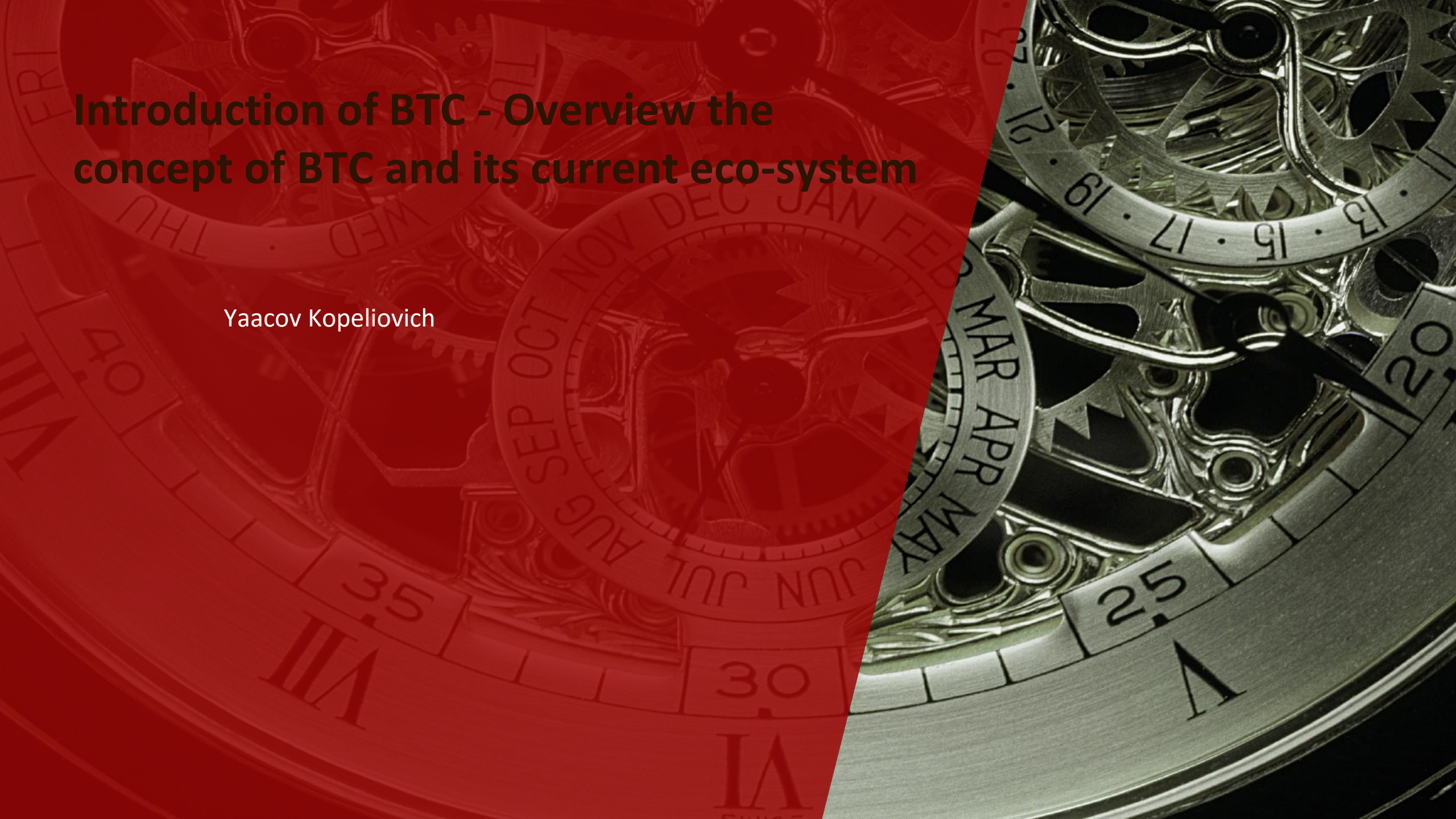


# Introduction of BTC - Overview the concept of BTC and its current eco-system

Yaacov Kopeliovich



# 1. Overview



- BTC Algorithm and its applications to finance
- BTC Mining – PoW
- BTC Exchanges
- BTC Wallets
- BTC Price Performance
- BTC forks and concept of free money
- BTC Extensions – Ethereum and Ripple

## 2. Disclaimer

---



What I am not going to do in this talk is to express my opinions about crypto-assets. I am not going to recommend investing in BTC and other Crypto-Assets. Invest in your own peril if you have decided to do it.

### 3. Overview



## Why do we need Financial Institutions?

- We trust the Centralized Hubs like Banks and Investment Companies to Perform the following main functions:
- Keep an orderly ledger of our debits and credits (Ordering Financial Transactions)
- Prevent malicious states where one person can send multiple checks to many accounts without having funds to cover them in his own account.



# 1. Overview

---



## **Trust without a middle man – make all transactions public**

- Until the financial crisis it was an accepted truth that trust couldn't function peer to peer and we need a centralized hub.
- In January 2009 a whitepaper appeared that revolutionized this field as we know it
- The anonymous author made the clever observation that trust will not be needed if EVERYBODY would participate in one giant public ledger.

# 1. Overview

---



## Verifying Identity Online – Digital Signatures

- How do we verify somebody's identity online?
- Suppose I like to track whether Assaf entered his office.
- I can track his computer office remotely and every time he comes I record his logging in and out from his office computer
- I don't know Assaf's password to know that he is in his office.

# 1. Overview

---



## Verifying Identity Online – Digital Signatures

- The idea of digital verification is very close to Assaf's example.
- To accomplish that we generate a pair of strings ( called keys)
- One string we publish for everybody to see
- One is Kept Private

# 1. Overview

---

*Overview*

→ *Advantage*

→ *Size of  
market*

→ *Correlation*

→ *Comparison*

→ *future*

→ *Regulation*

## Verifying Identity Online – Digital Signatures

To send payment to somebody we perform the following actions:

- Find the public key address of the person we like to send BTC too
- Use our private key to encrypt the message : We are sending so many BTCs to this public key.
- Anybody with our public key can decrypt our message and verify that we sent the transaction.



# 1. Overview

---



## Public Key Cryptography – Trapdoor functions

- Is it black magic? – How can you decrypt the message without knowing private keys?
- Think about squaring and extracting square roots. One is easy and one is harder.
- Yet if somebody gives you a square root you can verify the solution easily

# 1. Overview

---



## Public Key Cryptography – Trapdoor functions

- This is exactly the idea behind this private and public key.
- You use public key generated in the pair to verify the solution to the puzzle produced by private keys.
- And the puzzle is so hard that only the private key owner could produce a solution to it!

# 1. Overview

---



## Ledger Management

- So far we discussed the method to send payments. But who is managing the ledger?
- This is Satoshi's clever innovation and where the blockchain concept comes from.

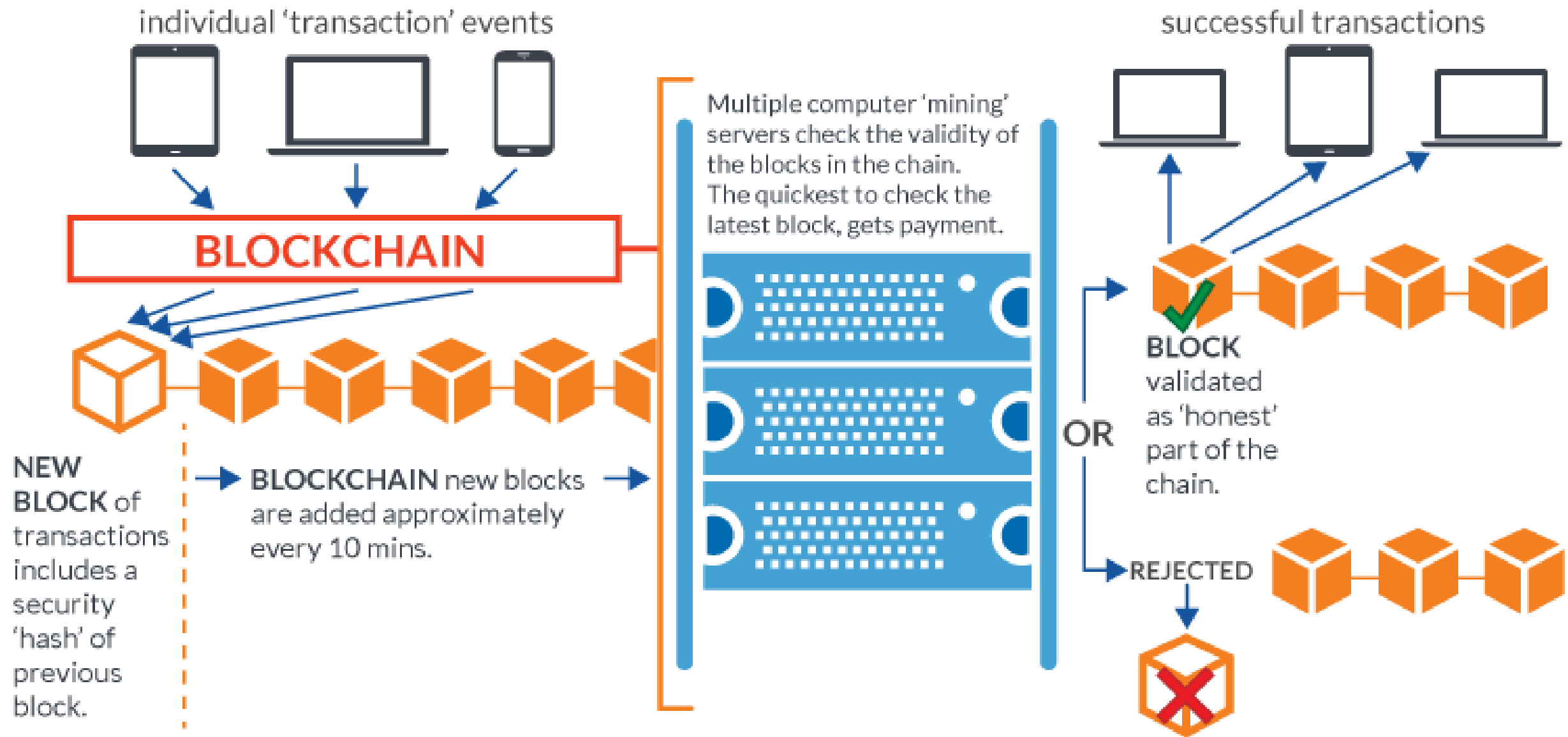
# 1. Overview

---



## Ledger Management

- So far we discussed the method to send payments. But who is managing the ledger?
- This is Satoshi's clever innovation and where the blockchain concept comes from.



# 1. Overview

---



## Ledger Management

- The Previous slide describes the blockchain as a chain of blocks
- Each Block collects inside it a number of transactions from the BTC network
- The generation of the blocks and transactions into them is the job of the miners



# 1. Overview

---



## Ledger Management

- The Header of each new block contains a unique identifier for the entire previous blocks.
- Any tampering with any of the blocks modifies the header and will make the block-chain invalid
- A miner sends his next block only after he solves a certain mathematical puzzle.

# 1. Overview

---



## Ledger Management

- The solution of the puzzle is called PoW
- The trick in the puzzle that it's hard to solve but it is easy to verify the solution ( These types of puzzles are called trapdoor functions.
- Any node that runs the BTC network is able to verify the solution in a speedy way

# 1. Overview

---



## Ledger Management

- The solution of the puzzle is called PoW
- The trick in the puzzle that it's hard to solve but it is easy to verify the solution ( These types of puzzles are called trapdoor functions.
- Any node that runs the BTC network is able to verify the solution in a speedy way

# 1. Overview

---



## Ledger Management

- However more than one miner can solve the puzzle.
- In case we have a conflict we always will opt to the longest chain.
- Any node that runs the BTC network is able to verify the solution in a speedy way
- Whoever solved the puzzle first is credited with new BTCs!!

# 1. Overview

---



## Ledger Management

- How
- In case we have a conflict we always will opt to the longest chain.
- Any node that runs the BTC network is able to verify the solution in a speedy way
- Whoever solved the puzzle first is credited with new BTCs!!

# 1. Overview

---



## Ledger Management - Prevention of Double Attacks

- Any attempt to change blocks in the block-chain will immediately result in an invalid chain ( no solution to the puzzle)
- Hence you need to change the ENTIRE sequence of blocks and solve the puzzle each time
- This becomes un-feasible for malicious actors



# 1. Overview

---



## Ledger Management

- The individual transactions of BTCs are signed through pairs of private public key.
- The management of the chain involves mining process that essentially solves mathematical
- This prevents double spending attacks.

### 3. Size of Market

Overview

Advantage

Size of market

Correlation

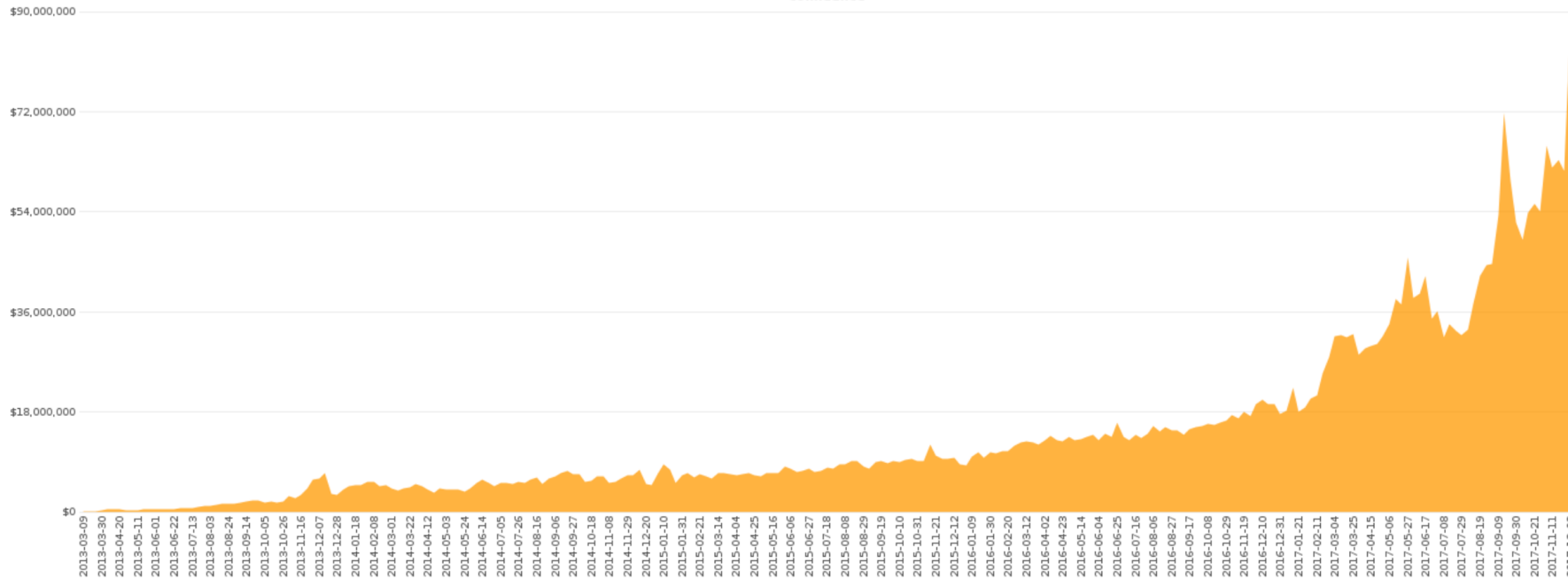
Comparison

Future

Regulation

Global

Weekly LocalBitcoins Volume (Global)  
coin.dance



Total Bitcoin Issuance:  
21 Million  
Currently existing  
Bitcoin: 16 Million

Chart source: coindance.com

# l Distribution

24h

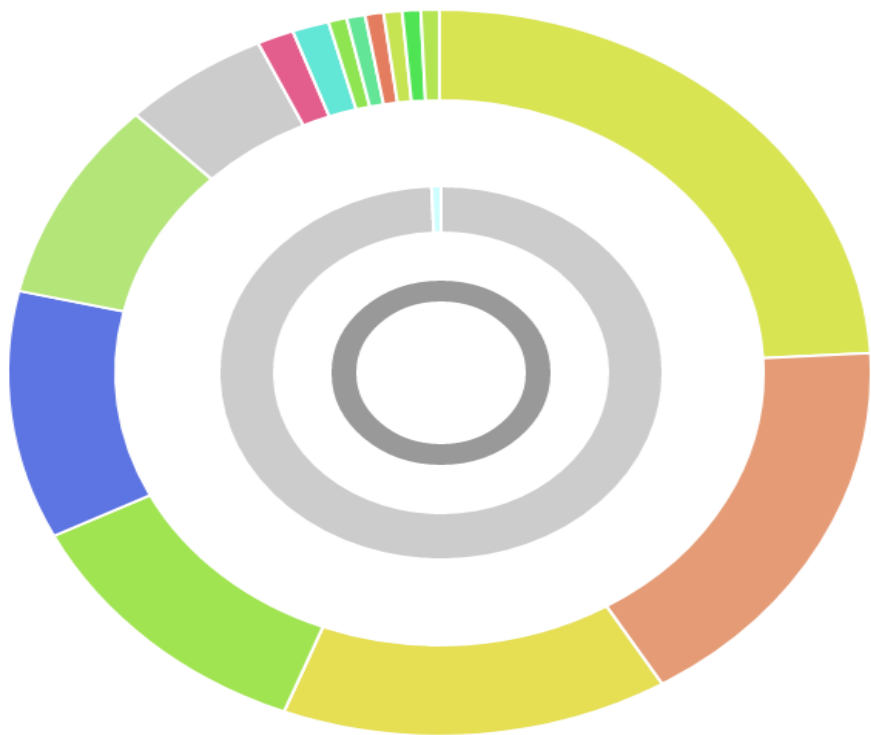
1W

1M













6M

1Y

Max



Size Vote	Blocks	%
ault	144	99.31%
48	1	0.69%

Pool	Blocks	%
 BTC.com	35	24.14%
 AntPool	25	17.24%
 ViaBTC	21	14.48%
 BTC.TOP	17	11.72%
 Slush	16	11.03%
 DiscusFish / F2Pool	13	8.97%
 unknown	8	5.52%
 Bitfury	2	1.38%
 BitClub Network	2	1.38%
 ConnectBTC	1	0.69%
 BTCC	1	0.69%
 Kano CKPool	1	0.69%

## 3.Price Performance

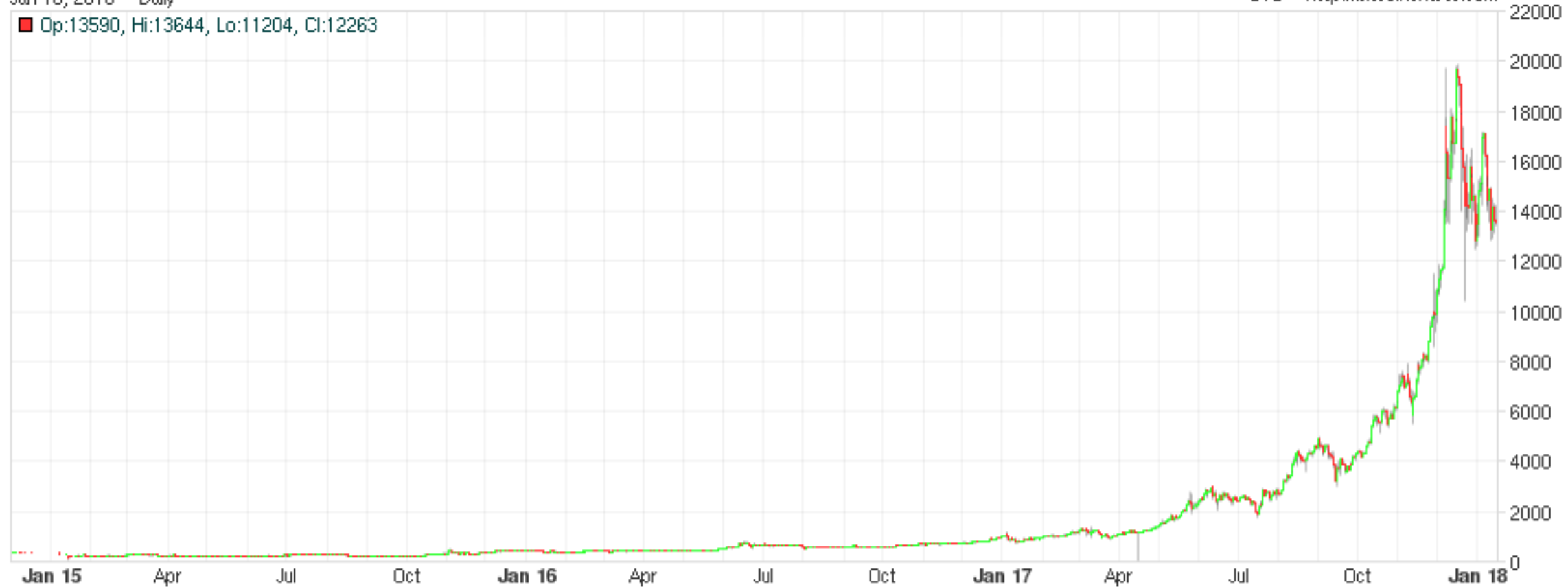
GDAX (USD)

Jan 16, 2018 - Daily

coinbaseUSD

UTC - <http://bitcoincharts.com>

■ Op:13590, Hi:13644, Lo:11204, Cl:12263



Graph source: [bitinfocharts.com](http://bitinfocharts.com)

# 3.Size of Market

Overview

Advantage

**Size of market**

Correlation

Comparison

Future

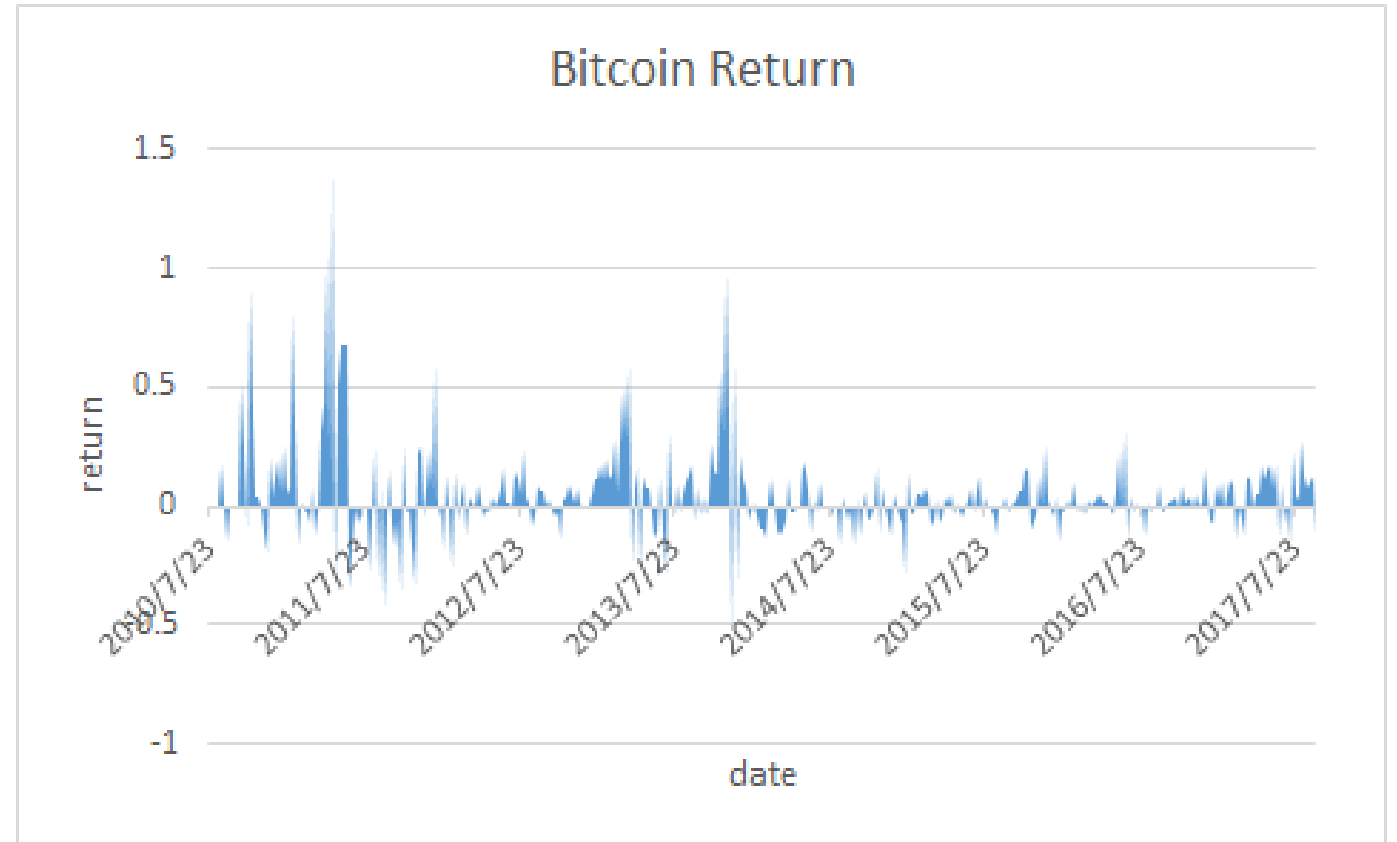
Regulation

Bitcoin purchaser:

- Retail investors
- Financial hedger
- Criminals
- People who concentrate in block chain technology, etc.

Bitcoin Stats:

- Annualized Return 100%
- Annualized Volatility 80%
- Weak Correlation with other indices



## 4. Correlation With Major Assets

Overview

Advantage

Size of market

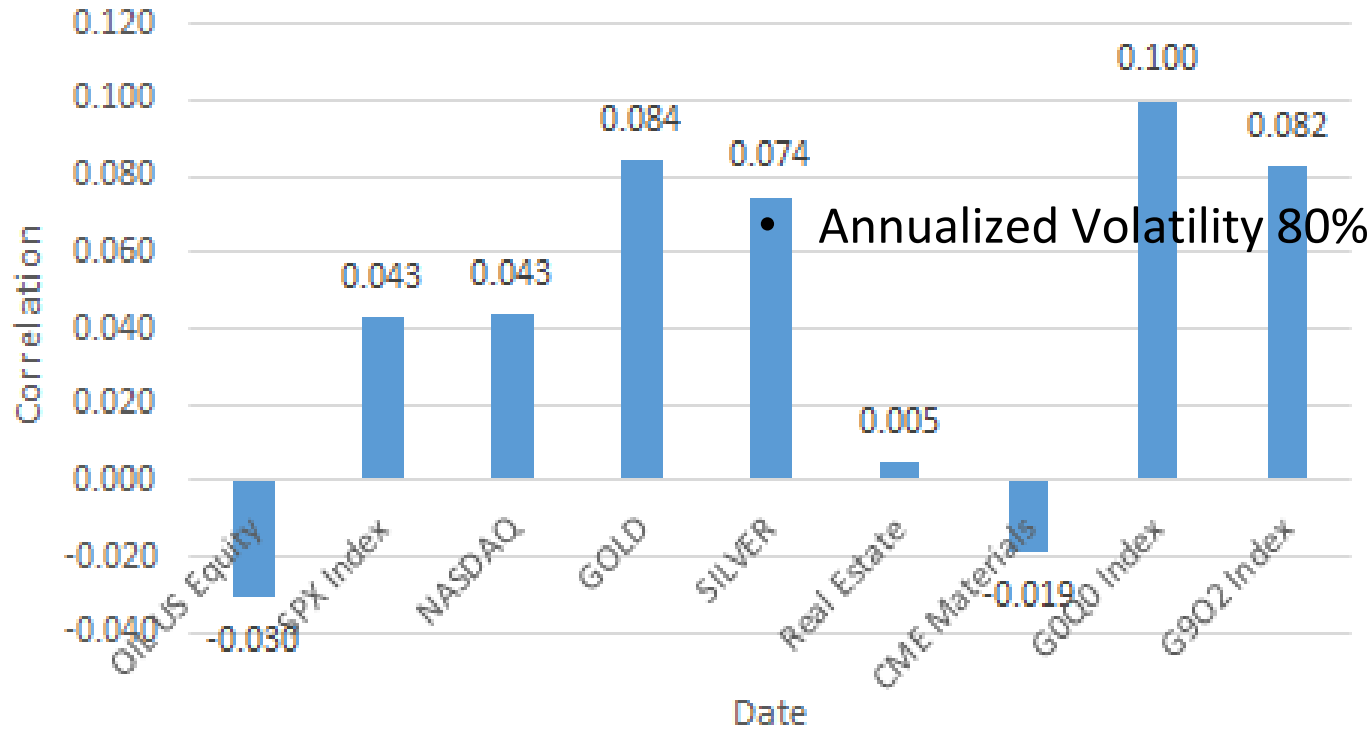
Correlation

Comparison

Future

Regulation

Correlation Between Assets and Bitcoin



• Annualized Volatility 80%

- The absolute value of correlation is low, we can.
- Conversely, Bitcoin can't be used as a diversify risk tool because of its volatility



# 1. Overview

---



## BTC Trading

- The trading of BTC takes place on exchanges or peer peer websites ( local bitcoins.com)
- I will explain how to trade BTCs through exchanges
- My preferred exchange is coinbase.com but I warn you that it's loosely regulated and you can lose all your money

# 1. Overview



## BTC Trading- Establish Coinbase Account

The screenshot shows the Coinbase homepage with a dark blue background. At the top, the 'coinbase' logo is on the left, and navigation links for 'Products', 'Help', 'Charts', 'Sign In', and 'Sign Up' are on the right. The main heading 'BUY AND SELL DIGITAL CURRENCY' is in large white capital letters. Below it, a subtitle states: 'Coinbase is the world's most popular way to buy and sell bitcoin, ethereum, and litecoin.' A central form contains a white input field with the placeholder text 'Enter your email address' and a blue 'Get Started' button. At the bottom, there are two links: 'New to bitcoin?' and 'What is ethereum?'.

# 1. Overview

---



## BTC Trading- Establish Coinbase Account

- Coinbase operates is regulated in the US and hence requires KYC ( Know your client ) documents.
- Coinbase operates through ACH network and hence may ask for your account
- Once you establish an account you can start trading directly from your Savings/Checking or credit card account



 Buy/Sell  Accounts  Tools  Settings

By clicking on buy/sell buttons  
you can start trading BTCs

let

BTC ≈ \$5.44

end

 Receive

...

allet

BCH ≈ \$1,084.84

end

 Receive

...

allet

ETH ≈ \$4,837.36

end

 Receive

...

## Transactions

 Search

DEC  
19



**Sold Bitcoin**

Using Chase - Chase Plus Sav... \*\*\*\*\*6407

−0.6840 BT  
−\$11,947.

DEC  
13



**Sold Bitcoin**

Using Chase - Chase Plus Sav... \*\*\*\*\*6407

−1.0000 BT  
−\$15,708.

SEP  
14



**Sold Bitcoin**

Using Chase - Chase Plus Sav... \*\*\*\*\*6407

−2.0000 BT  
−\$7,157.

JUL  
21




**Bought Bitcoin**

Using Chase - Chase Plus Sav... \*\*\*\*\*6407

+3.68453678 BT  
+\$10,149.


# 1. Overview


## Your Accounts




My Wallet

0.0005 BTC ≈ \$5.48

 Send


 Receive


...




BCH Wallet

0.6845 BCH ≈ \$1,080.72

 Send


 Receive


...



ETH Wallet

5.5798 ETH ≈ \$4,860.01

 Send

 Receive

...



LTC Wallet

By clicking on Buttons send/receive you can send any amount of BTCs to anybody in the world without any restrictions and not going to the bank. It takes couple of hours to transfer millions of dollars.

Transactions			Q Se
DEC 19		Sold Bitcoin	Using Chase - Chase Plus Sav... *****6407
DEC 13		Sold Bitcoin	Using Chase - Chase Plus Sav... *****6407
SEP 14		Sold Bitcoin	Using Chase - Chase Plus Sav... *****6407
JUL 21		Bought Bitcoin	Using Chase - Chase Plus Sav... *****6407
JUL 15		Sent Bitcoin	To Bitcoin address

## 5. Comparison

---



### Wallets

- In order to hold large number of BTCs usually the best practice is to have your own wallet.
- You can download and store your BTCs on your computer or online wallet.
- The oldest online wallet is Blockchain.info.
- To establish a wallet go to the website and go through the registration process



# 1. Overview



## BTC Trading- Establish Coinbase Account

Welcome Back!

or [Sign Up](#)

Sign in to your wallet below

Wallet ID

4e642528-9d0b-454c-9dc7-8a9d5e0eedb1

Find the login link in your email, e.g. *blockchain.info/wallet/1111-222-333...* The series of numbers and dashes at the end of the link is your Wallet ID.

Password

LOG IN

[Log in via Mobile](#)

Having some trouble? [View Options](#)

## 5. Comparison



- Once you login into your wallet you will be able to send and receive BTC or any other Cryptocurrency
- Be aware there is no password RECOVERY mechanism.
- If you lose your password most probably you have lost all your BTCs

## 5. Comparison



### Etherium and ICOs

- Currently there are around 1300 crypto-currencies improving on BTC in all shape or forms
- I am not going to address the Blockchain technology in this talk as it will require another seminar
- However one particular comparison to BTC is especially interesting as this is ETH

## 5. Comparison



### Etherium and ICOs

- Ethereum is a currency enabling programming within the Blockchain.
- Just like BTC eliminates the middle men in transferring money Ethereum has the potential to modify other industries like insurance and real estate transactions
- In particular ETH immensely simplifies ICO issuance
- ICO is BANNED in the USA

## 5. Comparison

---



### Initial Currency Offering

- ICO issues cryptocurrency that is associated with the company similar to stock issuance through the IPO process.
- However there is no company ownership in ICOs.
- The role of VCs and Private equity firms is eliminated or diminished.
- Kodak and Telegram prepare to issue ICO during 2018.

## 5. Comparison

---



### Forks And the Concept of Free Money

- Developers that handle the BTC code tend to disagree on BTC functionality
- An example occurred during 2017 where developers refused to increase the block size
- As a result BTC was forked ( new code branch introduced)
- However anybody that held BTC prior to split got the new tokens BCH for free.
- BCH appreciated in its price 10 fold in a matter of 3 months

## 5. Comparison



### Forks And the Concept of Free Money

- Developers that handle the BTC code tend to disagree on BTC functionality
- An example occurred during 2017 where developers refused to increase the block size
- As a result BTC was forked ( new code branch introduced)
- However anybody that held BTC prior to split got the new tokens BCH for free.
- BCH appreciated in its price 10 fold in a matter of 3 months

## 5. Comparison

---



### Forks And the Concept of Free Money

- This is free money in my view
- Anybody can create his own fork. This was being automated
- Gives users unprecedented power of literally printing their own money





# BitcoinCobaltExtreme Core - Wallet



Overview



Send



Receive



Transactions

Pay To:

Enter a BitcoinCobaltExtreme address (e.g. FTG7aX1m13XM5T63MDQ5JamKbZR4jVdPDQ)



Label:

Enter a label for this address to add it to your address book

Amount:



BCX

☐

Subtract fee from amount

Transaction Fee: 0.00020000 BCX/kB

Choose...

**Warning: Fee estimation is currently not possible.**

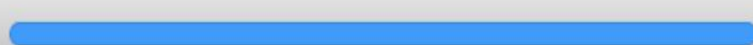
Send

Clear All

Add Recipient

Balance: 0.00000000 BCX

Syncing Headers (17.3%)...



BCX HD  

## 7. Regulation



### **Regulation of cryptocurrency in the U.S.**

The U.S. Securities and Exchange Commission said the cryptocurrencies are subject to federal securities laws. SEC Chairman Jay Clayton said that “Offers and sales of digital assets by ‘virtual’ organizations are subject to the requirements of the federal securities laws”. The regulations apply to entities that use distributed ledger or blockchain technology, as in, “Initial Coin Offerings” or “Token Sales.” Unregistered offerings will be liable for violation of federal securities laws.

# 7. Regulation



United States Regulation Map		
Bitcoin friendly	Bitcoin Unfriendly	Bitcoin Hostile
Texas	Wisconsin	Hawaii
Kansas	North Carolina	New Mexico
Tennessee	California	Connecticut
South Carolina	Pennsylvania	Georgia
Montana	Florida	Washington
		New York
		New Hampshire

## 7. Regulation



### Regulation of cryptocurrency in China

On Sept.4th 2017, 7 Chinese ministries announced that from the date of announcement issue, all kinds of initial coins offerings should be stop immediately. The organizations and individuals who have completed funding raising by issuance of tokens shall clearing out and make some arrangements to protect investor's rights and interests and to allocate risks properly.

The announcement determined the nature of initial coins offerings specifically as the financial entities raise bitcoins, ETH and other so-called “virtual currency” from investors through illegal sale and circulation of tokens. The essence of it is an unauthorized illegal act of financing including illegal sale of tokens, illegal securities issuance and illegal fund-raising, financial fraud, pyramid sale and other criminal activities.

Then, all Chinese cybercurrency transaction platforms stopped trading, and BTCCHINA, the biggest Chinese online bitcoin trading platform will stop the withdrawal in Oct.30.

## 7. Regulation

Overview

→ Advantage

→ Size of  
market

→ Correlation

→ Comparison

→ **Regulation**

→ Future

### Some other countries' attitude towards cryptocurrency

<b>Russia</b>	The cryptocurrency such as bitcoin composites “serious risk”, allows people to “wash white crime income, tax evasion and even support terrorism, as well as those will obviously affect the ordinary citizens perpetuate scam”.
<b>Vietnam</b>	Virtual currencies such as bitcoin are not legal forms of payment in Vietnam. Virtual currencies such as bitcoin, which are issued, supplied and used as payment, are banned in Vietnam.
<b>South Korea</b>	South Korea’s central bank governor Lee Joo-yeol has announced that cryptocurrency such as bitcoin will be regulated as a commodity rather than as currency.
<b>Singapore</b>	The monetary authority of Singapore and the Singapore central bank are moving ahead with a law that will introduce some retail payment services in a piece of legislation, including bitcoin and cryptocurrency exchanges

# Conclusion

---

- At present every cyber currency is at an early stage of evolution and widespread acceptance.
- Cyber currencies have many benefits, but also have shortcomings, some of which will be addressed with the evolvement of an effective regulatory structure
- As an investments vehicle, it is at present used mainly by speculators, due to high volatility. It will take time for the market to have depth and stability and wider participation.

## BIBLIOGRAPHY

---

- <https://www.coindesk.com/price/>
- <https://coinmarketcap.com/currencies/ethereum/>
- <http://www.reuters.com/article/us-usa-regulation-bitcoin/former-sec-chief-says-regulator-not-equipped-to-take-on-bitcoin-idUSKCN1C32LN>
- <https://www.buybitcoinworldwide.com/volatility-index/>
- <https://blockgeeks.com/>
- <https://coinmarketcap.com/>
- <https://steemit.com/>
- IMF staff discussion note - Virtual currencies and beyond: initial considerations
- Baur Dirk G. Kühne (Logistics University), Hong KiHoon (Hongik University), LeeAdrian D (UTS Business School): Bitcoin: Currency or Asset?
- Coin BR Blockchain Tech - Bitcoin: A new financial asset?

# Question?

