BITCOIN

THE INTERNET MONEY

CAMERON WINKLEVOSS @winklevoss
TYLER WINKLEVOSS @tylerwinklevoss

WINKLEVOSS
CAPITAL

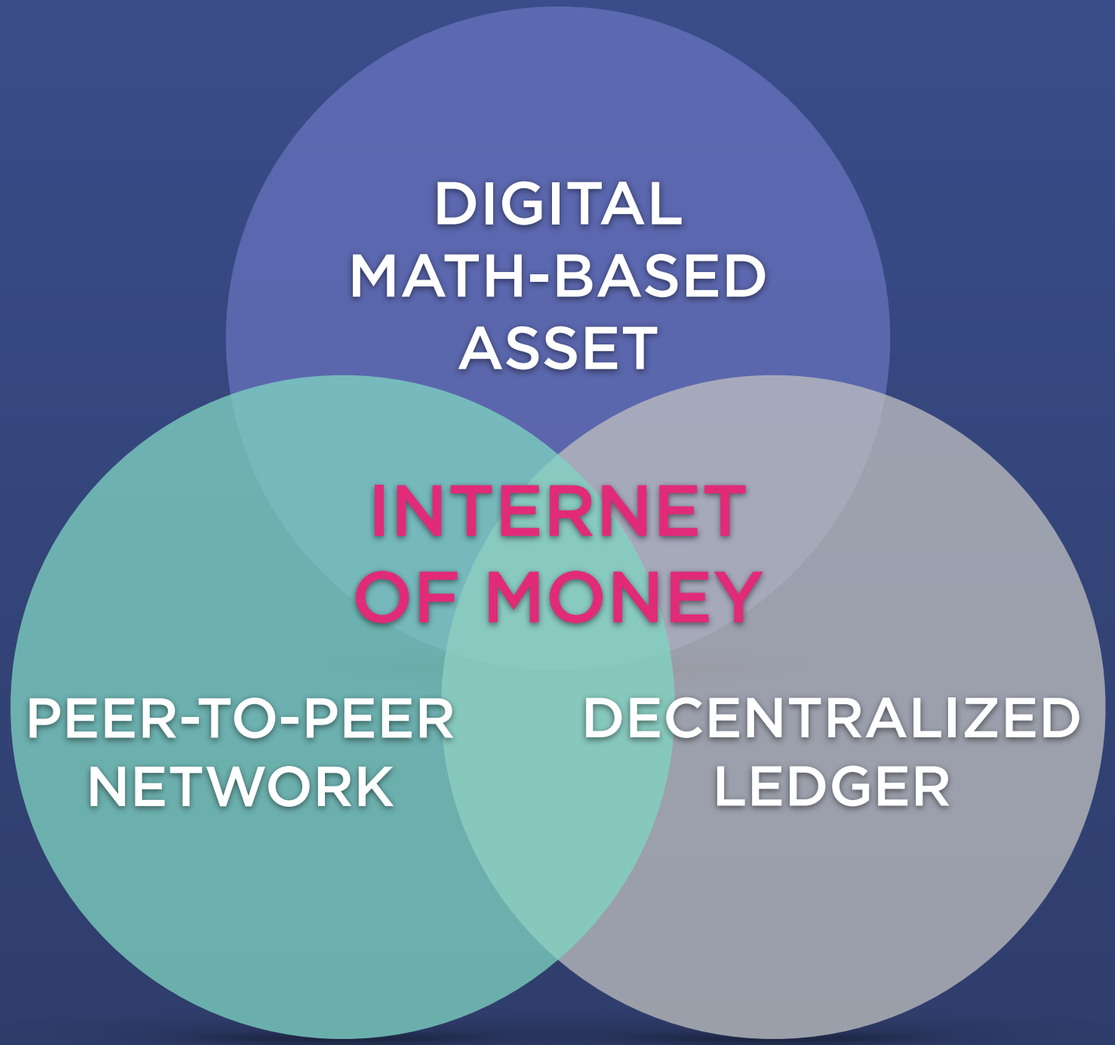
WHAT IS BITCOIN?

- Bitcoin (capital “B”) is a peer-to-peer network that maintains a public decentralized ledger of digital math-based assets known as bitcoins (lowercase “b”). The integrity of this ledger is backed and secured by a subnetwork of computers (miners) who audit and archive its transactions for a reward.

- The supply of bitcoins is fixed at 21 million and each bitcoin can be divided into a hundred million pieces.

- Their ownership cannot be changed within the ledger without instructions from their current owner that have been cryptographically authenticated (digital signatures) by a majority of nodes on the Bitcoin network. In essence, “sending a bitcoin” is sending instructions to the network to make a change of custody in the public ledger.

- These attributes make the Bitcoin network a financial network, or the “Internet of Money”.



WHO CREATED BITCOIN?

OCTOBER 31, 2008

Satoshi Nakamoto publishes white paper titled *Bitcoin: A Peer-to-Peer Electronic Cash System* via "The Cryptography Mailing List".

JANUARY 3, 2009

Satoshi releases Bitcoin source code and software client to the world.

2009-2010

Satoshi updates the source code and writes hundreds of posts totaling 80,000 words (length of a novel).

APRIL 23, 2011

Satoshi vanishes from the Internet after emailing a developer saying he has "moved onto other things".

WHO CREATED BITCOIN?

CLUES

- Satoshi Nakamoto is believed to be a pseudonym for the individual or group of individuals responsible for Bitcoin. No record of a programmer by this name exists prior to Bitcoin.
- His P2P Foundation account details say he is a 38-year old male living in Japan.
- In Japanese satoshi means “clear-thinking” or “wise”, naka can mean “inside” or “relationship” and moto is used to describe “the origin” or “the foundation.” Strung together it reads “thinking clearly inside the foundation”.
- If an individual, he is a world class programmer with deep knowledge of C++, economics, cryptography and peer-to-peer networking.
- He writes in flawless English. His first post used American spellings; every post thereafter employed British spellings and British colloquialisms.
- He has read a British newspaper. He embedded Times of London headline (“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”) into first Bitcoin transaction (Genesis Block).
- His timestamps do not reflect a particular timezone.

PHILOSOPHY
IN CRYPTOGRAPHY WE TRUST

"What is needed is an electronic payment system based on ***cryptographic proof instead of trust***, allowing any two willing parties to transact directly with each other without the need for a trusted third party."

-Satoshi Nakamoto, ***"Bitcoin: A Peer-to-Peer Electronic Cash System"*** **| October 31, 2008**

PHILOSOPHY
IN CRYPTOGRAPHY WE TRUST

*"**The root problem** with conventional currency **is all the trust that's required** to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micro-payments impossible."*

-Satoshi Nakamoto, blogpost in P2P Foundation forum **| February 11, 2009, 22:27**

PROBLEM

HOW TO REACH CONSENSUS IN A DECENTRALIZED SYSTEM

"A group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. ***The problem is to find an algorithm to ensure that the loyal generals will reach agreement.***"

-Marshall Pease, Robert Shosthak and Leslie Lamport, *The Byzantine Generals Problem*

BREAKTHROUGH MINING

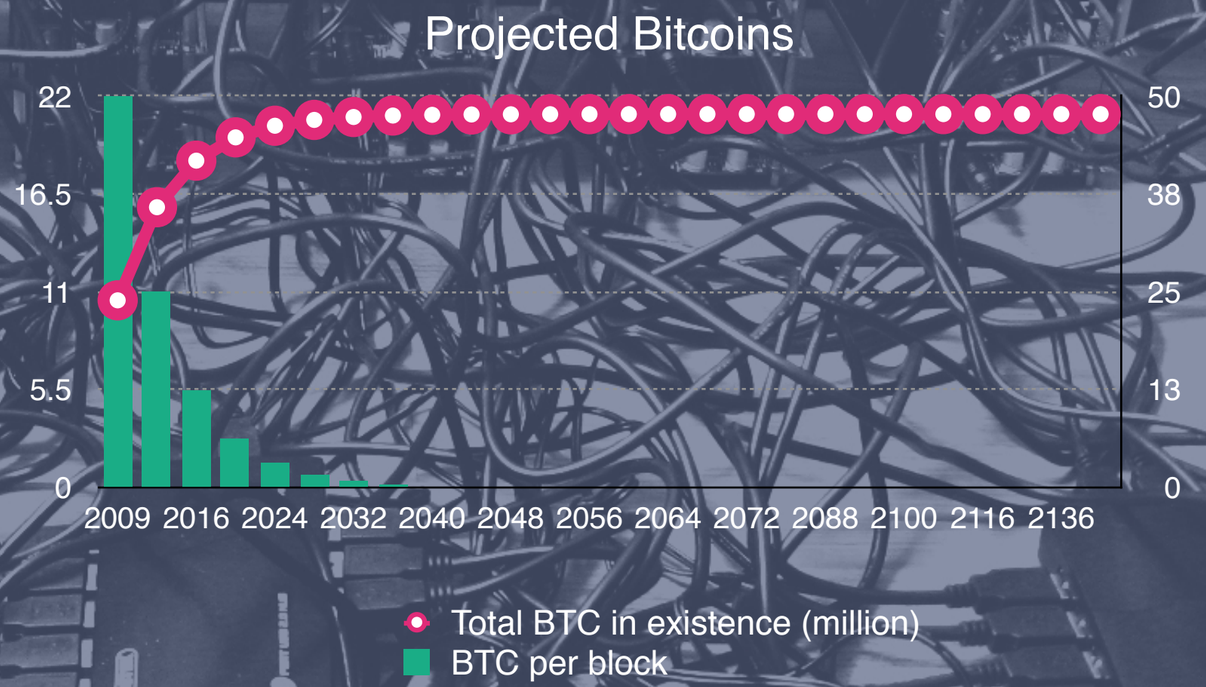
- The Bitcoin “mining algorithm” is the breakthrough that solved the Byzantine General’s Problem and allows the network to reach majoritarian consensus as to which bitcoin transactions are valid and which are not, without the need for a trusted 3rd party.

- Mining ensures "digital scarcity" in a decentralized system by preventing the same bitcoin from being spent twice by the same person (i.e., it solves the double-spend problem).

- By dedicating computing power to solving the mining algorithm, miners act as the network's scrupulous accountants.

- For their efforts, miners are rewarded with newly minted bitcoins (or very small transaction fees) roughly in proportion to the computing power they provide.

- Mining makes decentralization possible by taking all of the costs associated with centralized trusted 3rd parties out of the system, giving the Bitcoin network and bitcoin the asset its technological intrinsic value.



HOLY TRINITY OF MONEY

COMMODITY

CURRENCY

TECHNOLOGY

COMMODITY: BITCOIN VS GOLD

	Scarce	Durable	Portable	Divisible	Authenticity Verification	Storage	Fungible	Difficult to Counterfeit	Widespread Use
Gold	✓	✓	✗	!	!	✗	!	!	✗
Bitcoin	✓	✓	✓	✓	!	✓	✓	✓	✗

✓ YES

! NEUTRAL

✗ NO

COMMODITY: BITCOIN VS GOLD

- **Scarce**: The supply of bitcoin is more fixed than the supply of gold. While gold can still be found on earth and possibly mined on asteroids, there will never be more than 21 million bitcoins minted.

- **Durable**: Due to its decentralized and distributed public ledger, Bitcoin could survive a nuclear attack, whereas Ft. Knox could not. Gold boils at 2,856°C (5,127°F), while the temperature of a nuclear explosion is ~100,000,000°C (~180,000,000°F) or 10x the surface temperature of the sun. Moreover, there are plans to launch a Bitcoin node with the public ledger into space via satellite.

- **Portable**: Any amount of bitcoin can be sent around the world instantly and for free with a data connection. Gold is heavy, and transporting large quantities requires infrastructure (i.e., armored truck, bonded guards) and customs declarations if cross-border.

- **Divisible**: A bitcoin can be divided into 100 million pieces. Gold must be smelted, which is possible but not easy. Gold cannot be divided into infinitesimal amounts.

- **Authenticity Verification**: A bitcoin is digital, therefore, it must be identified in the public ledger by software. Gold requires a trained eye or chemical test.

- **Storage**: Private keys that control bitcoin ownership can be stored on paper, in your brain (brain wallet) or on a USB stick. Storing large quantities of gold requires infrastructure (i.e., safe or vault).

- **Fungible**: At the moment, all bitcoins are treated equally. Chemically, gold is equal, but purity levels vary and gold bars must be weighed to detect counterfeit authority stamps.

- **Difficult to Counterfeit**: It is mathematically impossible to counterfeit a bitcoin, and the possibility of a “double spend attack” remains remote and highly unlikely. Gold cannot be counterfeited, but gold bars can be tampered with, and vaults don’t generally test every bar.

- **Widespread Use**: Once a medium of exchange, today gold serves almost entirely as a store of value with a small percentage of it used in jewelry and industrial applications. Bitcoin does not currently have widespread adoption as a medium of exchange, however, large scale retailers are beginning to accept it as a form of payment. Many institutional and professional investors have added bitcoin to their portfolios alongside gold and other commodity/capital asset holdings.

**If 51% of miners agreed to change the supply, they could. This, however, is viewed as be unlikely given that this would decrease the value of bitcoin, and thereby decrease the profits of miners.*

CURRENCY: BITCOIN VS FIAT

	Scarce	Durable	Portable	Divisible	Authenticity Verification	Storage	Fungible	Difficult to Counterfeit	Widespread Use
Fiat	!	!	✓	✓	✓	!	✓	!	✓
Bitcoin	✓	✓	✓	✓	!	✓	✓	✓	✗

✓ YES

! NEUTRAL

✗ NO

CURRENCY: BITCOIN VS FIAT

- **Scarce**: Bitcoin's supply is fixed at 21M; fiat's is not. Since 2008, the Fed has more than tripled the U.S. Monetary Base with its quantitative easing policies.

- **Durable**: Bitcoins have been lost or stolen, but never destroyed. Fiat currency can be easily lost, stolen, or destroyed, however, damaged bills can be replaced without loss of value. With proper backup, bitcoins can last forever.

- **Portable**: Bitcoins are digital, therefore, any amount can easily be transported over any distance with an internet/data connection for free. It is relatively easy to transport cash up to a certain amount (i.e., wallet), however, larger amounts can require infrastructure (i.e., armored truck), customs declarations for cross-border transportation and/or instruments (i.e., debit/credit cards and their fees).

- **Divisible**: One bitcoin can be divided into 100 million pieces; the USD, for example, is divisible into 100 pieces (i.e., penny).

- **Authenticity Verification**: Bitcoins are digital, therefore, they must be identified in the public ledger by software; the USD is easily identifiable by eye or chemical tests (i.e., markers).

- **Storage**: Private keys that control bitcoin ownership can be stored on paper, in your brain (brain wallet) or on a USB stick. You can only store a limited amount of fiat before requiring infrastructure (i.e., mattress, bank vault).

- **Fungible**: At the moment, all bitcoins are treated equally, as are fiat denominations that are equivalent to one another.

- **Difficult to Counterfeit**: It is mathematically impossible to counterfeit a bitcoin, and a "double spend attack" has never been successfully perpetrated. Fiat currencies have dealt with counterfeiting since their inception.

- **Widespread Use**: Fiat money achieves status of legal tender via government decree. As a result, merchants must accept it and citizens must settle their taxes with it. Bitcoin is ~5 years old and does not currently have widespread adoption, however, large scale retailers are beginning to accept it as a form of payment. Many institutional and professional investors have added bitcoin to their portfolios alongside gold and other commodity/capital asset holdings.

TECHNOLOGY: A NETWORK

net·work: a system of devices that are connected to each other.

INTERNET

Global computer network

AMAZON

Server-based network

BITCOIN

Peer-to-peer network

TECHNOLOGY: A PROTOCOL

pro·to·col: (computer science) a set of rules or procedures for transmitting data between electronic devices, such as computers.

INTERNET

Internet Protocol Suite (TCP/IP)

WEBPAGES

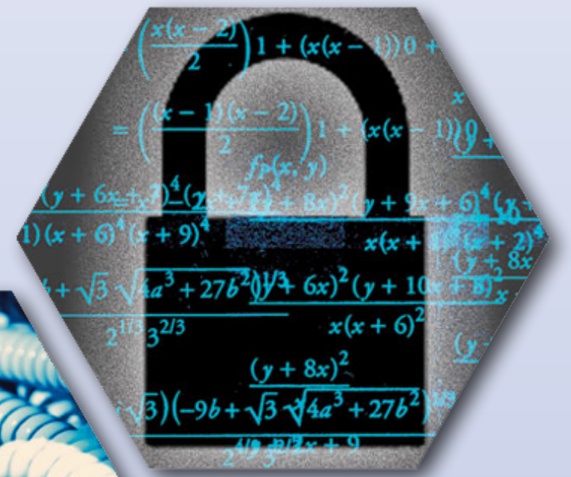
(HTTP)

EMAIL

(SMTP/IMAP)

VOICE

(VoIP)



BITCOIN

(MoIP)

POSTAL SERVICE

Slow+
Costly

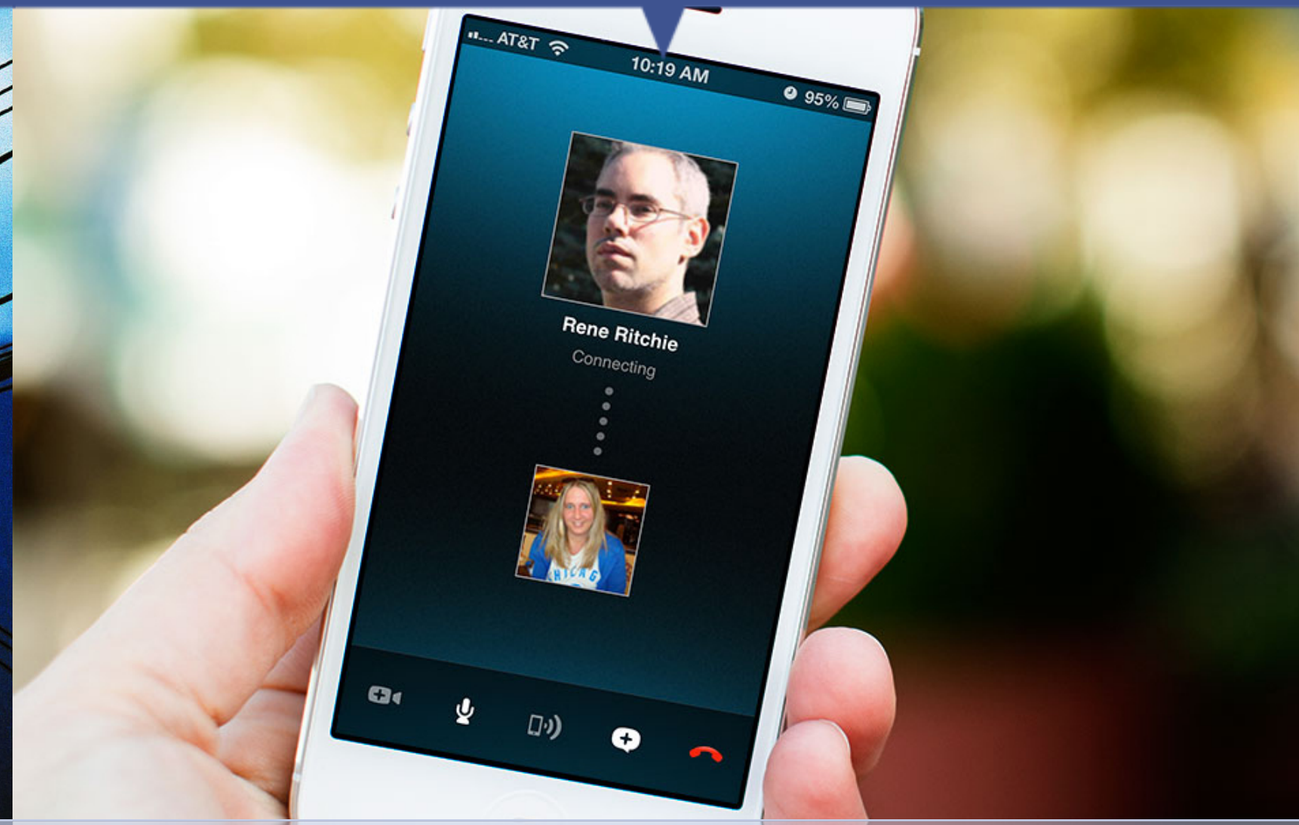
SMTP

Instant+
Free

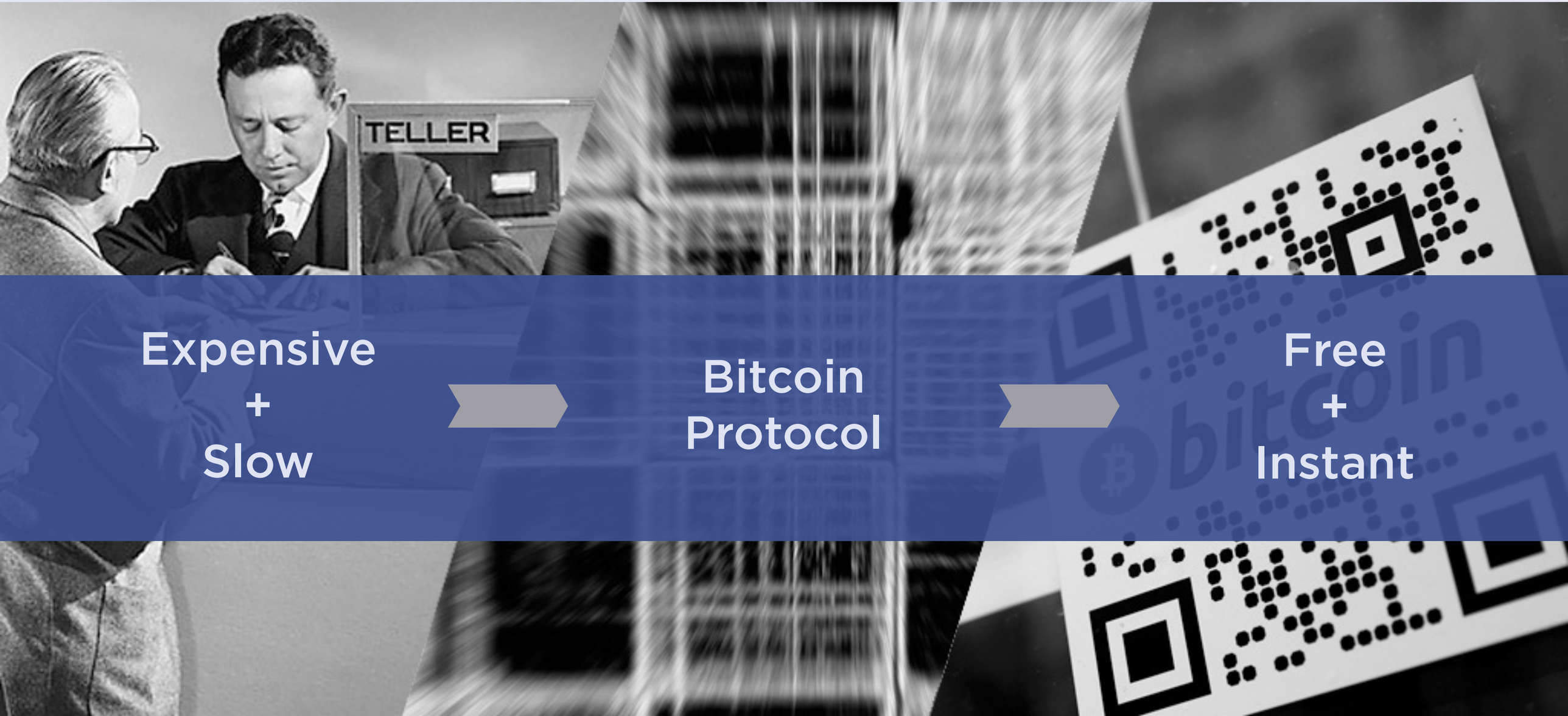
TELECOMMUNICATIONS

Circuit-switching telephone networks convert voices into electronic signals and transmit them over **costly**, duopolistic infrastructure (e.g., AT&T).

Packet-switching networks like the Internet, digitize and transmit voices via real-time data packets over **protocols** like the Voice over Internet Protocol (VoIP), for **free** (e.g., Skype).



FINANCIAL SERVICES



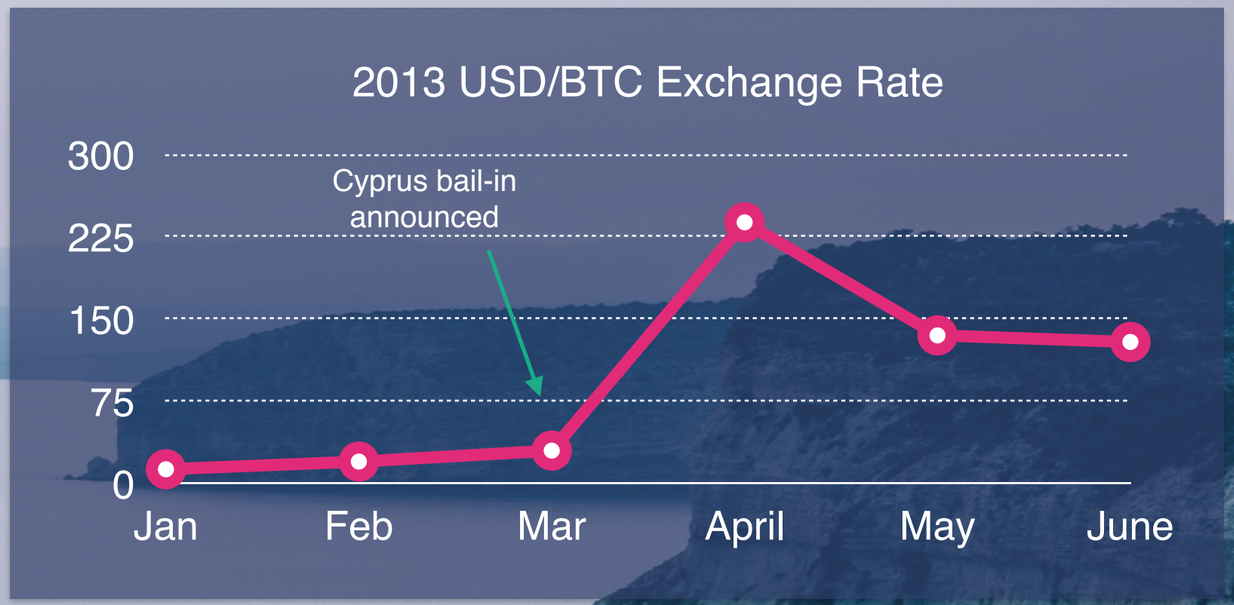
Expensive
+
Slow

Bitcoin
Protocol

Free
+
Instant

IMPLICATIONS

IMPLICATIONS: CYPRUS



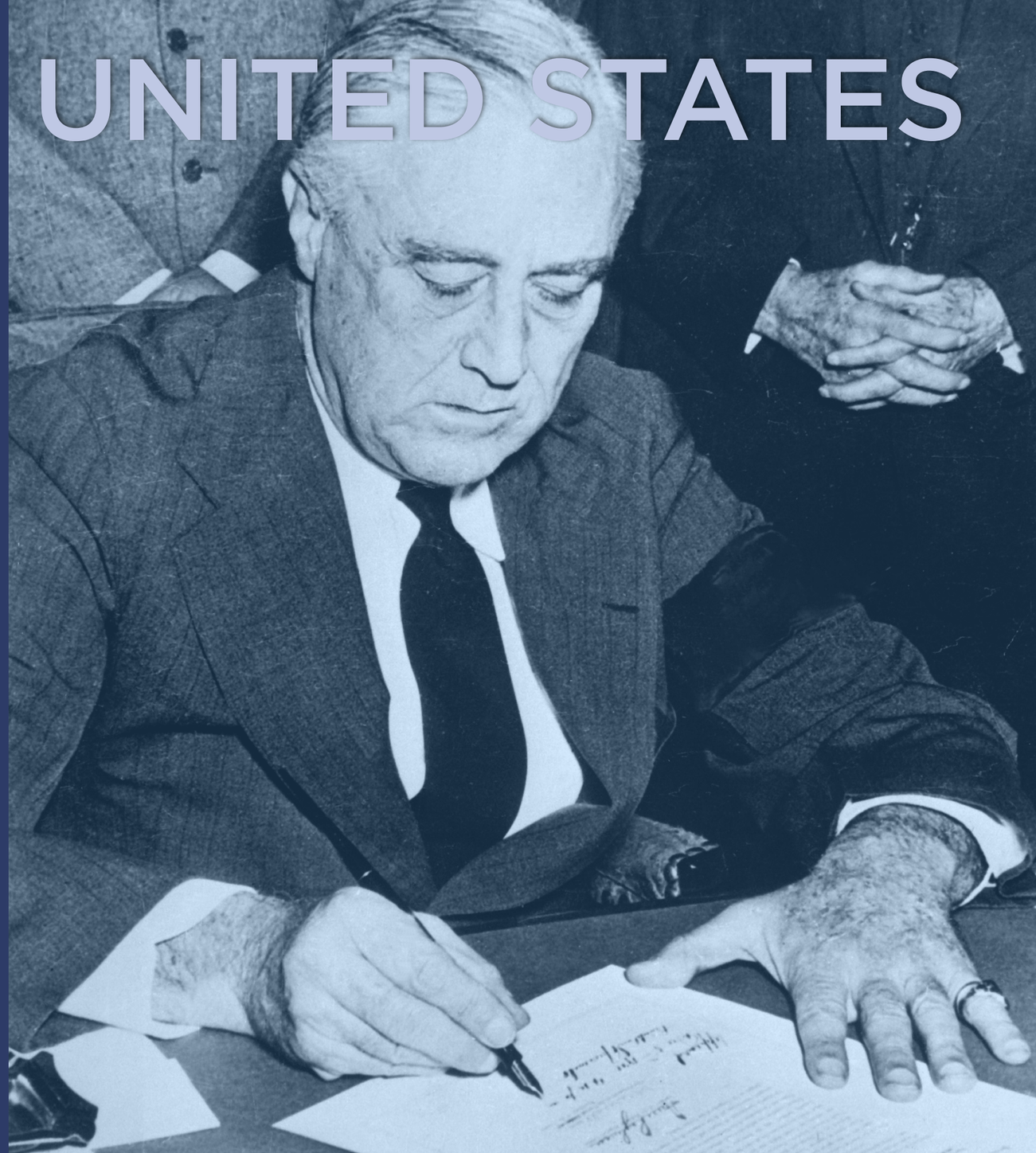
- March 25, 2013 - **Cypriot Financial Crisis**: “The shot heard round the world”.
- Cyprus freezes all bank accounts, restricting all withdrawals and transfers of money.
- €10B Eurozone bail-out contingent upon a **Cyprian bail-in** or **haircut** of 40% or more on all domestic bank accounts > €100K (including those insured).
- March to June of 2013 - Cyprus faces greatest risk of stagflation and greatest drop in Eurozone bank deposits (-15.68% or -€10B).
- Crisis introduces bitcoin to the world as an asset class immune to bail-ins and fiscal mismanagement; price of a bitcoin increases 10x.

IMPLICATIONS: UNITED STATES

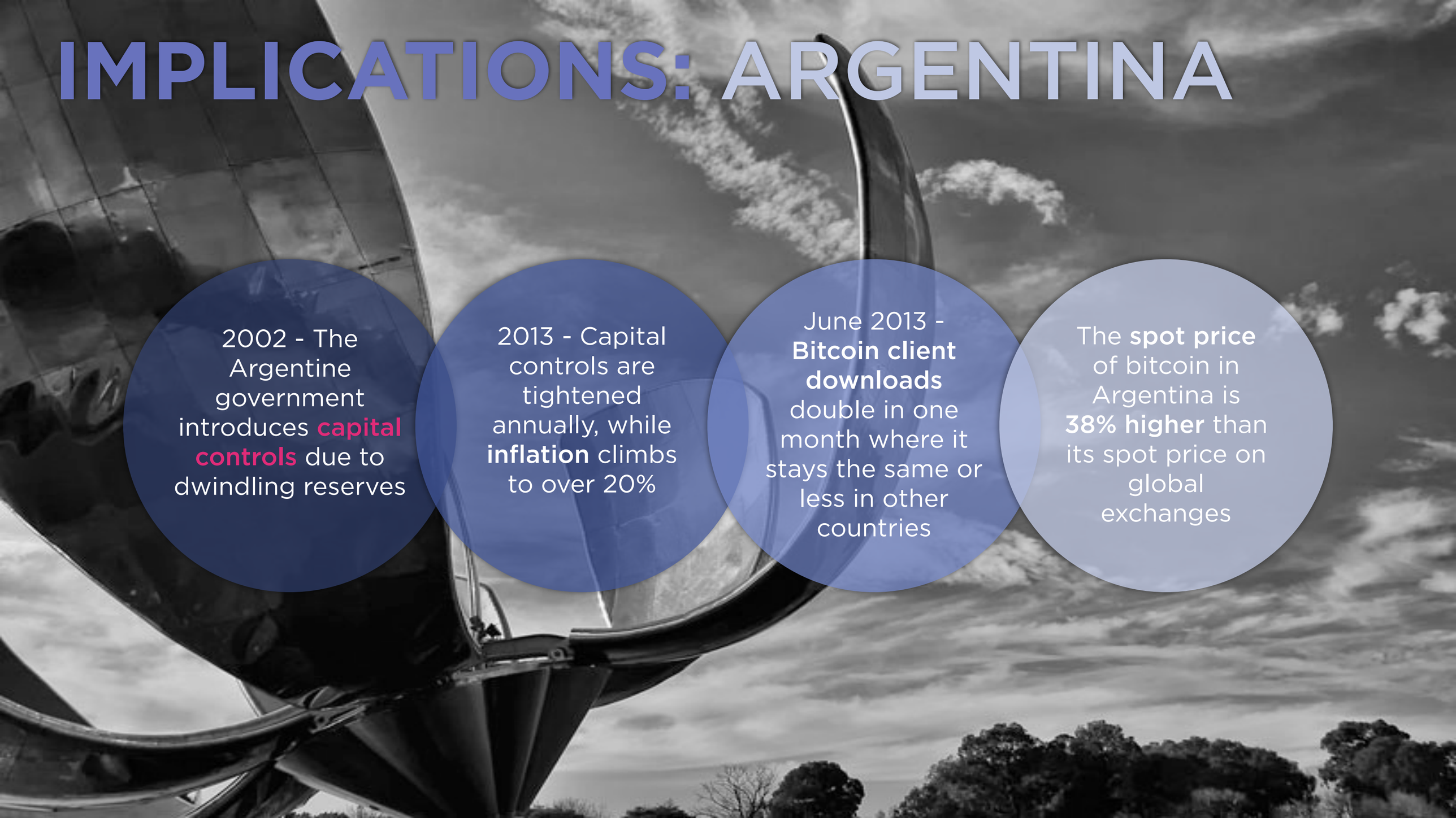
- April 5, 1933 - President Roosevelt signs **Executive Order 6012** “forbidding the hoarding of gold coin, gold bullion and gold certificates within the continental United States”.

- A bitcoin lives in a distributed public ledger and is associated with a specific **256-bit private key**, the possession of which determines its ownership.

- A private key can be stored in your memory (i.e., **brain wallet**), making it and the bitcoins associated with it difficult to appropriate.



IMPLICATIONS: ARGENTINA

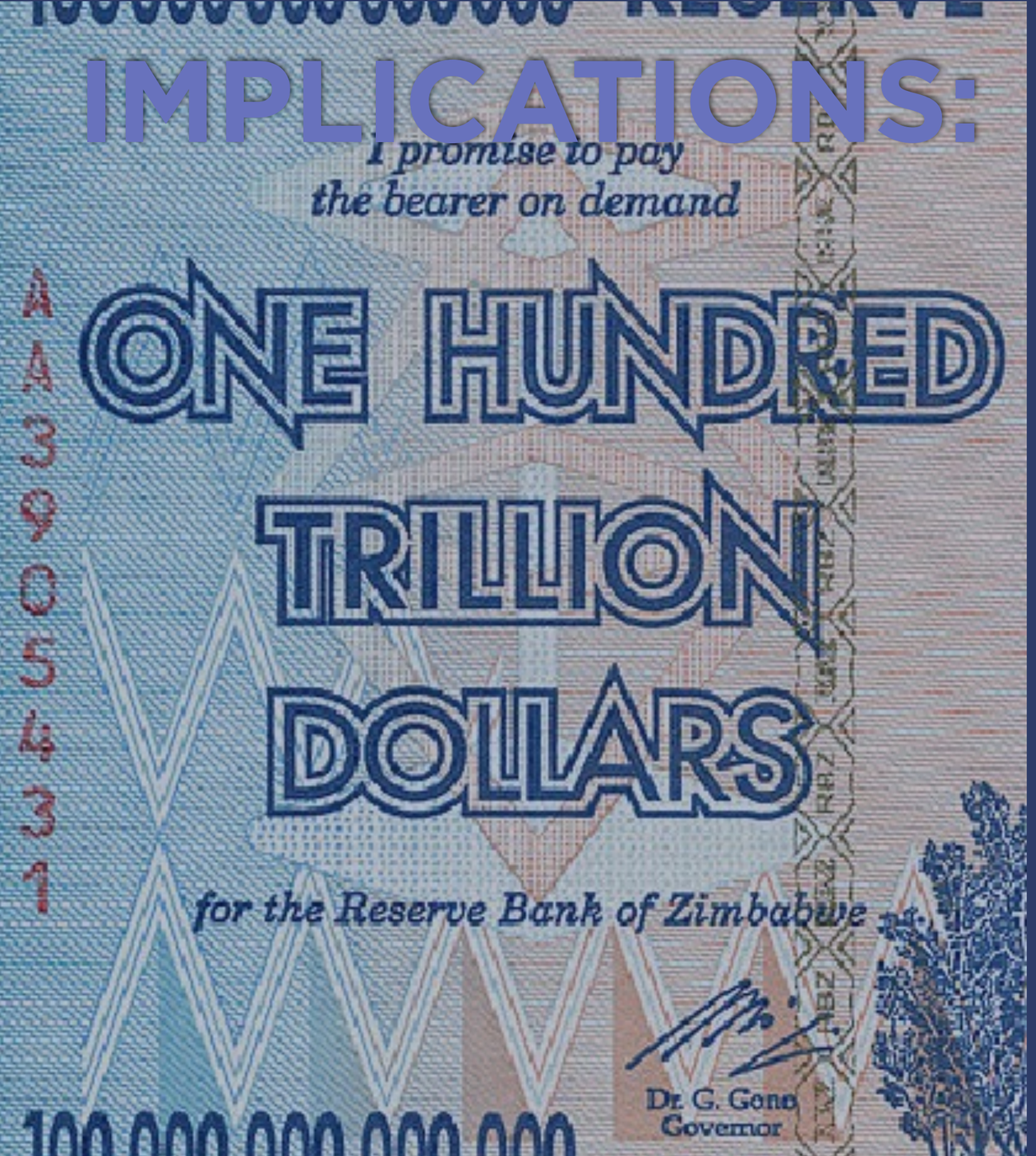


2002 - The Argentine government introduces **capital controls** due to dwindling reserves

2013 - Capital controls are tightened annually, while **inflation** climbs to over 20%

June 2013 - **Bitcoin client downloads** double in one month where it stays the same or less in other countries

The **spot price** of bitcoin in Argentina is **38% higher** than its spot price on global exchanges

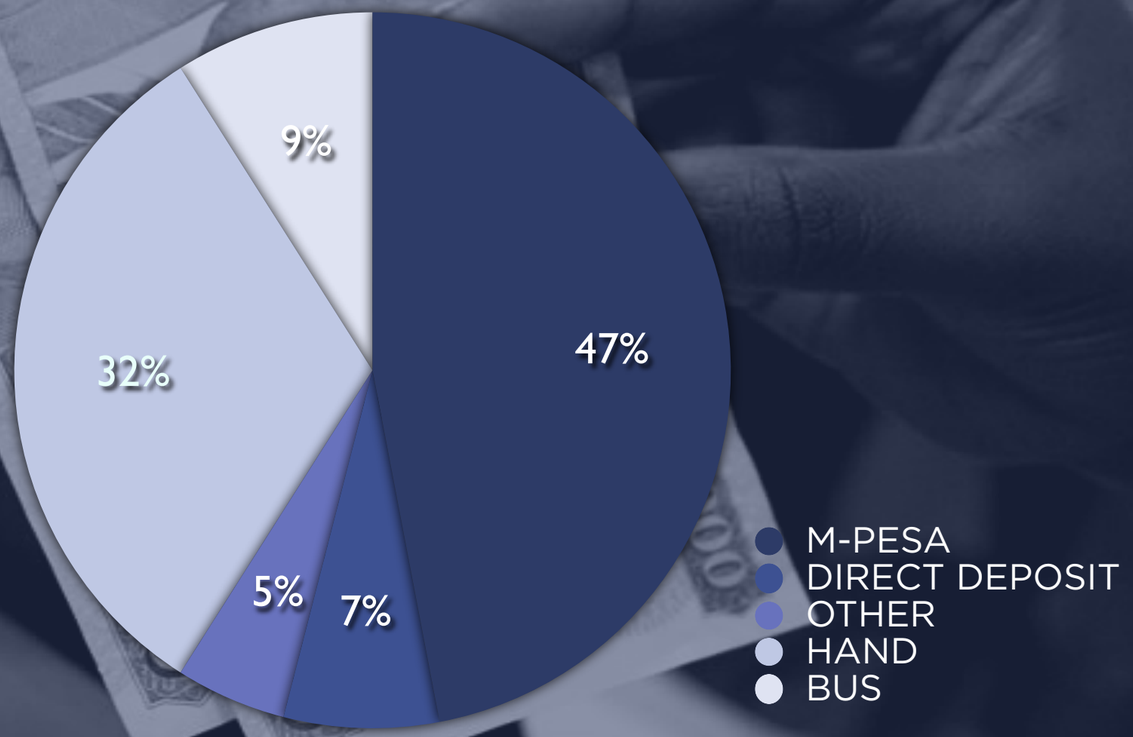


IMPLICATIONS: ZIMBABWE

- 1999 - Zimbabwe president Robert Mugabe begins redistributing private farm land, leading to a steep drop in economic productivity.
- 2000 - Mugabe **prints an excessive amount of money** to finance the Second Congo War, spending ~$22M per month.
- 2008-2009 - **Inflation climbs** to an alleged **6.5 sextillion percent**.
- 2009 - Zimbabwe abandons the Zimbabwean Dollar (Z$) and does not replace it with another fiat currency.
- Bitcoin is decentralized system which adheres to a strict set of rules and parameters - requiring a **majority network consent** to change - making it more immune to this type of manipulation and mismanagement.

IMPLICATIONS: KENYA

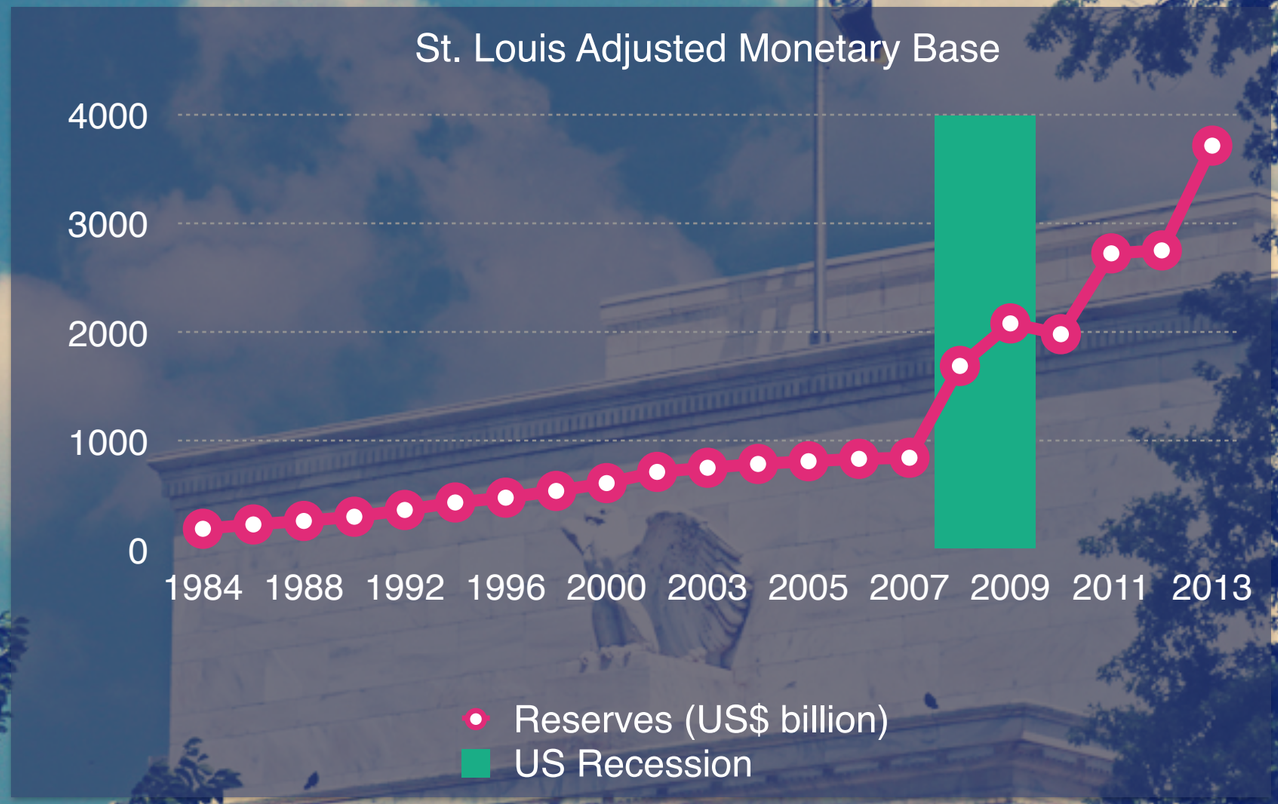
- M-PESA is a private, mobile phone-based centralized currency that facilitates money transfers
- Used by over 35M people in Kenya, Tanzania, South Africa, Afghanistan and India
- Users can buy and sell prepaid cellphone “minutes” and transfer them to pay bills, satisfy debts and make purchases
- Volume-based fee structure of ~1-15% (the smaller the transactions, the larger the fee percentage)
- In 2011, $10B (30% of Kenya’s GDP) was transferred via M-PESA on mobile phones
- Bitcoin payments, including micro-payments, are instant and free



How people in Kenya send money after the introduction of M-PESA

IMPLICATIONS: UNITED STATES

- 2008 - Global Financial Crisis
- 2009-2014 - The U.S. Federal Reserve more **triples the monetary base in five years**.
- Inflation remains low, however, much of this newly minted money is not in the system yet.
- Outcome of these policies remains to be seen.
- Bitcoin's **supply is fixed** at 21M BTC.



POSSIBILITIES

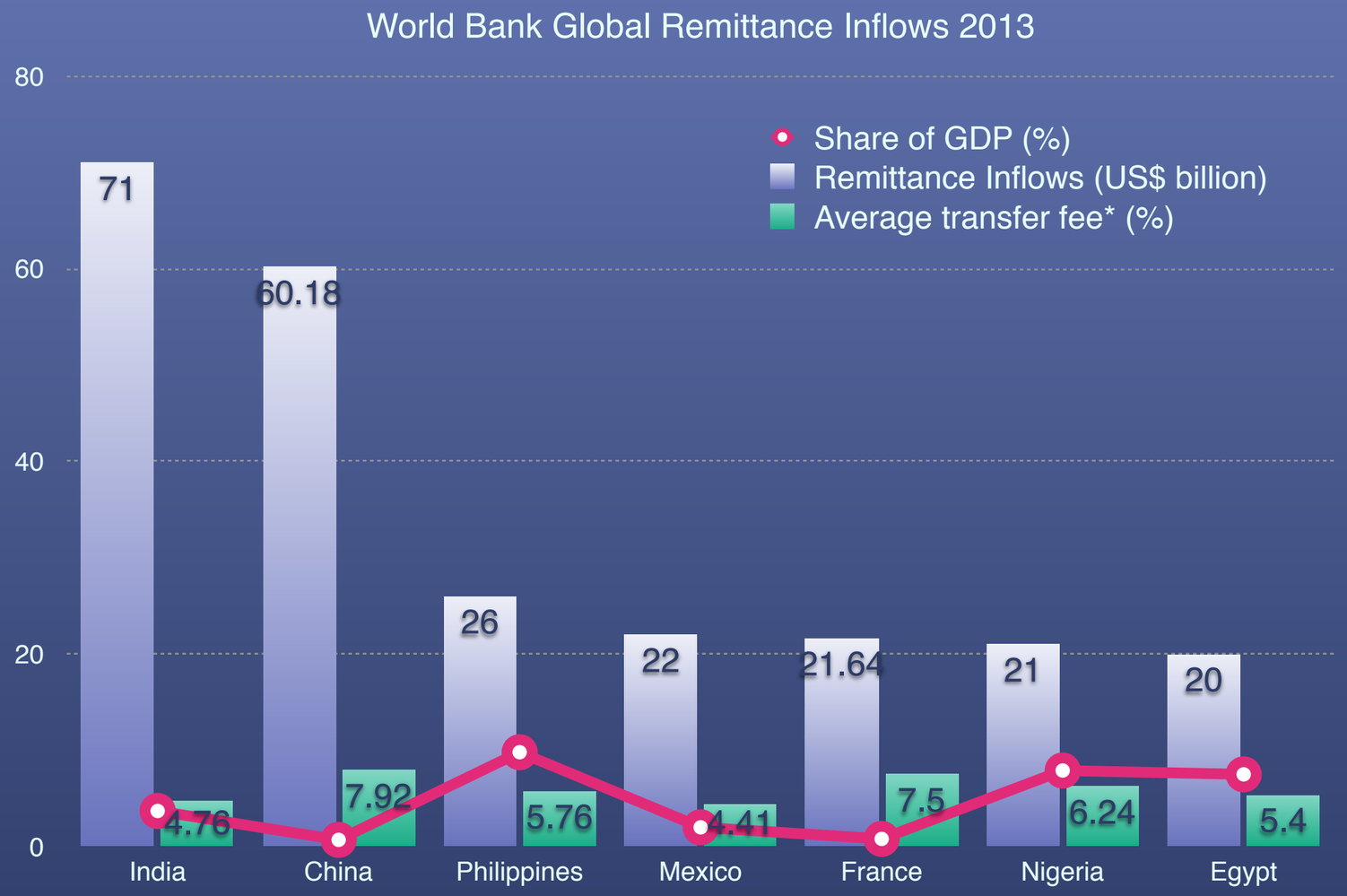
REMITTANCES

BANK THE UNBANKED

MICROPAYMENTS

POSSIBILITIES: REMITTANCES

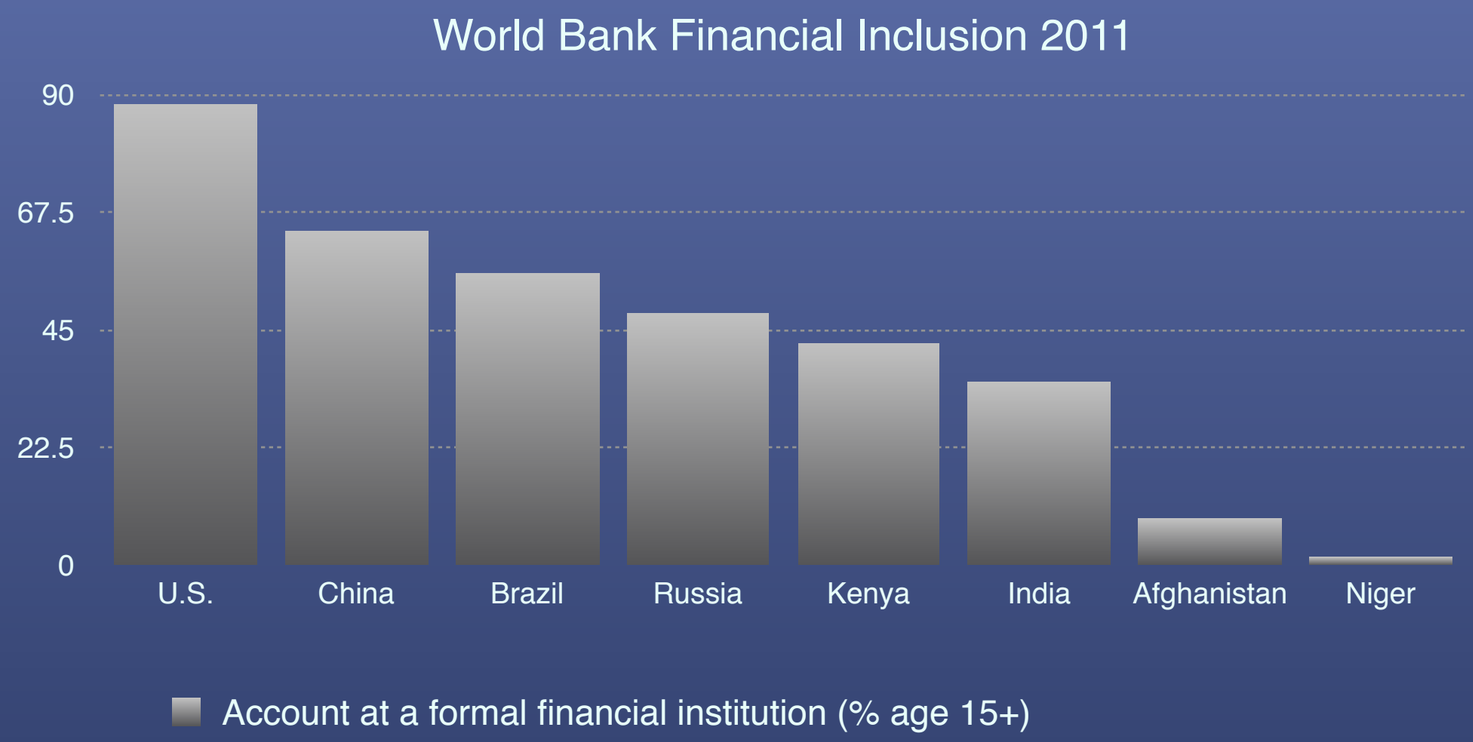
- In 2012 **remittances** hit an all time high of $534B.
- On average, global remitters pay an **8.3% transfer fee**, with some inter-African remittance fees as high as 30%.
- Bitcoin can be sent for **free** and **instantly** around the world with a data or Internet connection.



*Transfer fees based on sending US$200 from US and selecting the quickest option

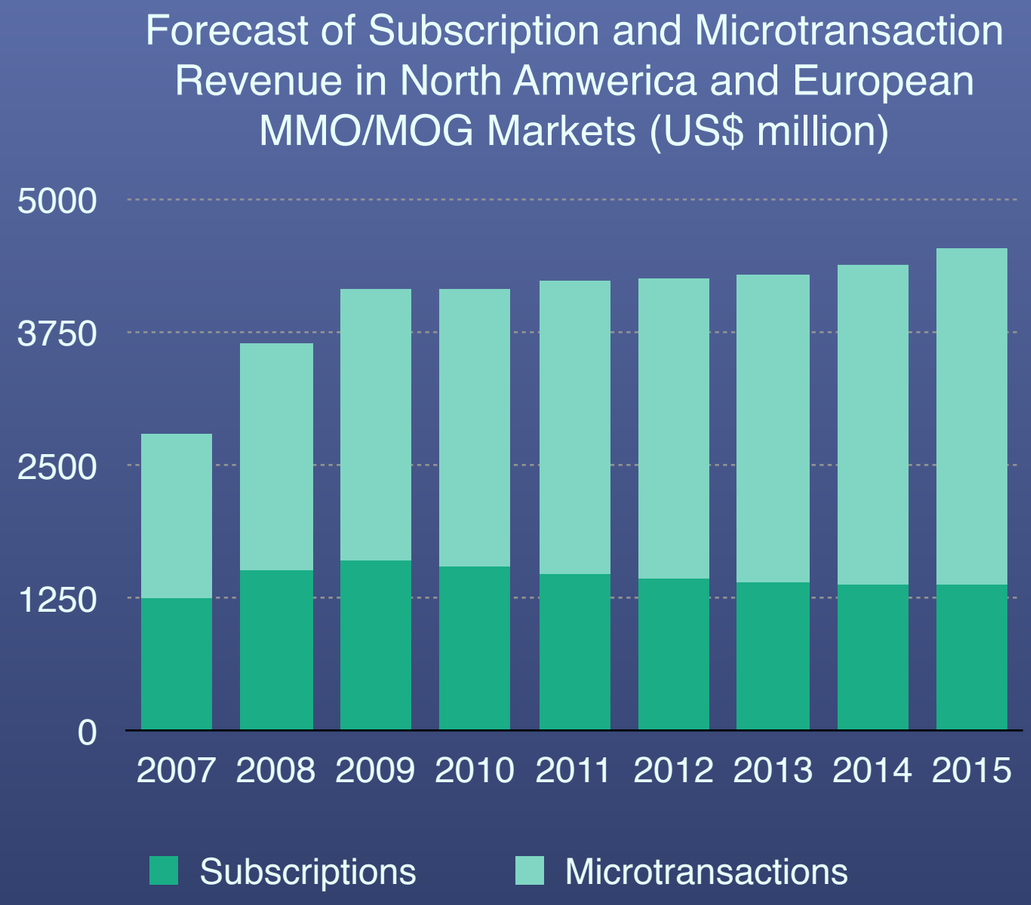
POSSIBILITIES:
BANK THE UNBANKED

- 2.5 Billion adults (half the global population) are **underbanked/ unbanked**.
- 2/3 of the unbanked do not have enough money to use a bank.
- A Bitcoin wallet allows anyone to send and receive money, much like a bank account, only quicker and without fees.
- A Bitcoin wallet is **free** - all you need is Internet access or a data connection.



POSSIBILITIES: MICROPAYMENTS

- PayPal defines a micropayment as anything less than $12 USD, while Visa defines them as less than $17 USD.
- Research shows that consumers are more willing to spend money on incremental payments as opposed to subscriptions, however, **payments less than $2 USD are impractical** given the costs of the current global banking system
- Bitcoin allows for **true micropayments** (even less than $0.01 USD) giving consumers a more dynamic and fairer offering, thereby increasing revenues and decreasing IP theft (e.g., individual article paywalls vs. monthly subscription paywalls)
- True micropayments would facilitate an **economy of micro consumption** (e.g., virtual goods, in-app purchases, gaming credits, etc.).



POSSIBILITIES:
EXCHANGE-TRADED FUND

POSSIBILITIES: REGULATION

"Our agency approaches the issue of virtual currencies without any prejudgements. A lot of people initially react to a very outside-the-box idea like virtual currencies with immediate skepticism. I think we should resist being completely overtaken by that urge. It's hard to say precisely what the future holds for virtual currency and its associated technology. Currently, there is not widespread adoption of virtual currencies among the general public. And some doubt whether there will ever be. But the same has been said about many other technologies that have since become everyday features of our lives. It's generally a difficult proposition for financial regulators to forecast technological trends. It's not something we do particularly well...**Indeed, virtual currency could ultimately have a number of benefits for our financial system. It could force the traditional payments community to "up its game" in terms of the speed, affordability, and reliability of financial transactions.**

-Ben Lawsky, *Superintendent, New York State Department of Financial Services (NYSDFS)*

FUTURE

Imagine if you could take a time machine back to the early days of the Internet:

how would you act differently?

REFERENCES

Page 3: Satoshi White Paper
Page 4: New Yorker, Motherboard, Fast Company
Page 6: P2P Foundation
Page 8: Bitcoin Wiki
Page 10-13: The Genesis Block
Page 20 BlockChain.info
Page 24: Groupe Speciale Mobile Association (GSMA)
Page 25: St. Louis Fed
Page 27: The World Bank, Send Money Africa
Page 28: The World Bank
Page 29: Digital Media Academy
Page 31: New York Department of Financial Services

IMAGES

Page 1: Stock
Page 3-4: Flickr | Stig Nygaard
Page 5-6: Flickr | Dennis Gerbeckx
Page 7: Joey De Villa
Page 8: Wikipedia
Page 9: Stock
Page 14: Getty | Chris Cheadle
Page 15: Seinit, Stock, Stock, Stock, Unknown
Page 16: Unknown, 9to5Mac
Page 17: Flickr | Kevin Meredith, iMore
Page 18: Getty, Stock, Getty
Page 19: Stock
Page 20: Flickr | fragglerocks
Page 21: Wikipedia
Page 22: Flickr | Rod Waddington
Page 23: Wikipedia
Page 24: Think M-PESA
Page 25: Flickr | Steve Thompson
Page 26: DiMola Bros, Oxfam, Unknown
Page 30: Unknown
Page 31: Mike Stimpson
Page 32: Getty
Page 33: Flickr | Pearled