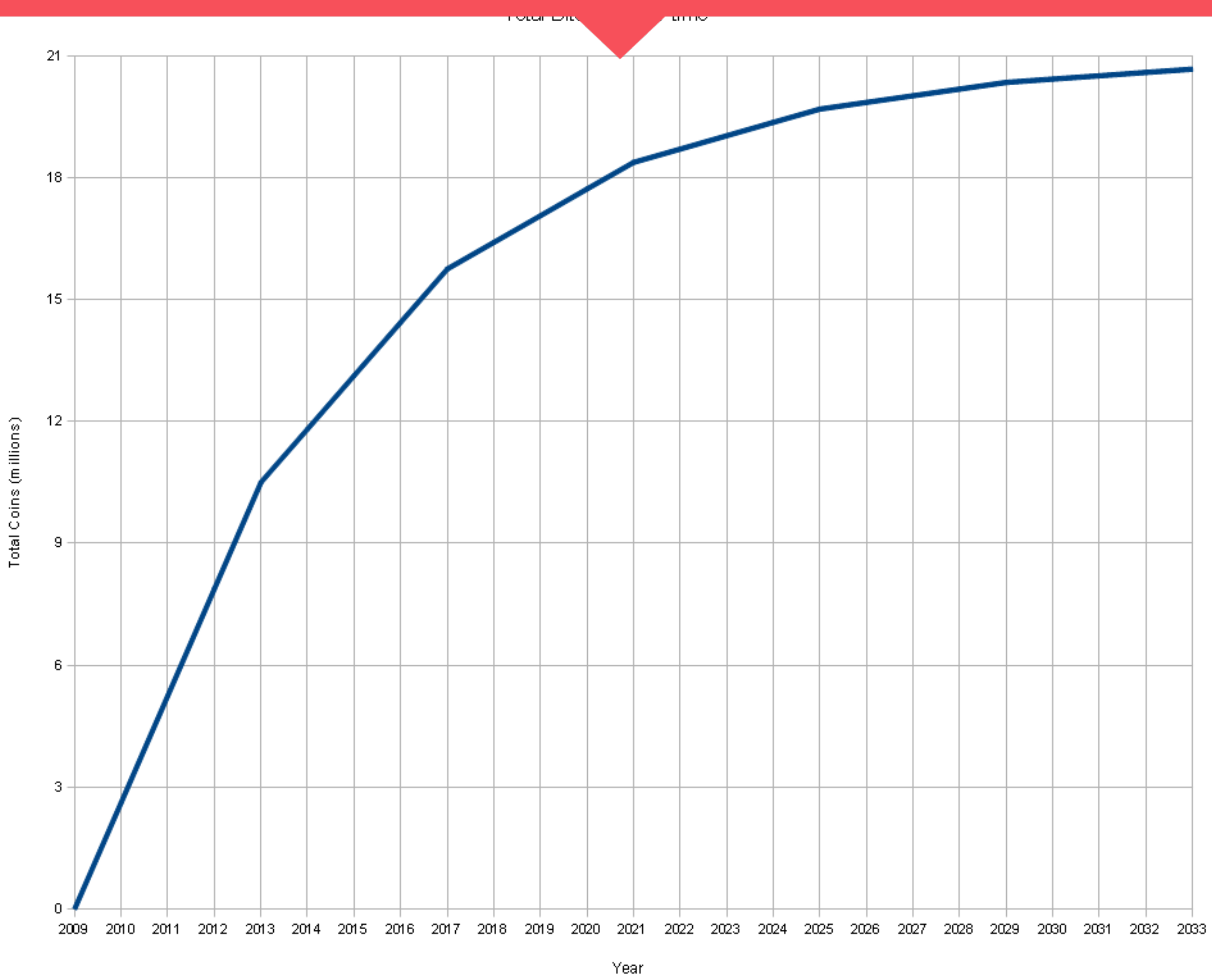
As a commodity
Some people view Bitcoin as a commodity, and have invested in Bitcoin and speculate on the price.

The Currency (bitcoin)

How many bitcoins exist?

21 million

Total bitcoin over time



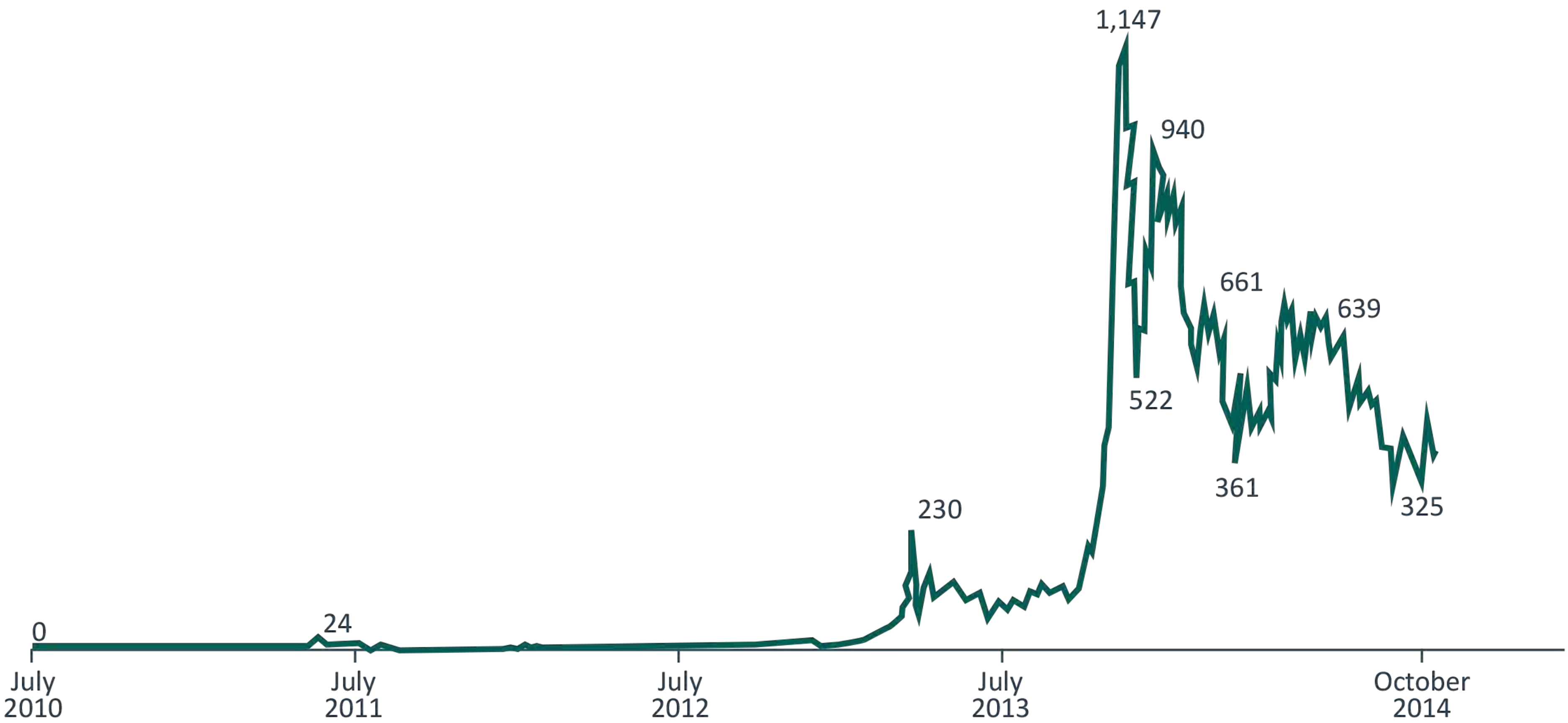
The Currency (bitcoin)

How many bitcoins have been mined?

15 554,575

Bitcoin Volatility

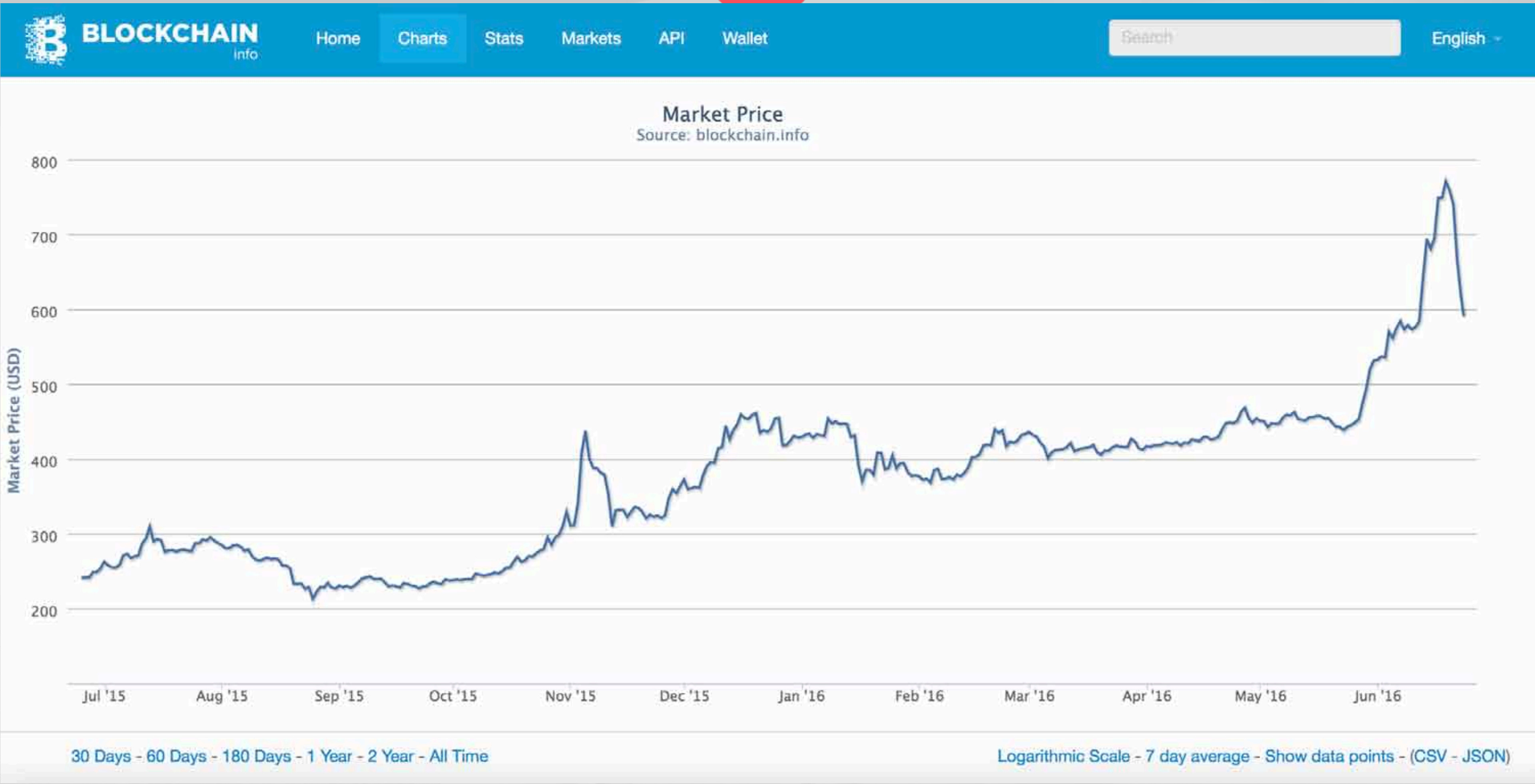
($, July 2010–October 2014)



Source: Bitcoin Price Chart, CoinDesk

BITCOIN ACADEMY

Market Price: Over 1 Year



Market Price
Source: blockchain.info

800
700
600
500
400
300
200
Market Price (USD)
Jul '15
Aug '15
Sep '15
Oct '15
Nov '15
Dec '15
Jan '16
Feb '16
Mar '16
Apr '16
May '16
Jun '16
30 Days - 60 Days - 180 Days - 1 Year - 2 Year - All Time
Logarithmic Scale - 7 day average - Show data points - (CSV - JSON)

BITCOIN ACADEMY

Market Price

On BitX exchange:

19 May 2016

- Price of 1 BTC = ZAR 7,556.00
- Volume of BTC traded in last 24 hours > about 102 BTC
- Over R770,000.00 traded in one day

On BitX exchange:

23 June 2016

- Price of 1 BTC = ZAR 9,546.00
- Volume of BTC traded in last 24 hours > about 401 BTC
- Over R3 million traded in one day

Types of Currencies

There are two main types of currencies:

1. **Commodity backed currencies -** convertible into a commodity such as gold

2. **Fiat currencies -** derives its value from government regulation or law

Bitcoin is Deflationary

A finite number of bitcoins available: 21 million

VERSUS

Inflation: occurs due to unrestrained printing of fiat currency by governments & central banks. This creates an increase in the money supply in a country.

How is the price of bitcoin determined?

Purely by supply and demand:

- Demand high = price high
- Demand low = price low
- Limited supply & demand high = price high
- Influenced by perception based on media reports and incidences and speculation of the price
- Small market capitalization of 21 million limits the supply & therefore increases the price

Acquiring bitcoin

1. Mining bitcoin
2. Buying bitcoin
3. Earning bitcoin

What is Mining?

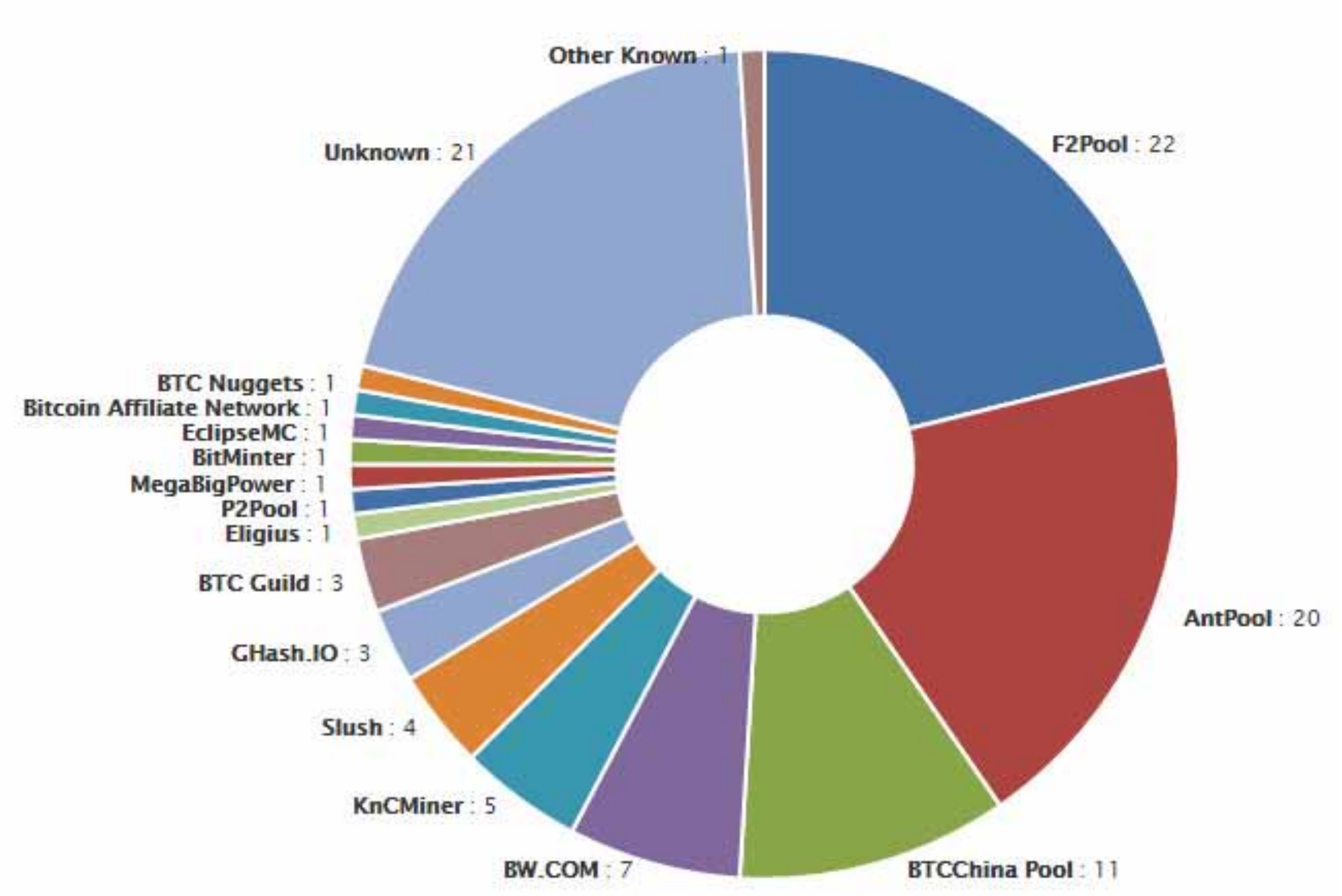
- Process where all bitcoin transactions are stored on the blockchain
- Miners use special computers and software to solve mathematical ***algorithms*** to validate each bitcoin transaction on the blockchain
- Fastest miner gets rewarded with bitcoin as an incentive
- **25 bitcoin** are released each time
- Miners keep network **secure**

Purpose of Mining?

1. Confirms all bitcoin transactions ever made
2. Creates new bitcoins

Mining Investment

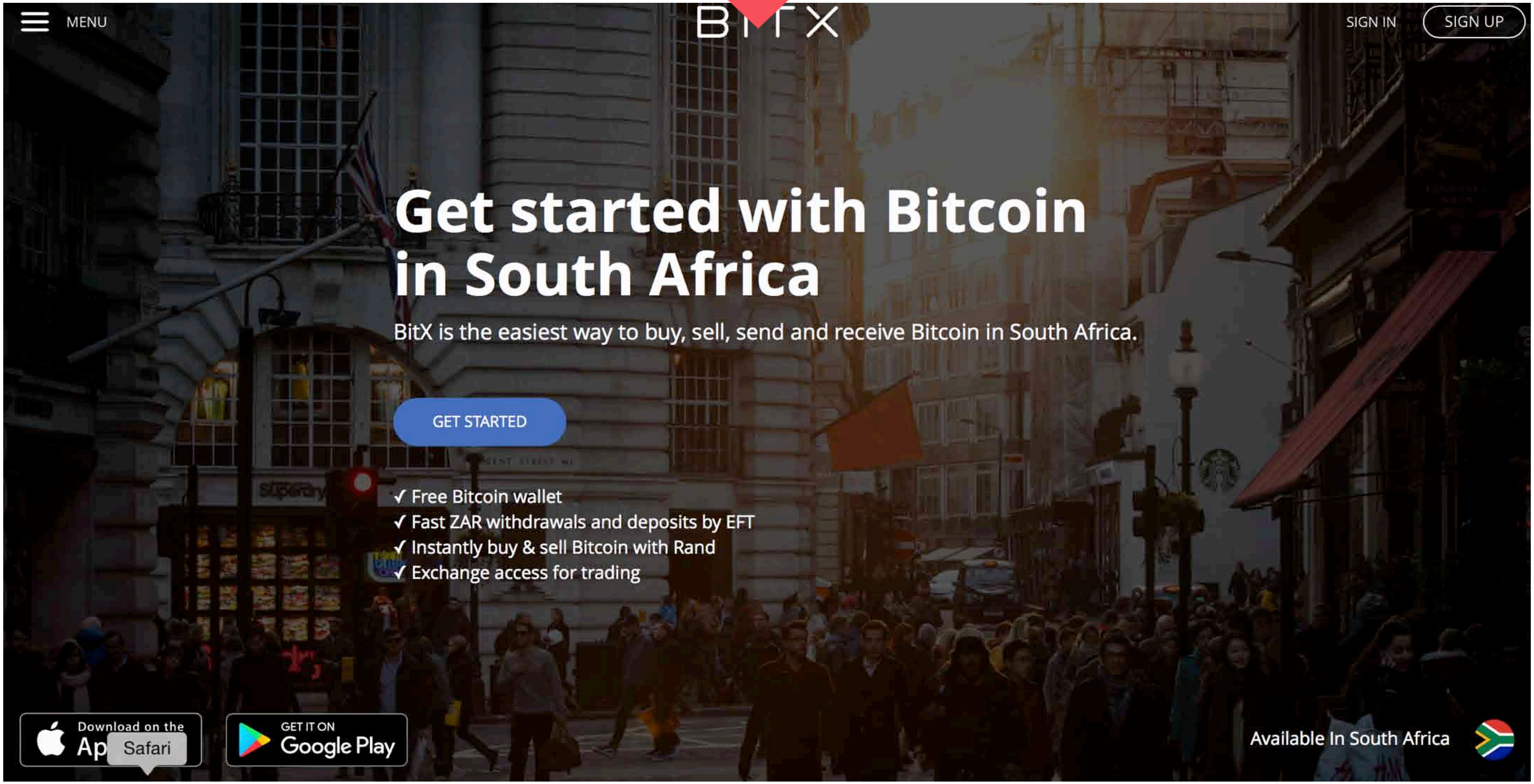
Mining Centralisation



How to buy bitcoin?

- Online Exchange: 3 in South Africa
  recommend BitX (www.bitx.co)
  AML & KYC Compliant: Upload ID & proof of address
- Operates like a traditional exchanges
- Market for buyers and sellers
- Buyer places bids: no. of bitcoin & price
- Sellers places no. of bitcoin & sets the ask price
- If both happy – exchange matches the order

BitX Website



Get started with Bitcoin in South Africa

BitX is the easiest way to buy, sell, send and receive Bitcoin in South Africa.

GET STARTED

✓ Free Bitcoin wallet
✓ Fast ZAR withdrawals and deposits by EFT
✓ Instantly buy & sell Bitcoin with Rand
✓ Exchange access for trading

BITCOIN ACADEMY

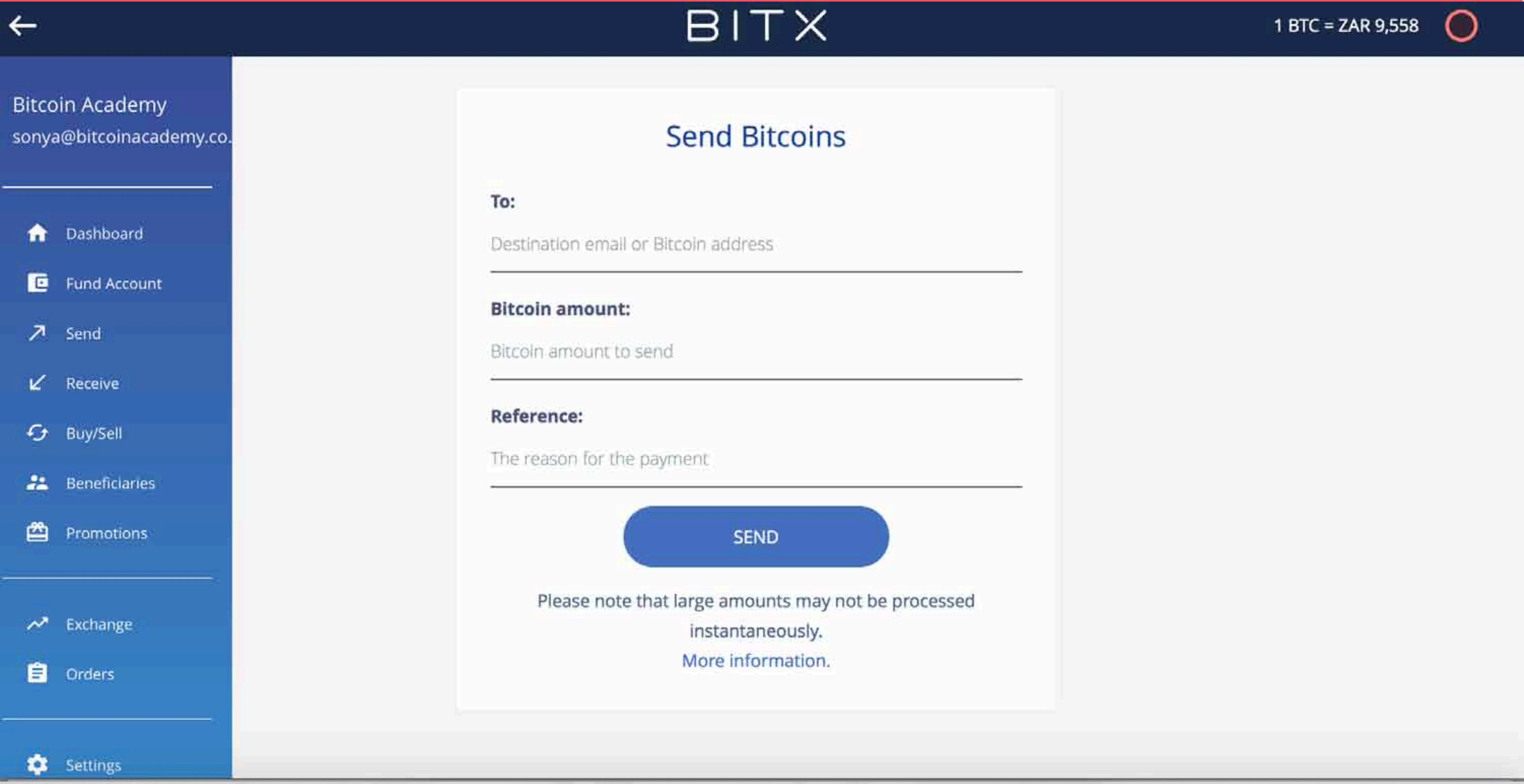
How to send bitcoin?

- Send to a bitcoin address: a string of letters and numbers of between 27 and 34 alphanumeric characters that represents a destination for a bitcoin payment.

  Example: 19JjM72bmgA39fED9YsLfg1SNrXTD

  Similar to sending an email.

How to send bitcoin?



BITX

1 BTC = ZAR 9,558

Bitcoin Academy
sonya@bitcoinacademy.co.

Send Bitcoins

To:

Destination email or Bitcoin address

Bitcoin amount:

Bitcoin amount to send

Reference:

The reason for the payment

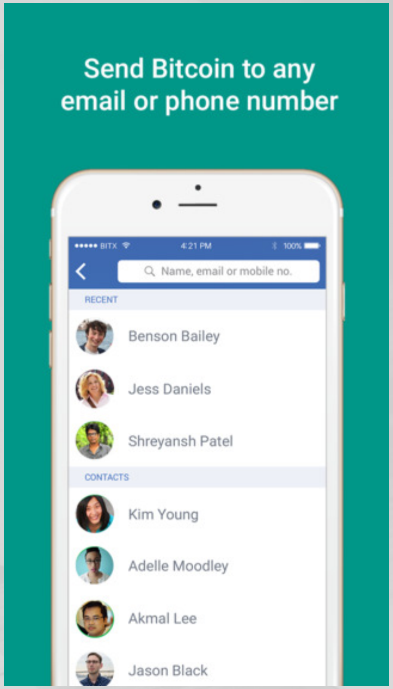
SEND

Please note that large amounts may not be processed instantaneously.
More information.

BITCOIN ACADEMY

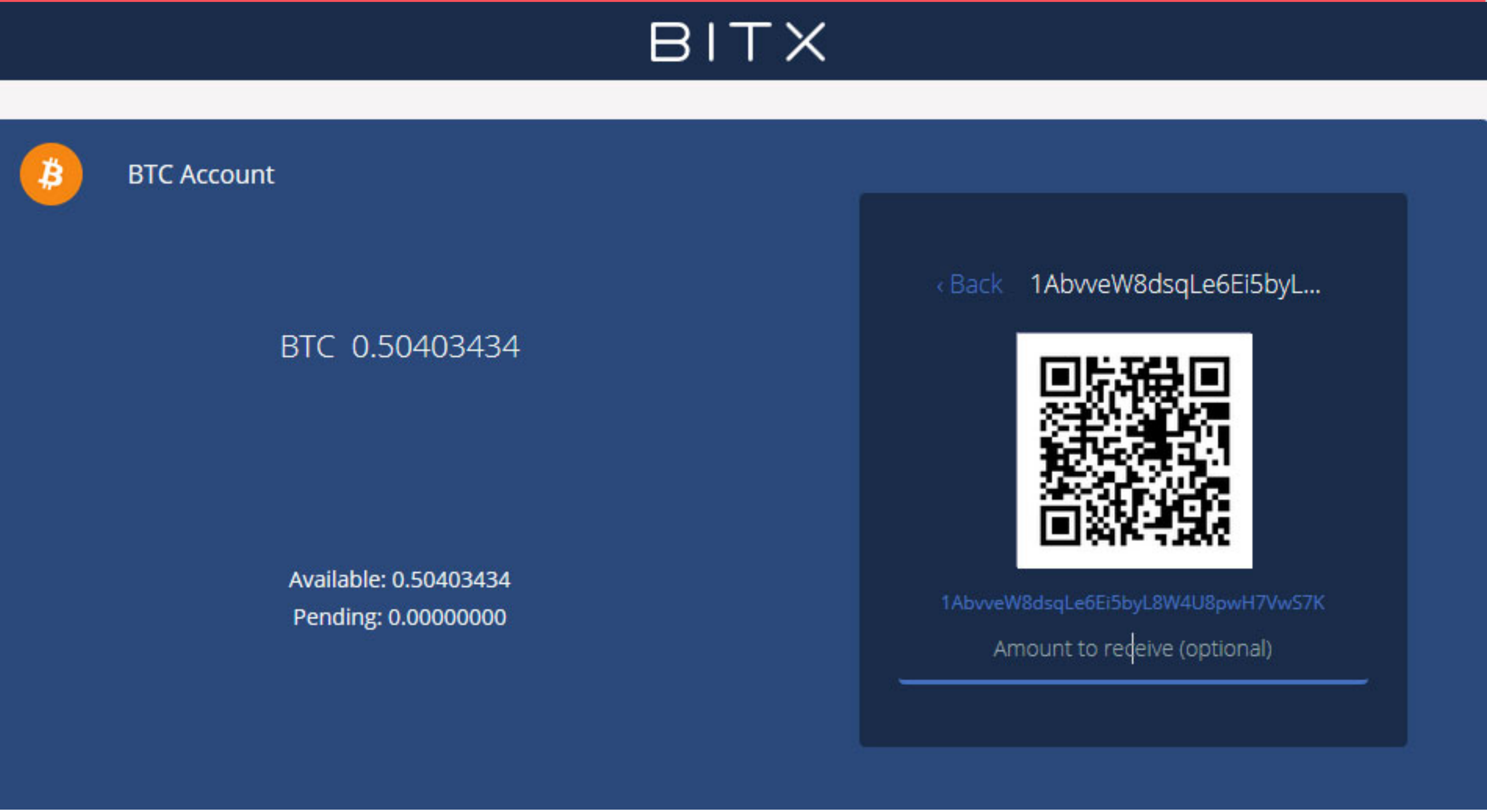
How to send bitcoin?

- Send to recipients email address
- Send to phone number (select from contacts)
- Scan a QR code



Send Bitcoin to any email or phone number

How to receive bitcoin?



BTC Account

BTC 0.50403434

Available: 0.50403434

Pending: 0.00000000

1AbvveW8dsqLe6Ei5byL...

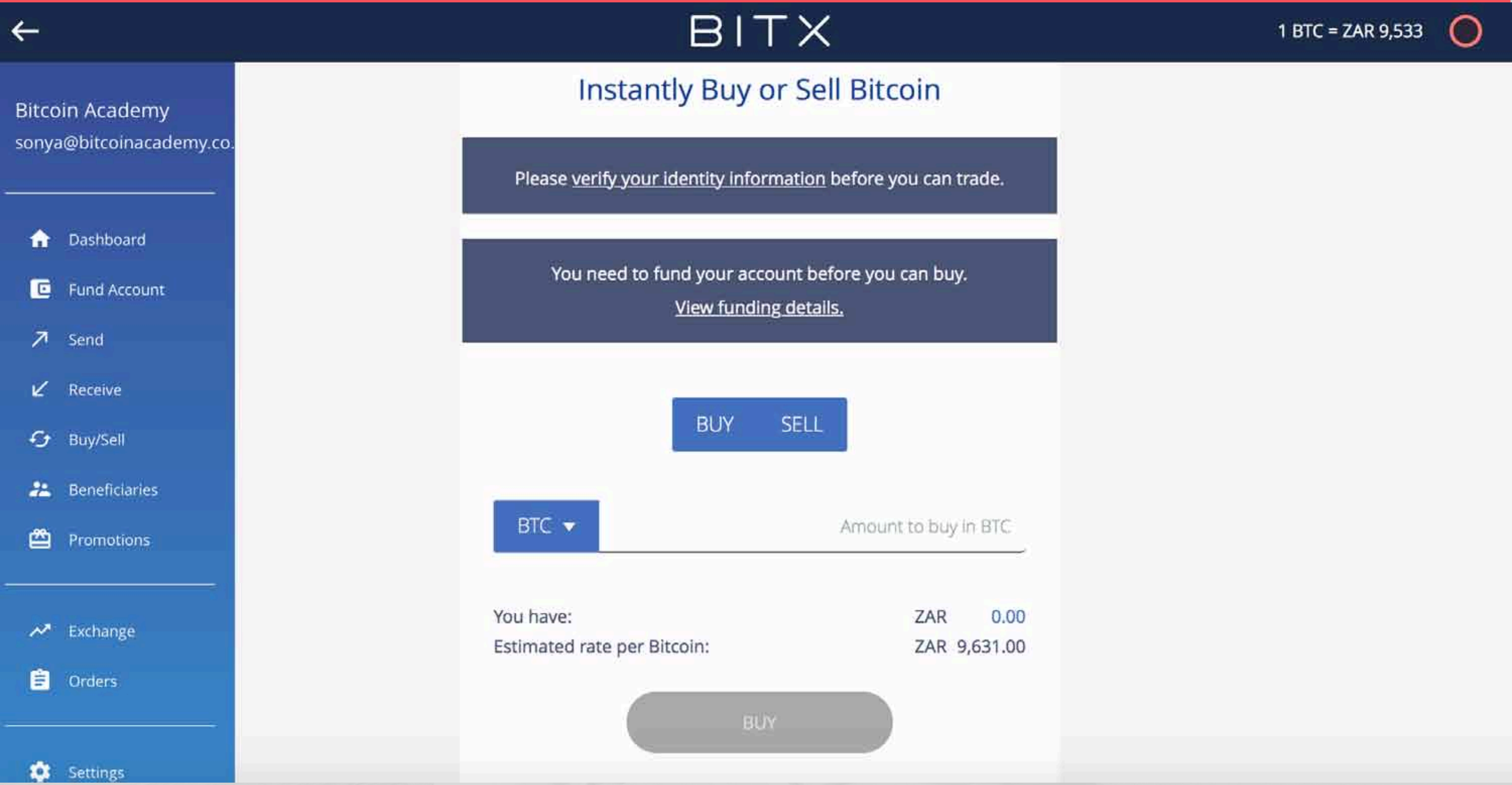
1AbvveW8dsqLe6Ei5byL8W4U8pwH7VwS7K

Amount to receive (optional)

How to receive bitcoin?

- Send bitcoin address to sender
- Send QR code to sender

How to buy & sell bitcoin?



Instantly Buy or Sell Bitcoin

Please verify your identity information before you can trade.

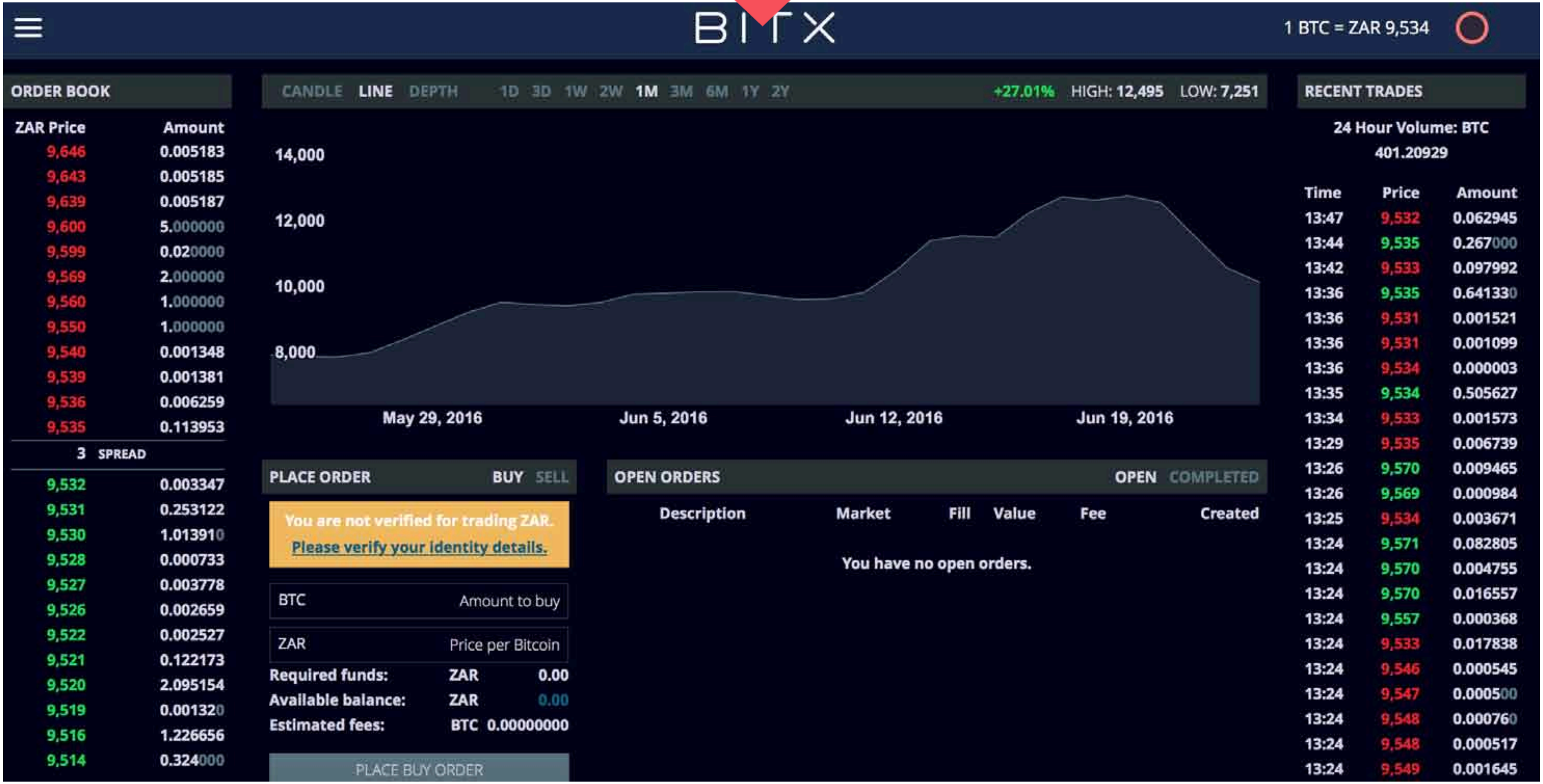
You need to fund your account before you can buy.
View funding details.

You have: ZAR 0.00

Estimated rate per Bitcoin: ZAR 9,631.00

BITCOIN ACADEMY

BitX Exchange



ORDER BOOK

ZAR Price	Amount
9,646	0.005183
9,643	0.005185
9,639	0.005187
9,600	5.000000
9,599	0.020000
9,569	2.000000
9,560	1.000000
9,550	1.000000
9,540	0.001348
9,539	0.001381
9,536	0.006259
9,535	0.113953
3 SPREAD	
9,532	0.003347
9,531	0.253122
9,530	1.013910
9,528	0.000733
9,527	0.003778
9,526	0.002659
9,522	0.002527
9,521	0.122173
9,520	2.095154
9,519	0.001320
9,516	1.226656
9,514	0.324000

+27.01% HIGH: 12,495 LOW: 7,251

PLACE ORDER

You are not verified for trading ZAR.
Please verify your identity details.

BTC Amount to buy

ZAR Price per Bitcoin

Required funds:	ZAR	0.00
Available balance:	ZAR	0.00
Estimated fees:	BTC	0.00000000

OPEN ORDERS

Description	Market	Fill	Value	Fee	Created

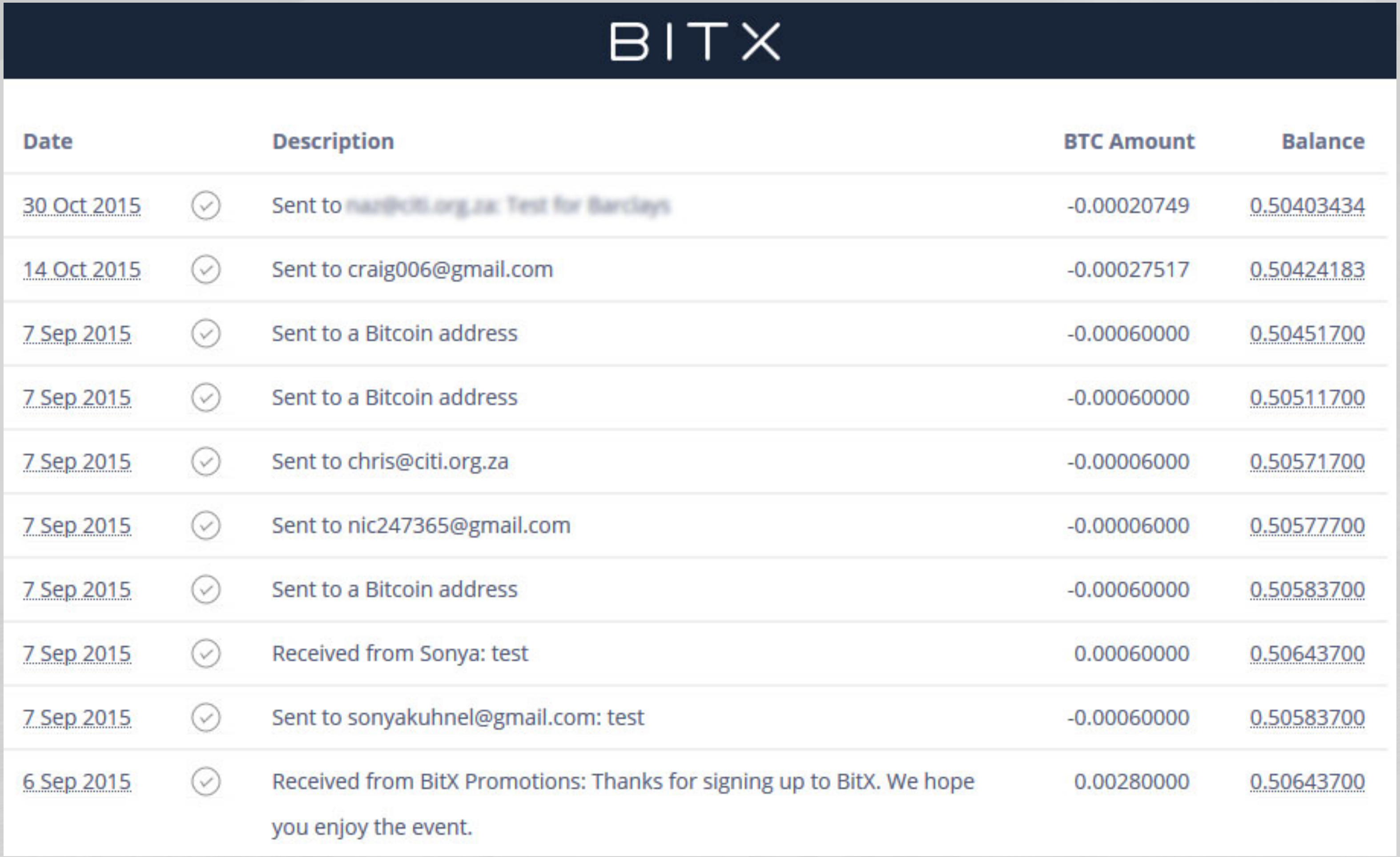
You have no open orders.

RECENT TRADES

24 Hour Volume: BTC 401.20929

Time	Price	Amount
13:47	9,532	0.062945
13:44	9,535	0.267000
13:42	9,533	0.097992
13:36	9,535	0.641330
13:36	9,531	0.001521
13:36	9,531	0.001099
13:36	9,534	0.000003
13:35	9,534	0.505627
13:34	9,533	0.001573
13:29	9,535	0.006739
13:26	9,570	0.009465
13:26	9,569	0.000984
13:25	9,534	0.003671
13:24	9,571	0.082805
13:24	9,570	0.004755
13:24	9,570	0.016557
13:24	9,557	0.000368
13:24	9,533	0.017838
13:24	9,546	0.000545
13:24	9,547	0.000500
13:24	9,548	0.000760
13:24	9,548	0.000517
13:24	9,549	0.001645

Bitcoin Transactions



BITX

Date		Description	BTC Amount	Balance
30 Oct 2015	✓	Sent to [redacted]	-0.00020749	0.50403434
14 Oct 2015	✓	Sent to craig006@gmail.com	-0.00027517	0.50424183
7 Sep 2015	✓	Sent to a Bitcoin address	-0.00060000	0.50451700
7 Sep 2015	✓	Sent to a Bitcoin address	-0.00060000	0.50511700
7 Sep 2015	✓	Sent to chris@citi.org.za	-0.00006000	0.50571700
7 Sep 2015	✓	Sent to nic247365@gmail.com	-0.00006000	0.50577700
7 Sep 2015	✓	Sent to a Bitcoin address	-0.00060000	0.50583700
7 Sep 2015	✓	Received from Sonya: test	0.00060000	0.50643700
7 Sep 2015	✓	Sent to sonyakuhnel@gmail.com: test	-0.00060000	0.50583700
6 Sep 2015	✓	Received from BitX Promotions: Thanks for signing up to BitX. We hope you enjoy the event.	0.00280000	0.50643700

Wallets

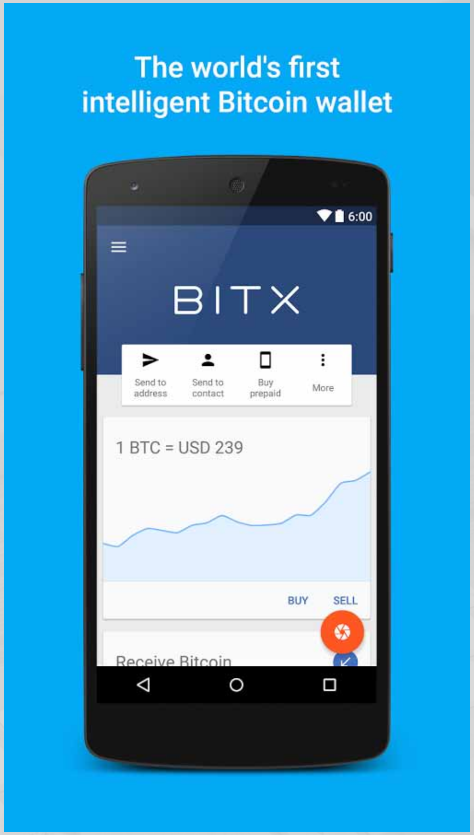
- Bitcoin wallets store the **public & private keys** (similar to a bank account and your pin)
- The public key is used to send someone bitcoin
- The private key needs to be kept a secret
- Bitcoin wallets don't hold actual bitcoin

Types of Wallets

1. **Software wallets:** installed on your computer
2. **Web or online wallets:** installed on mobile devices and web sites.
   Advantage = convenient
   Disadvantage = trust a third party, such as BitX

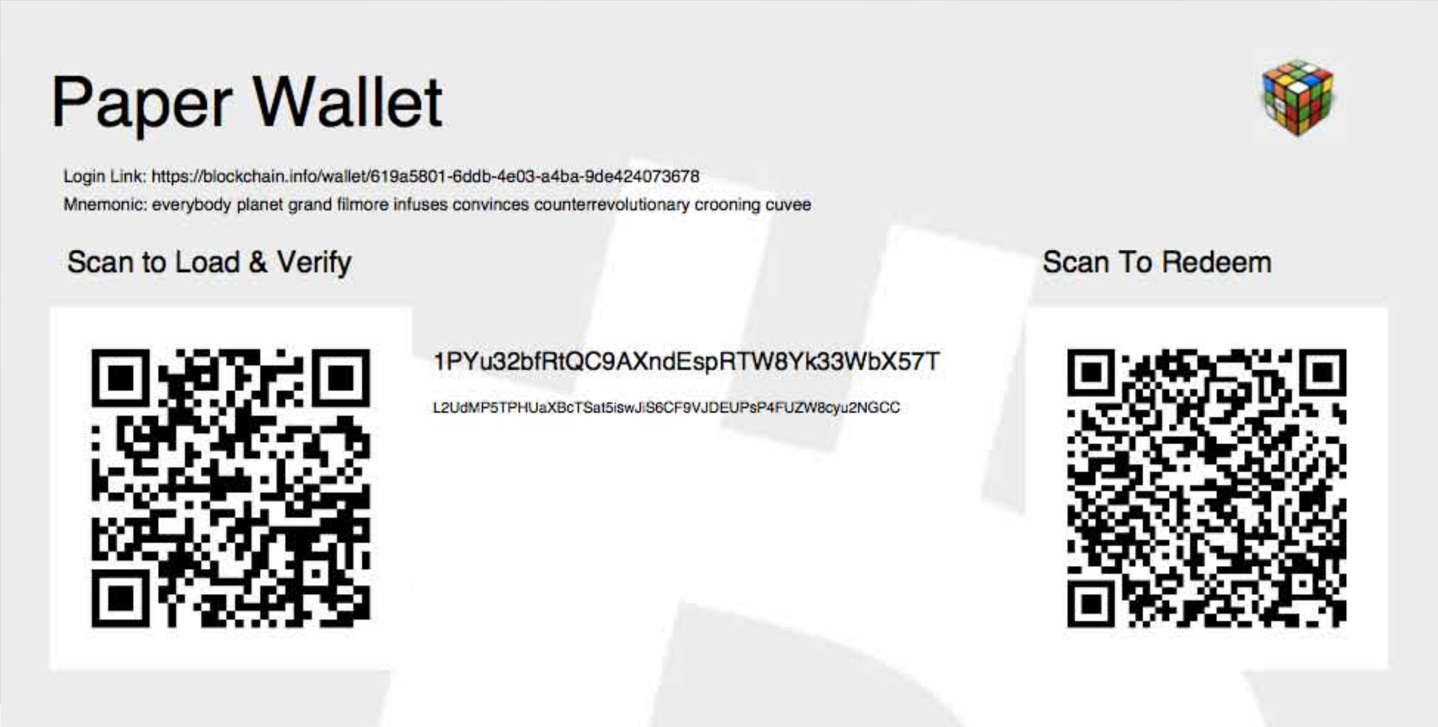
BitX Mobile Wallet (web wallet)

Bitcoin Smart Wallet: available for Android & iOS


The world's first intelligent Bitcoin wallet

Types of Wallets

3. **Paper wallets:** public and private keys are printed on a piece of paper



Paper Wallet

Login Link: https://blockchain.info/wallet/619a5801-6ddb-4e03-a4ba-9de424073678

Mnemonic: everybody planet grand filmore infuses convinces counterrevolutionary crooning cuvee

Scan to Load & Verify

1PYu32bfRtQC9AXndEspRTW8Yk33WbX57T

L2UdMP5TPHUaXBcTSat5iswJiS6CF9VJDEUPsP4FUZW8cyu2NGCC

Scan To Redeem

Paper Wallet

Types of Wallets

4. **Hardware wallets:** a physical device

Types of Wallets

5. **Brain wallets:** user commits a pass phrase to memory.
   Advantage = very secure

Wallet Safety

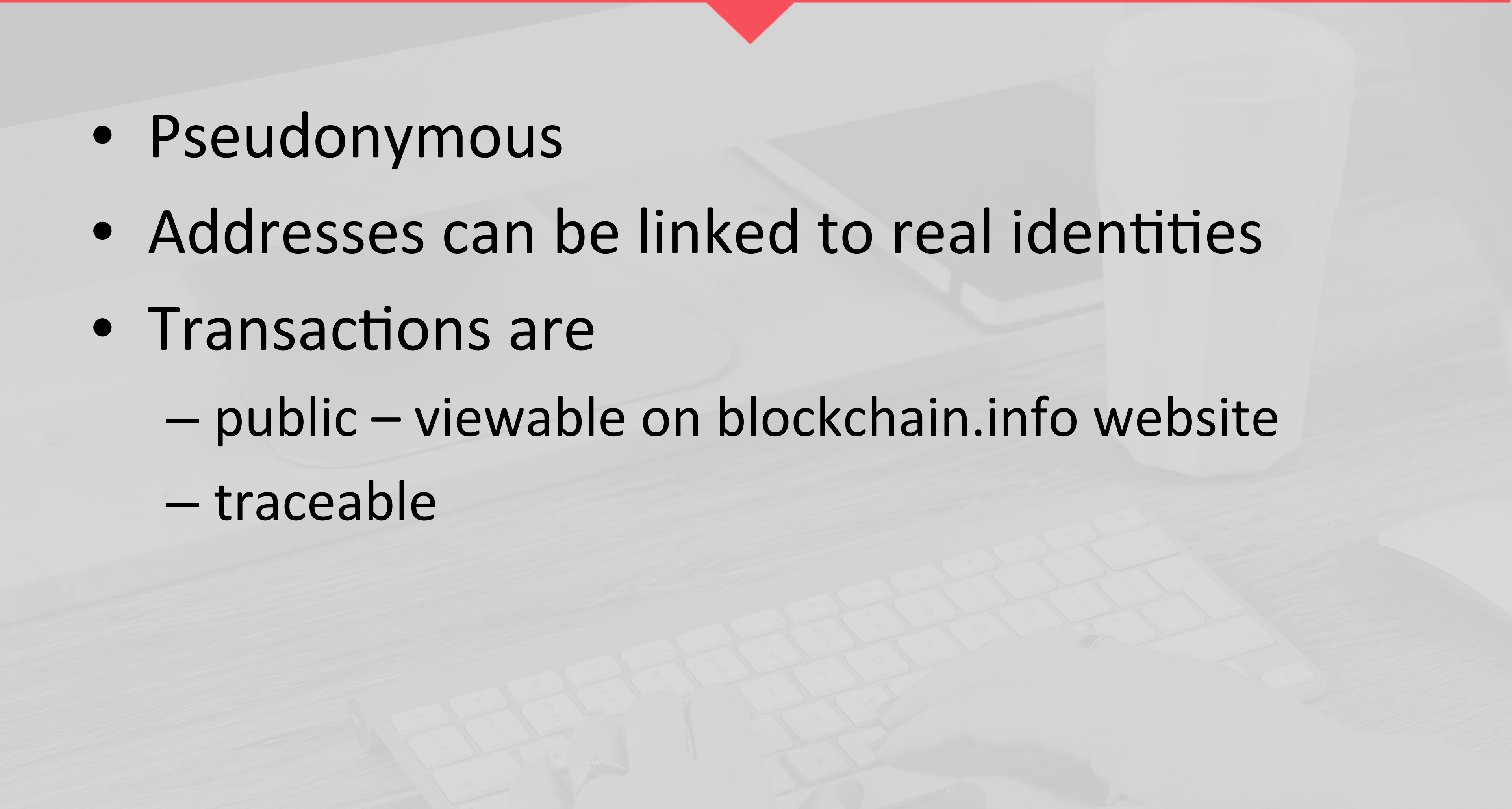
- **Wallet backups:**

  - Encrypt
  - Multiple locations
  - Regular backups of private keys

- **Cold storage:** completely offline: storing keys to a device not connected to the internet

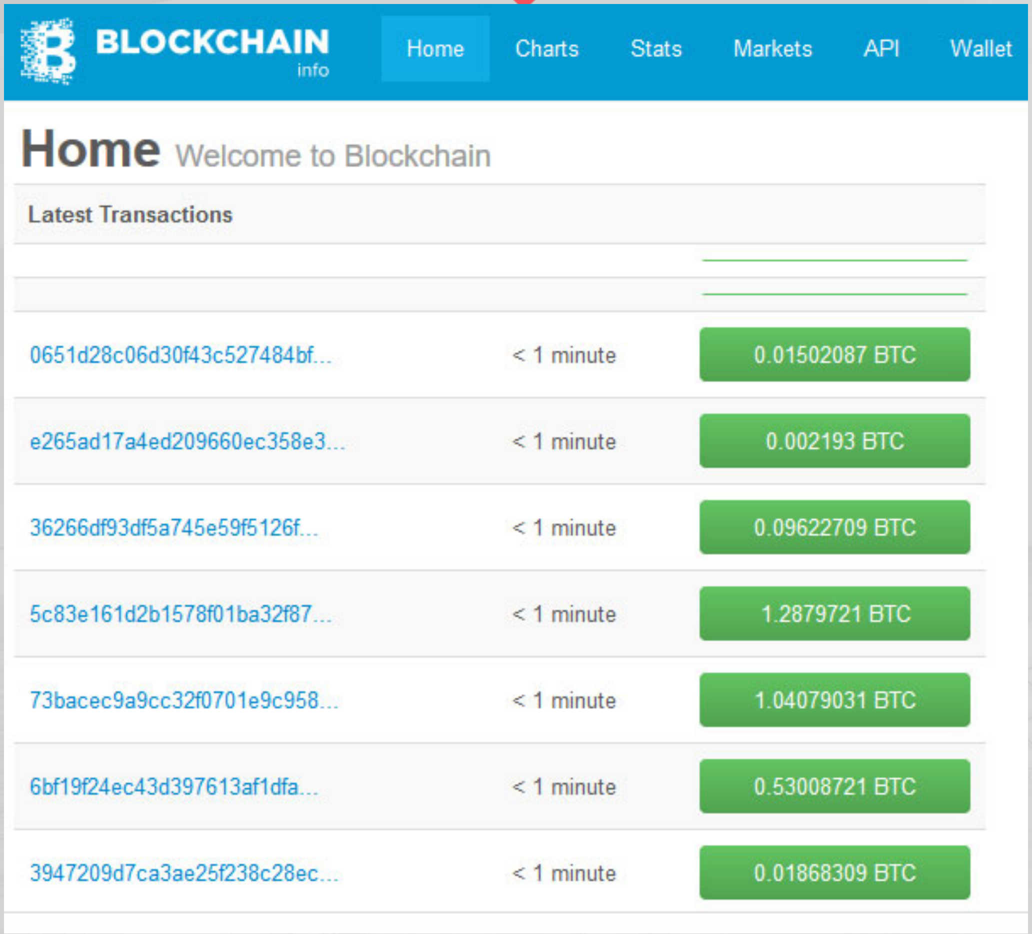
- **Multi-signature transactions:** the owner can specify rules which require a certain number of private keys to sign the transaction

How anonymous is Bitcoin?



- Pseudonymous
- Addresses can be linked to real identities
- Transactions are
  - public – viewable on blockchain.info website
  - traceable

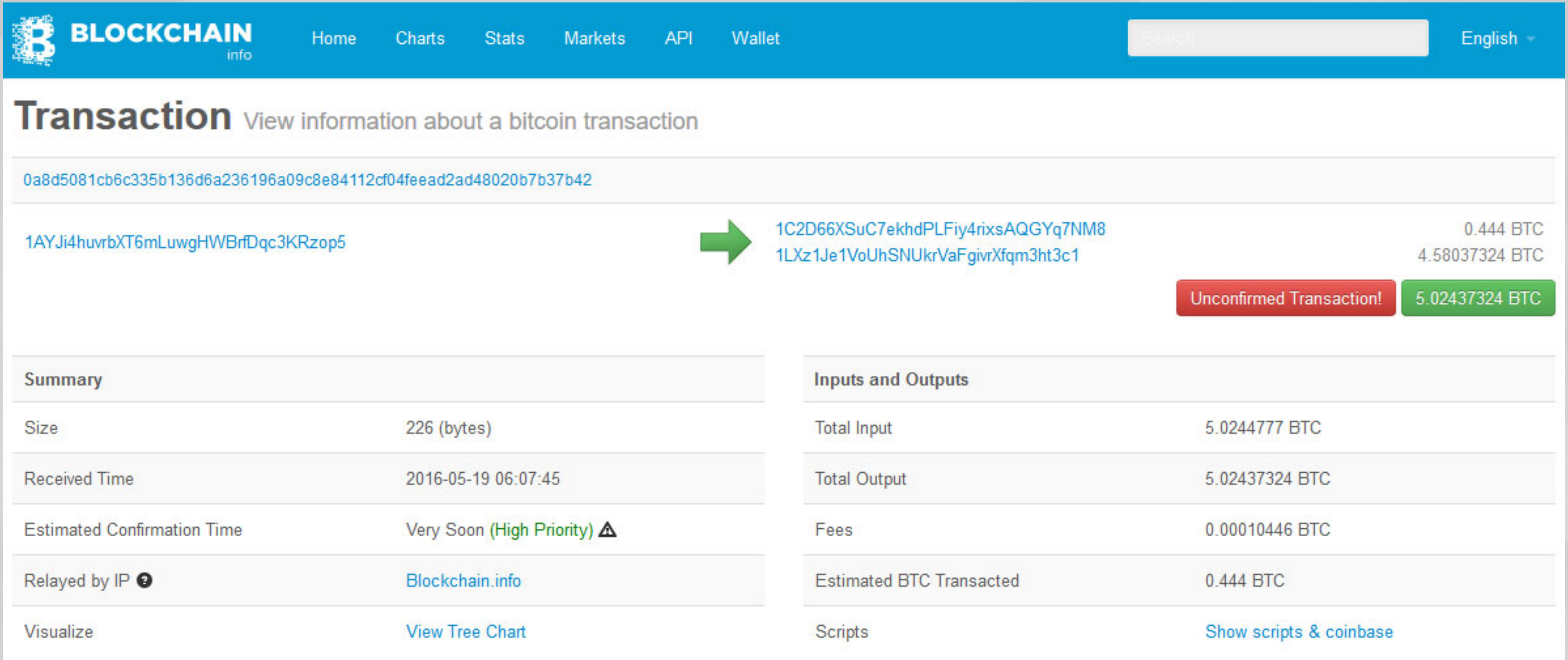
How anonymous is Bitcoin?



Home Welcome to Blockchain

Latest Transactions		
0651d28c06d30f43c527484bf...	< 1 minute	0.01502087 BTC
e265ad17a4ed209660ec358e3...	< 1 minute	0.002193 BTC
36266df93df5a745e59f5126f...	< 1 minute	0.09622709 BTC
5c83e161d2b1578f01ba32f87...	< 1 minute	1.2879721 BTC
73bacec9a9cc32f0701e9c958...	< 1 minute	1.04079031 BTC
6bf19f24ec43d397613af1dfa...	< 1 minute	0.53008721 BTC
3947209d7ca3ae25f238c28ec...	< 1 minute	0.01868309 BTC

How anonymous is Bitcoin?



Transaction View information about a bitcoin transaction

0a8d5081cb6c335b136d6a236196a09c8e84112cf04feead2ad48020b7b37b42

1AYJi4huvrbXT6mLuwgHWBrfDqc3KRzop5 →

1C2D66XSuC7ekhdPLFiy4rixsAQGYq7NM8 0.444 BTC
1LXz1Je1VoUhSNUkrVaFgivrXfqm3ht3c1 4.58037324 BTC

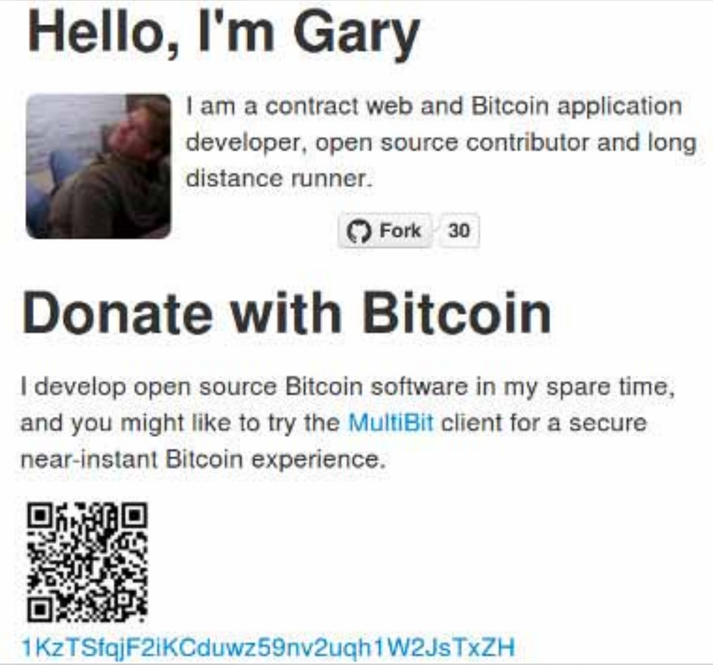
Unconfirmed Transaction! 5.02437324 BTC

Summary	
Size	226 (bytes)
Received Time	2016-05-19 06:07:45
Estimated Confirmation Time	Very Soon (High Priority) ⚠
Relayed by IP ❓	Blockchain.info
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	5.0244777 BTC
Total Output	5.02437324 BTC
Fees	0.00010446 BTC
Estimated BTC Transacted	0.444 BTC
Scripts	Show scripts & coinbase

How anonymous is Bitcoin?

- Publishing your name and bitcoin address online
- Who knows your address: anyone on the internet



Hello, I'm Gary

I am a contract web and Bitcoin application developer, open source contributor and long distance runner.

Donate with Bitcoin

I develop open source Bitcoin software in my spare time, and you might like to try the MultiBit client for a secure near-instant Bitcoin experience.

1KzTSfqjF2iKCduwz59nv2uqh1W2JsTxZH

How anonymous is Bitcoin?

- Trading bitcoin for national currency on an exchange
- Who knows your address: the exchange

BITX

How anonymous is Bitcoin?

- Buying goods and services online
- Who knows your address:
  the merchant / payment processor

PayFast

bitpay

How anonymous is Bitcoin?

- Using a Thin Client or Hosted Wallet
- Who knows your address:
  server administrators

BITX

Bitcoin has an image problem

Silk Road
anonymous marketplace

Silk Road was an online black market best known as a platform for selling illegal drugs.

MT.GOX

Mt. Gox was one of the largest bitcoin exchanges based in Tokyo, Japan.
Claimed to have lost 650,000 bitcoins
Closed in 2014 and filed for bankruptcy
Many people lost their bitcoin.

The Blockchain

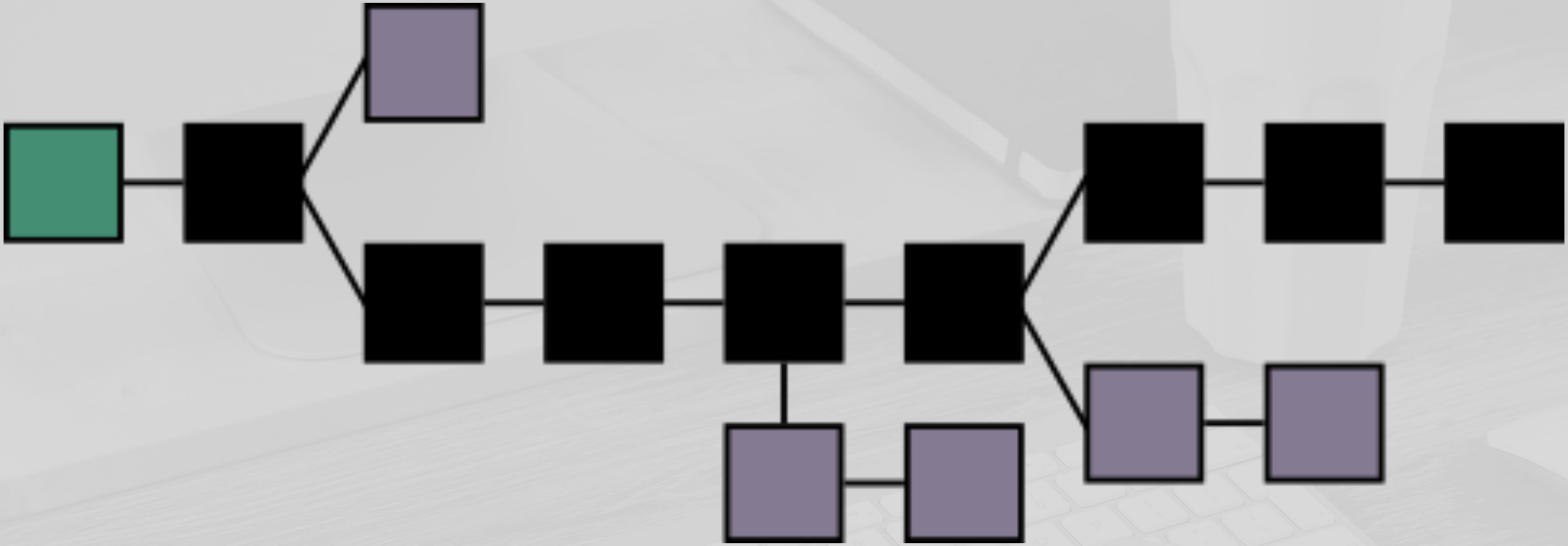
- Distributed, decentralised public ledger
- Available to anyone, anywhere in the world
- Stores all past bitcoin transactions
- Write-only: data can only be added, not edited or deleted
- Technology that underpins bitcoin

The Genesis Block

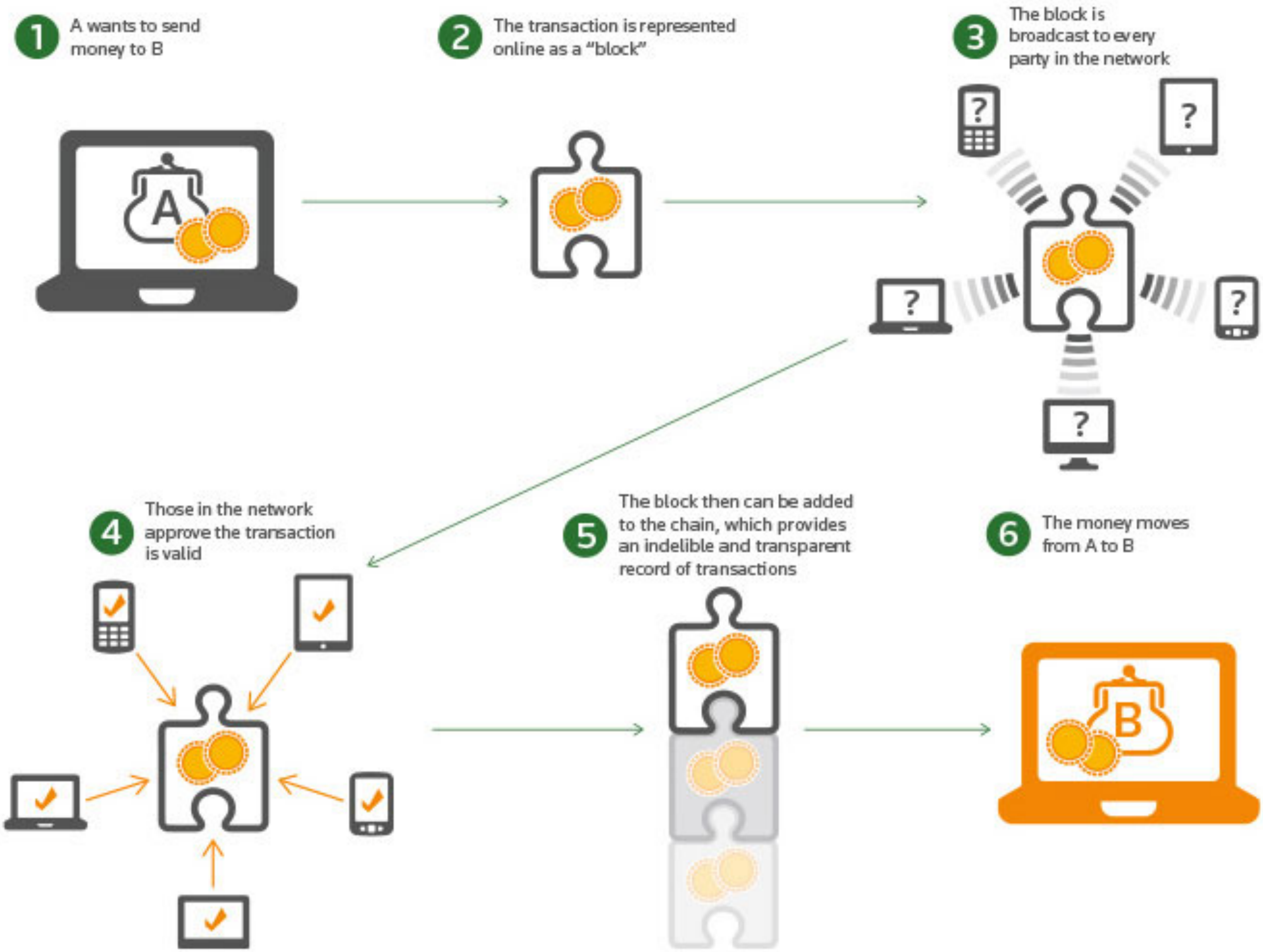
3 January 2009:

The Genesis Block is mined

The Blocks



How the Blockchain works



1 A wants to send money to B

2 The transaction is represented online as a "block"

3 The block is broadcast to every party in the network

4 Those in the network approve the transaction is valid

5 The block then can be added to the chain, which provides an indelible and transparent record of transactions

6 The money moves from A to B

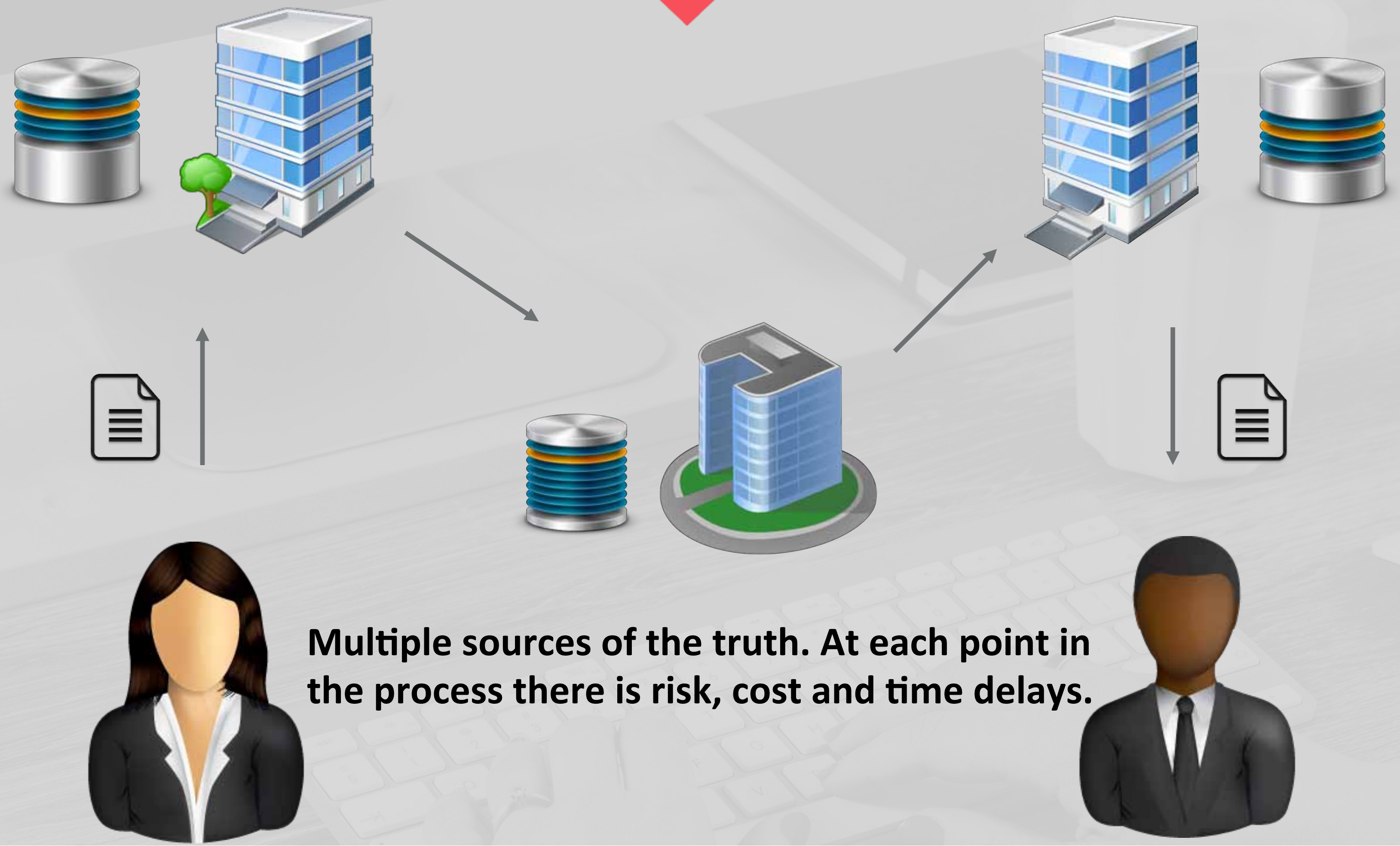
Trustless Payment System

“The one thing that’s missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A.”

– Milton Friedman, early 2000’s (Nobel winning economist)

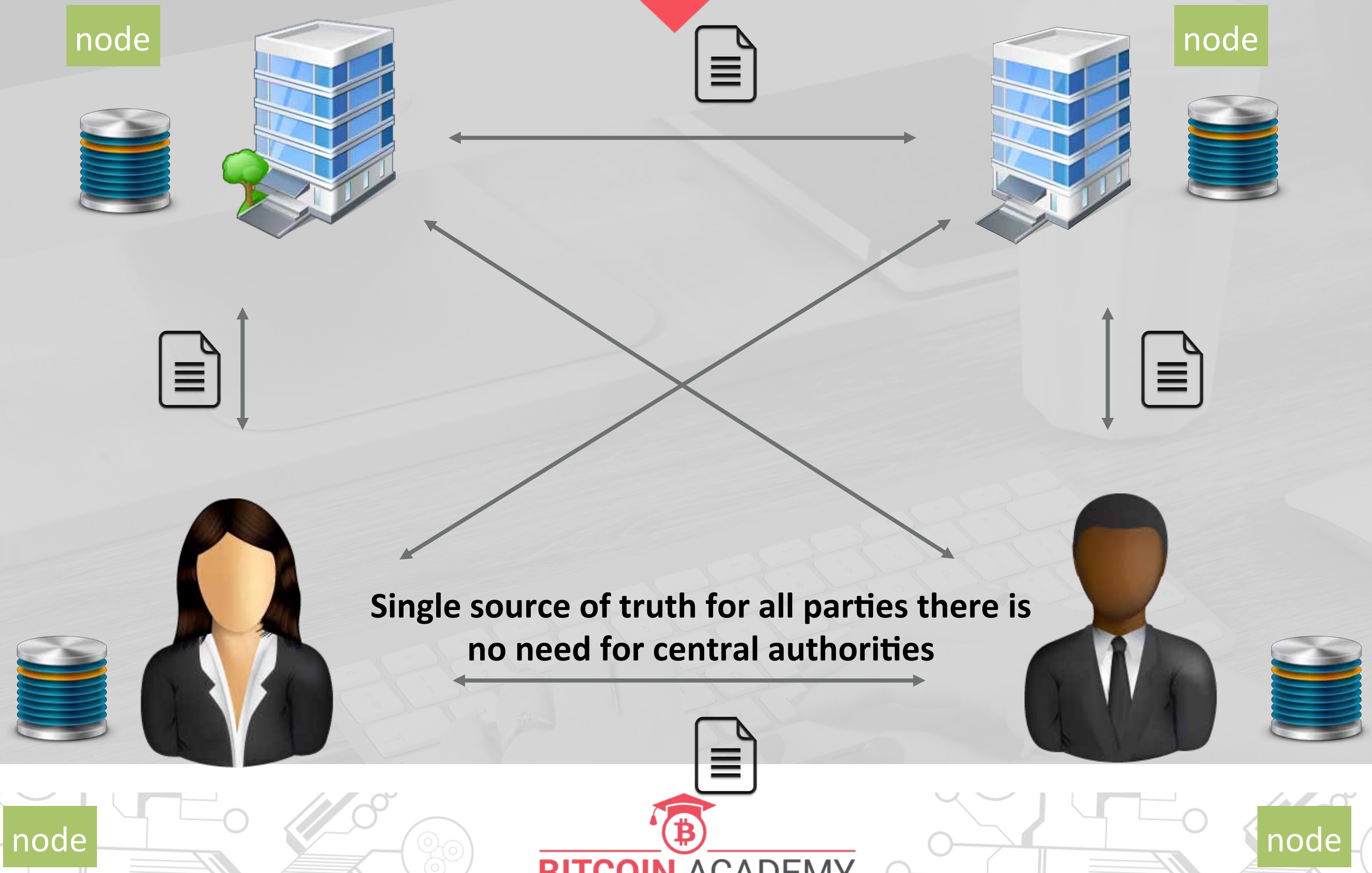
Transfer of money: traditional method

Transfer of money: traditional method



Multiple sources of the truth. At each point in the process there is risk, cost and time delays.

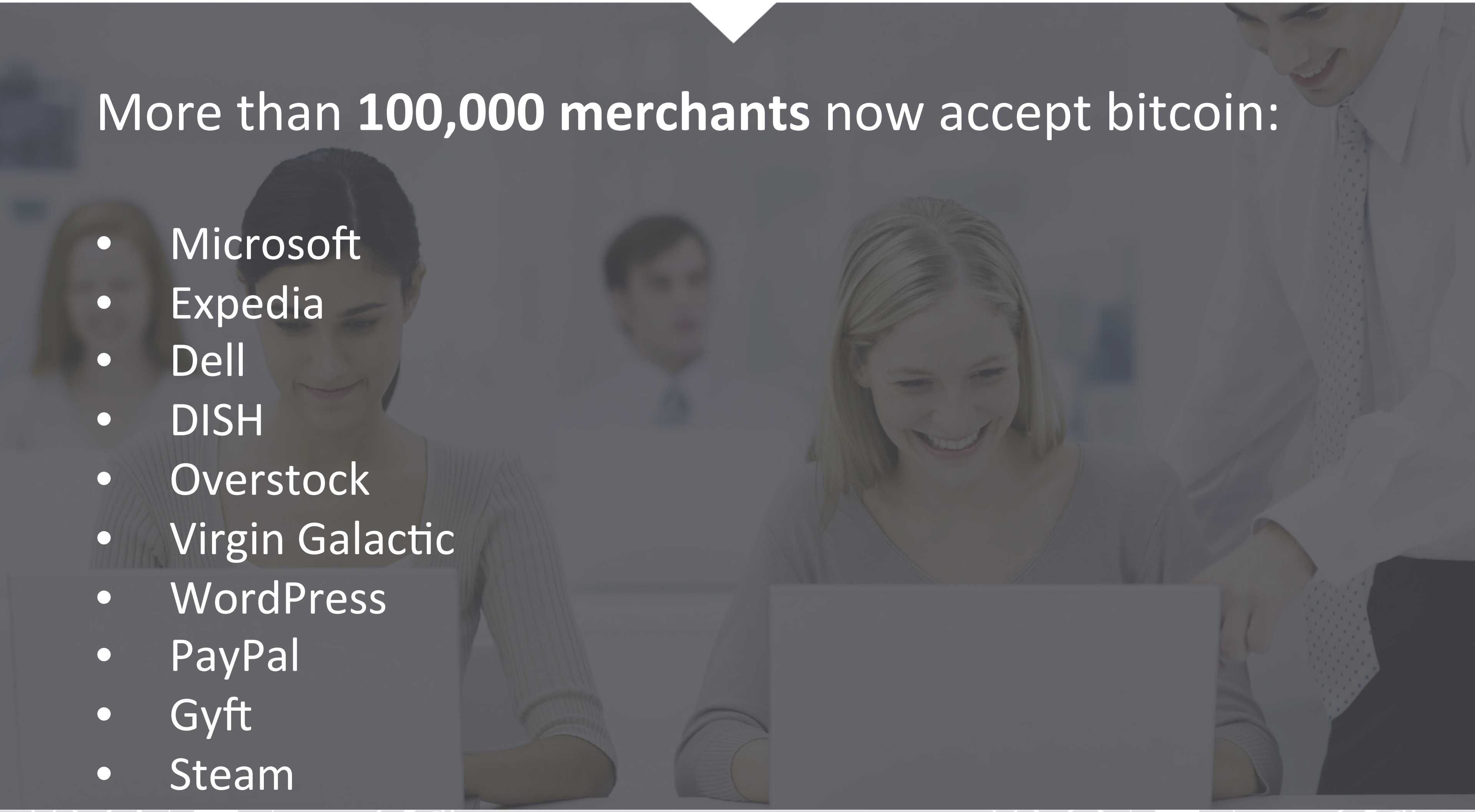
Transfer of bitcoin



Single source of truth for all parties there is no need for central authorities

BITCOIN ACADEMY

Merchant Acceptance



More than **100,000 merchants** now accept bitcoin:

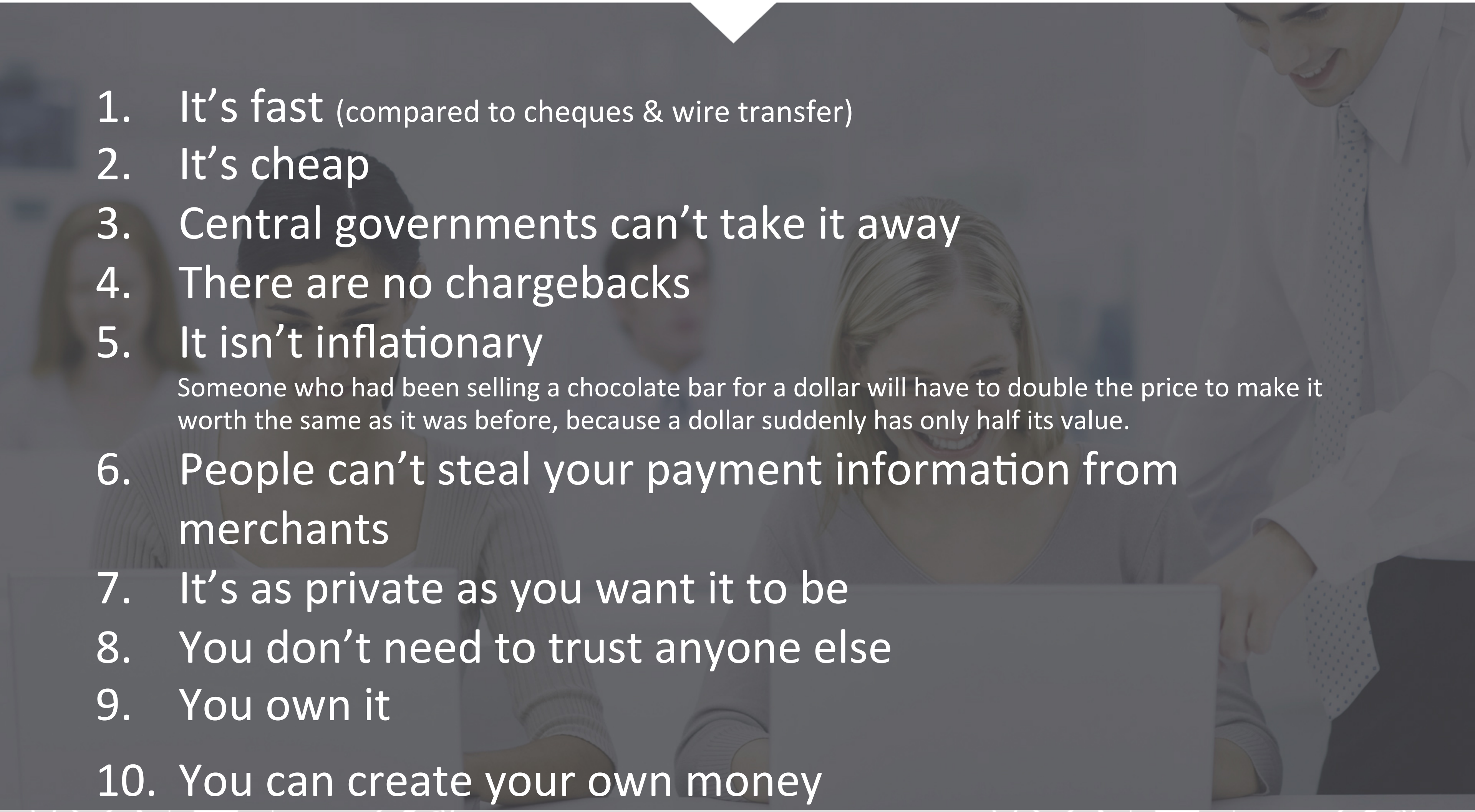
- Microsoft
- Expedia
- Dell
- DISH
- Overstock
- Virgin Galactic
- WordPress
- PayPal
- Gyft
- Steam

Merchant Acceptance

- Payment integration – 3rd Party Bitcoin payment processors such as BitPay
  They convert bitcoin into fiat so no volatility
- Benefits:
  - transaction fees lower (no intermediary)
  - no need for a bank account
  - no risk of chargebacks for merchants (can not be reversed)
  - payment information can not be stolen
- Payment processing companies eg. PayFast & BitPay
- Transaction verification / confirmations:

  1 confirmation for small vendors, up to 6

Why use Bitcoin?



1. It’s fast (compared to cheques & wire transfer)
2. It’s cheap
3. Central governments can’t take it away
4. There are no chargebacks
5. It isn’t inflationary
   Someone who had been selling a chocolate bar for a dollar will have to double the price to make it worth the same as it was before, because a dollar suddenly has only half its value.
6. People can’t steal your payment information from merchants
7. It’s as private as you want it to be
8. You don’t need to trust anyone else
9. You own it
10. You can create your own money

Compliance, regulation & tax

- **Regulation in South Africa:**
  No regulation
  Regulators have issued a warning only

- **Regulation world-wide:**
  Most governments around the world are applying existing regulatory frameworks for electronic and mobile payment systems
  Currently no countries where bitcoin is accepted as legal tender

Compliance and regulation

- **Countries that have banned bitcoin:**
  1. Bangladesh
  2. Bolivia
  3. Ecuador

Legality of bitcoin by country:
https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country

Why are people talking about it?

- Disrupting traditional ways of transacting and storing of information
- Almost US$1billion investment in bitcoin and blockchain technology startups since 2012
- In 2015 it was the worlds best performing currency
- Decentralised nature of this technology is out of the control of the regulators

The Economist
OCTOBER 31ST–NOVEMBER 6TH 2015
Economist.com
007 and the spectre of Britain's past
Turkey votes to the sound of bombs
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
The trust machine
How the technology behind bitcoin could change the world
IN BLOCKCHAIN WE TRUST

Financial Institutions researching or developing POC's

Goldman Sachs

BNP PARIBAS

SOCIETE GENERALE

J.P.Morgan

BARCLAYS

BANK OF ENGLAND

HSBC

RBS
The Royal Bank of Scotland

Santander

CREDIT SUISSE

COMMERZBANK

Bank of America

Nasdaq

citi

Morgan Stanley

VISA

Why are people talking about it?

- Payment rails: cross border payments & interbank settlements
- Remittances
- Immutable ledger
- Time-stamped records
- Proof of ownership
- Micro-transactions: 0.00005430 BTC = 0.26 Rands
- Smart contracts

Why are people talking about it?

Ripple:

- Enabling a real-time gross settlement system for cross-currency payments between banks
- Remittance service for retail customers
- International transaction banking service
- International corpoate payments
- Cross-border intra- bank currency transfers

Why are people talking about it?

Barclays:

- Helping business clients reduce costs associated with supply chain management
- Replacing printed documents with versions that are stored electronically in blockchain transaction metadata

Why are people talking about it?

NASDAQ:

- Using blockchain to streamline financial record keeping
- Trading of shares of pre-IPO private companies

IBM:

A platform that operates without a native currency like bitcoin and can be used to keep track of business to business, bank to bank, and bank to business transactions and enforce smart contracts

Why are people talking about it?

Deutsche Bank:

- Issuing corporate bonds and coupon payments, redeeming itself by means of a "smart contract" that automatically executes the terms
- Enforcement and clearing of derivatives contracts
- Know-your-customer and anti-money laundering registries and surveillance
- Securities asset servicing

Why are people talking about it?

Smart Contracts:

- Car rental agencies using smart contracts that automatically allow rentals when payment’s received and insurance information is confirmed through a blockchain record

- A refrigerator equipped with sensors and connected to the internet using the blockchain to manage automated interactions with the external world—anything from ordering and paying for food to arranging for its own software upgrades and tracking its warranty

Why are people talking about it?

Insurance:

- Transparent company ledger for real-time auditing by regulators and client confidence
- Gives the regulator the confidence to reduce the initial capitalisation requirement of an insurance program
- Enables the ensured individuals to see that premiums are being collected appropriately and that there are sufficient funds for claim payments in the event of a loss

BITCOIN ACADEMY

BLOCKCHAIN AND BITCOIN TRAINING FOR INDIVIDUALS,
INSTITUTIONS AND COMPANIES

Sonya Kuhnel
Managing Director

Address:
The Bandwidth Barn, Block B, 3rd Floor, Woodstock Exchange,
66-68 Albert Road, Woodstock, Cape Town, 7925

Tel: +27 (21) 409 1376
Email: sonya@bitcoinacademy.co.za