
cl@b2015
BITCOINS
Reality – Fiction – Fraud : Risks & Opportunities
FIBA
FELABAN 50 años

Bitcoin 101: technology and currency

Andrea Castillo
Technology Policy Manager
Mercatus Center at GMU

MERCATUS CENTER
George Mason University

Roadmap for today

1) **Distributed cash**
   - double spending problem
   - Byzantine General's problem

2) **How does it work?**
   - public key cryptography (wallets)
   - distributed ledger of transactions (blockchain)
   - distributed computer network (miners, nodes)

3) **Benefits, Challenges, and Opportunities**

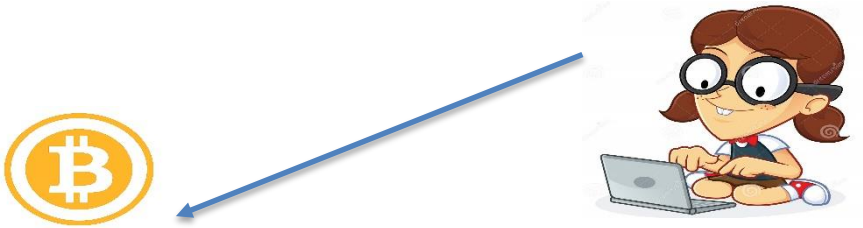
“I’ve been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party.”

November 1, 2008

MERCATUS CENTER
George Mason University

Trusted third parties are replaced by the **PROTOCOL** itself

MERCATUS CENTER
George Mason University



1 BTC 1kfjdkfjsfl38 -> 1kfjdkfjsfl357583hf
3.5 BTC 1kfjdkfjsfl357583hf -> 1dfkjr83roehskfjh
2 BTC 1dfkjr83roehskfjh -> 1kfjdkfjsfl38
1 BTC 1kfjdkfjsfl38 -> 1kfjdkfjsfl357583hf
3.5 BTC 1kfjdkfjsfl357583hf -> 1dfkjr83roehskf
2 BTC 1dfkjr83roehskfjh -> 1kfjdkfjsfl38
1 BTC 1kfjdkfjsfl38 -> 1kfjdkfjsfl357583hf

MERCATUS CENTER
George Mason University

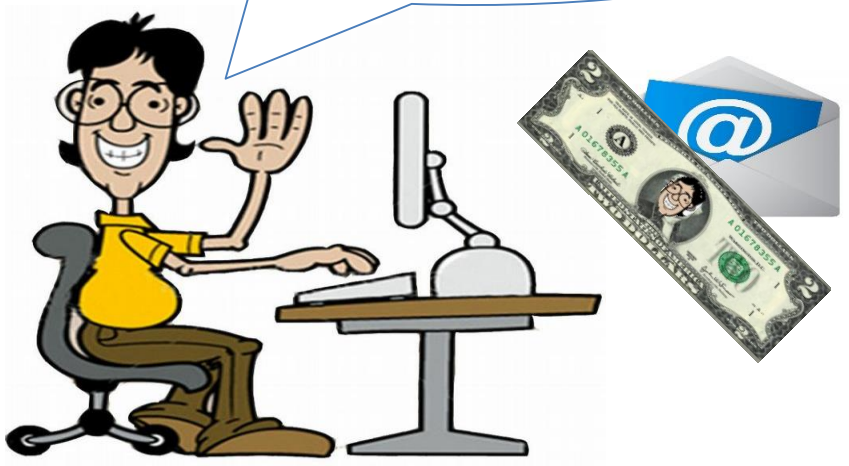
Two barriers to direct online payments: (1) the double-spending problem and (2) the Byzantine Generals problem.

Double spending: how to achieve scarcity in a trustless environment?

MERCATUS CENTER
George Mason University

The “double spending” problem

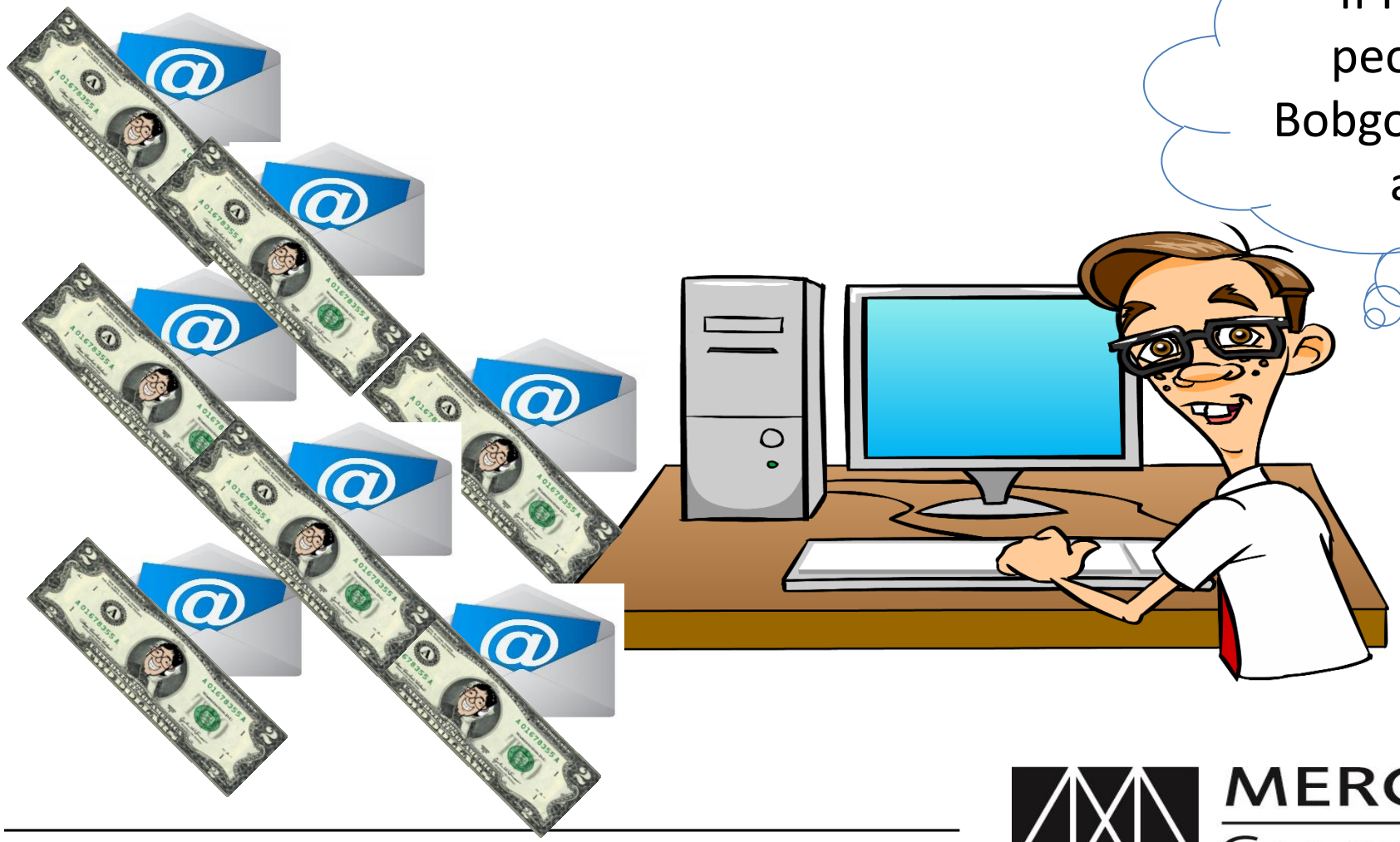
I’ll email you a payment in my new e-currency, Bobgold.



As an attachment? Okay I guess.

MERCATUS CENTER
George Mason University

The “double spending” problem



MERCATUS CENTER
George Mason University

Byzantine General: how to achieve consensus in a trustless environment?

MERCATUS CENTER
George Mason University

The “Byzantine Generals” problem

- It is very difficult to arrive at consensus in an environment without trust.
- Coding messages only works, but only to a point
- Coordinating a true payments ledger online is open to “attack” – falsification, fraud

The “Byzantine Generals” problem

MERCATUS CENTER
George Mason University

Bitcoin achieves digital scarcity and consensus with public key cryptography and distributed ledger-keeping (the blockchain)

MERCATUS CENTER
George Mason University

Public key cryptography (Bitcoin)

- Public and private Bitcoin key – like email address and password
- Gives us a way to verify identity without relying on a third party.
- He who controls the private key controls the bitcoins

Distributed ledger-keeping (blockchain)

- Like BitTorrent: no one server runs/controls transfer
- Network of connected computers – “p2p”
- “Nodes” running “Bitcoin” software
- What are those computers doing? Math! Validate and keep track of transfers

Mining

- Distributed computers apply processing power to solve math problems and verify blocks
- “Minting” bitcoins is the incentive
- 21 million bitcoin supply cap
- No one miner knows details of any one transaction, but all contribute to verification of ledger

Putti

Send 1BTC from my wallet to Alice's

BOB'S SE

Valid!

Square!

ALICE'S SECRET PRIVATE KEY

Public ledger of transactions

1 BTC DFLGKJSLKG -> DLFKGJSDLFG

3.5 BTC DLFKGJSDLFG -> FGGGDS

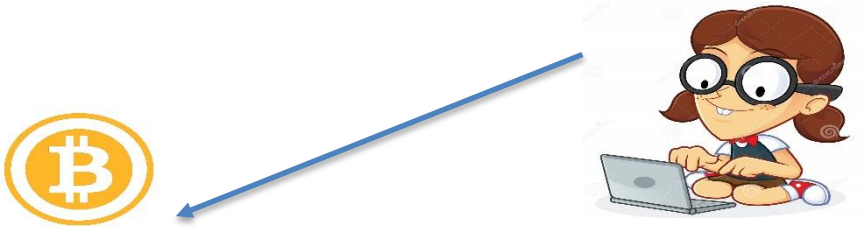
0.5 BTC FGGGDS -> DLFKGJSDLFG

1 BTC 1HneLqnWhXYe1kSXTDQay1WpdR734R2Wqy -> 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

BOB'S BITCOIN WALLET:
1HneLqnWhXYe1kSXTDQay1WpdR734R2Wqy

ALICE'S BITCOIN WALLET:
1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

MERCATUS CENTER
George Mason University



1 BTC 1kfjdkfjsfl38 -> 1kfjdkfjsfl357583hf
3.5 BTC 1kfjdkfjsfl357583hf -> 1dfkjr83roehskfjh
2 BTC 1dfkjr83roehskfjh -> 1kfjdkfjsfl38
1 BTC 1kfjdkfjsfl38 -> 1kfjdkfjsfl357583hf
3.5 BTC 1kfjdkfjsfl357583hf -> 1dfkjr83roehskf
2 BTC 1dfkjr83roehskfjh -> 1kfjdkfjsfl38
1 BTC 1kfjdkfjsfl38 -> 1kfjdkfjsfl357583hf

MERCATUS CENTER
George Mason University

What is a bitcoin?

- Fundamentally, a private key

- E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4 45 32 13 30 3D A6 1F 20 BD 67 FC 23 3A A3 32 62

- A digital representation of a claim to data on the blockchain

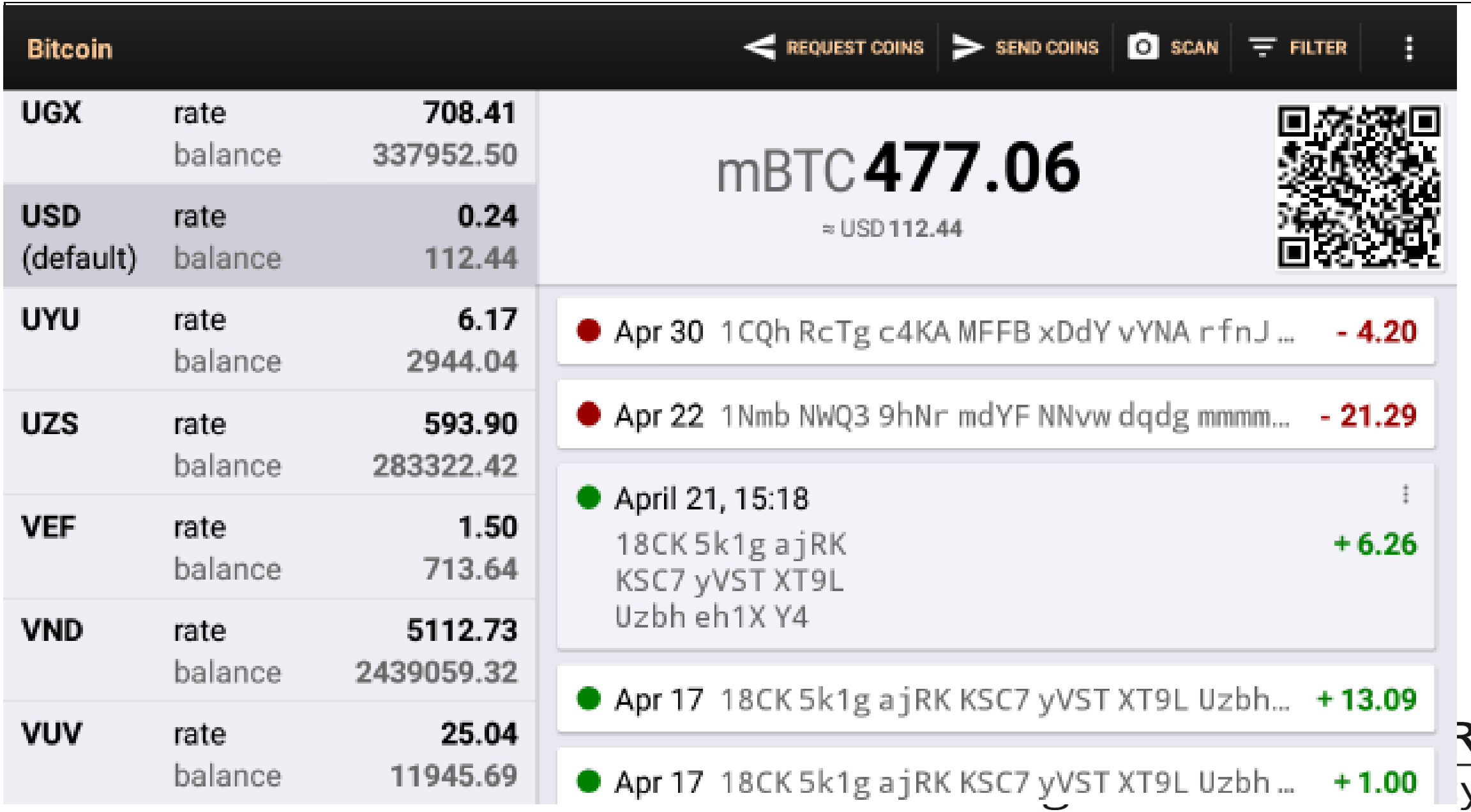
Benefits

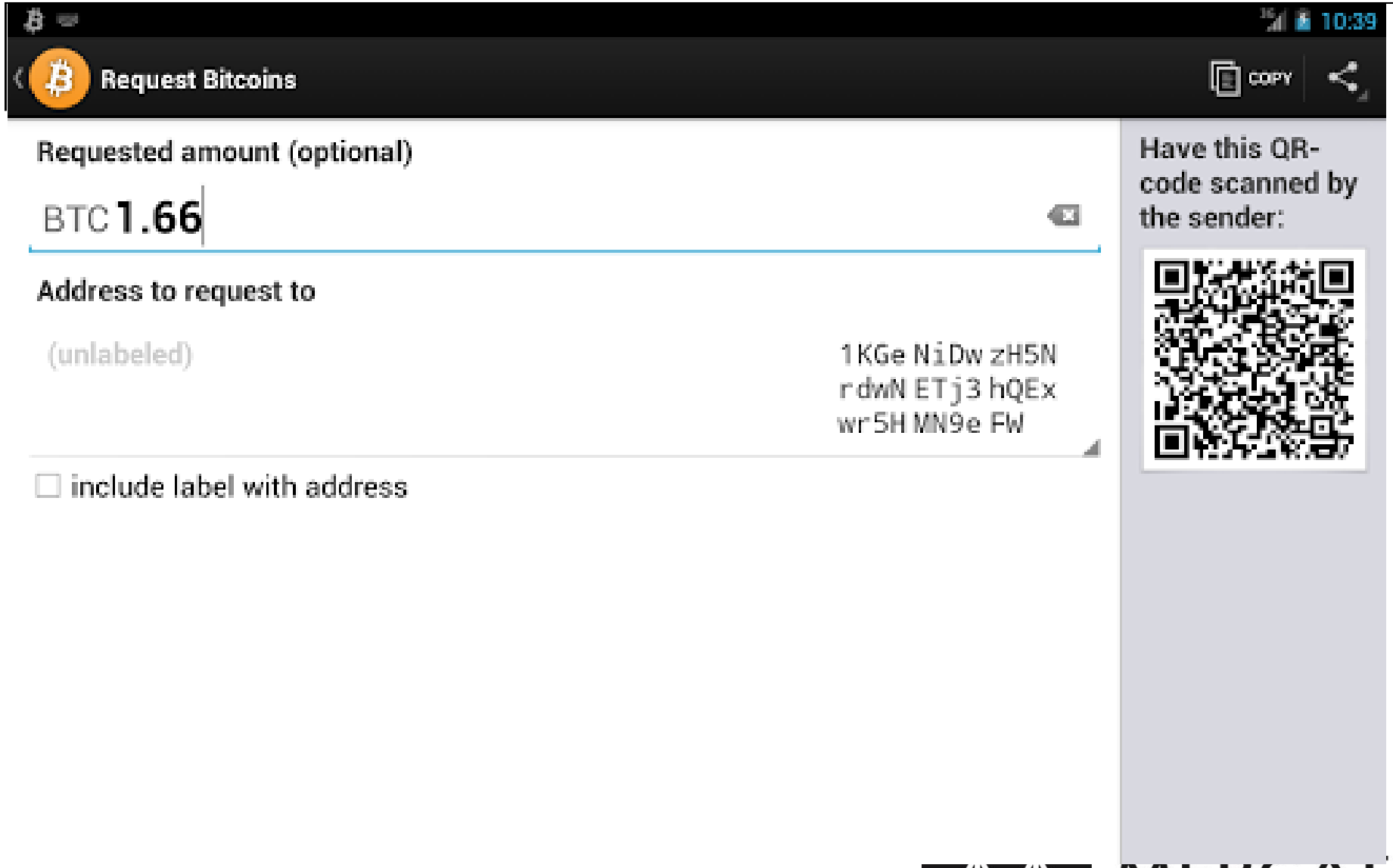
- Personal control – a “PUSH” technology
- Exit options – Greece, Argentina
- Censorship proof – Wikileaks
- Affordable – remittances, micropayments
- “Programmable money” – smart contracts, identity, titling, arbitration…

MERCATUS CENTER
George Mason University

A balance

- The cat is out of the bag! Technology cannot be shut down (unless you shut down the Internet)
- Do not want a situation where law-abiding users cannot receive benefits, while criminals still use it for ill
- Conversations between developers, users, industry, and regulators – how to reap these benefits while addressing concerns?


Bitcoin
REQUEST COINS
SEND COINS
SCAN
FILTER
UGX rate 708.41
balance 337952.50
USD (default) rate 0.24
balance 112.44
UYU rate 6.17
balance 2944.04
UZS rate 593.90
balance 283322.42
VEF rate 1.50
balance 713.64
VND rate 5112.73
balance 2439059.32
VUV rate 25.04
balance 11945.69
mBTC 477.06
≈ USD 112.44
Apr 30 1CQh RcTg c4KA MFFB xDdY vYNA rfnJ ... - 4.20
Apr 22 1Nmb NWQ3 9hNr mdYF NNvw dqdg mmmm... - 21.29
April 21, 15:18
18CK 5k1g ajRK
KSC7 yVST XT9L
Uzbh eh1X Y4
+ 6.26
Apr 17 18CK 5k1g ajRK KSC7 yVST XT9L Uzbh... + 13.09
Apr 17 18CK 5k1g ajRK KSC7 yVST XT9L Uzbh ... + 1.00


10:39
Request Bitcoins
COPY
Requested amount (optional)
BTC 1.66
Address to request to
(unlabeled)
1KGe NiDw zH5N
rdwN ETj3 hQEx
wr5H MN9e FW
include label with address
Have this QR-code scanned by the sender:

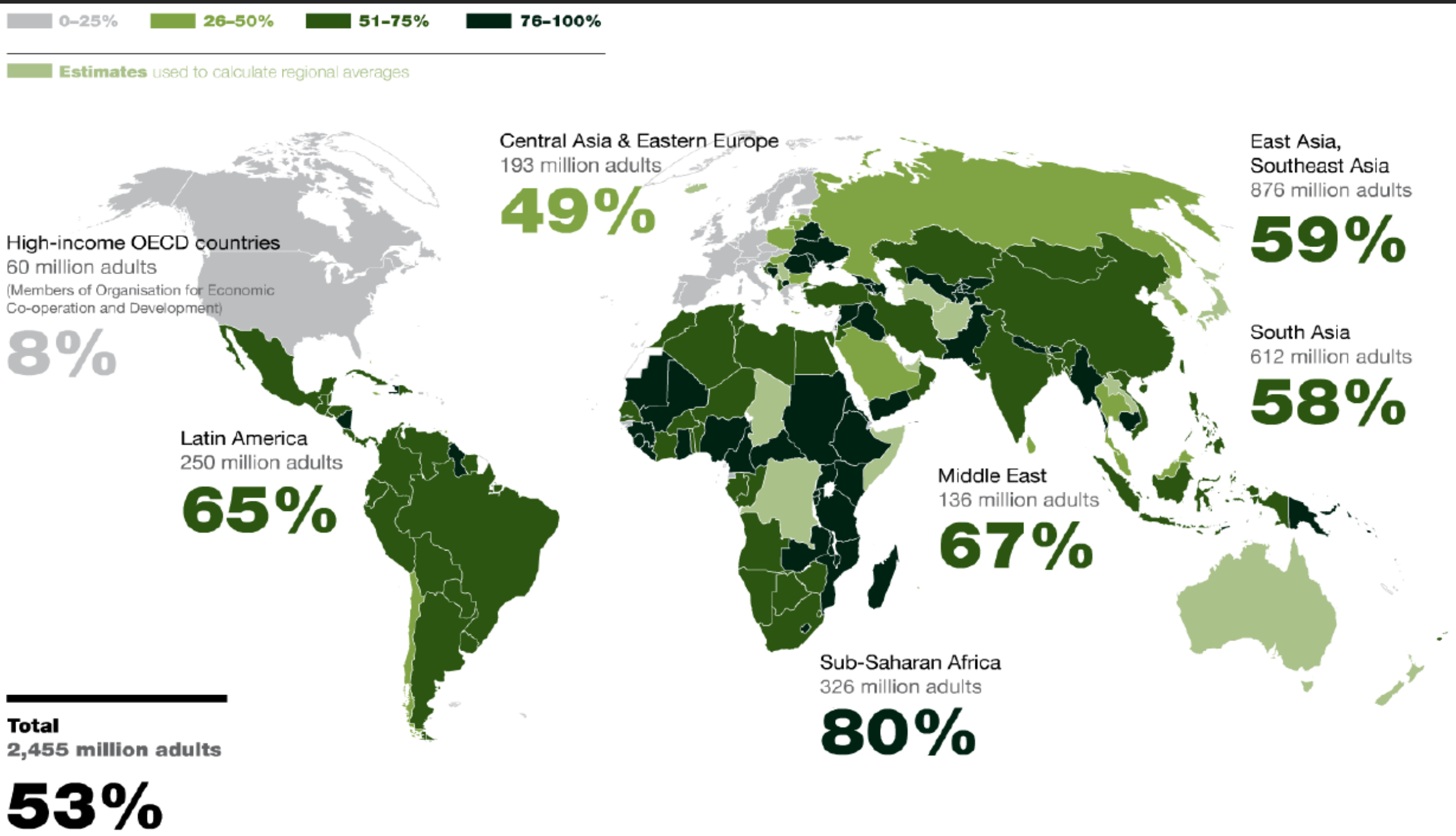
September 3, 2015

Miami

Opportunities RISKS & Regulation

of Bitcoin & Cryptocurrencies

@JuanLlanos


0–25%
26–50%
51–75%
76–100%
Estimates used to calculate regional averages
High-income OECD countries
60 million adults
(Members of Organisation for Economic Co-operation and Development)
8%
Central Asia & Eastern Europe
193 million adults
49%
East Asia, Southeast Asia
876 million adults
59%
South Asia
612 million adults
58%
Latin America
250 million adults
65%
Middle East
136 million adults
67%
Sub-Saharan Africa
326 million adults
80%
Total
2,455 million adults
53%

blockchain

blockchain 2.0

The **Blockchain Wars**

permissioned vs. permissionless
censorship-resistant vs. censorable
token vs. no token
financial vs. non-financial
open vs. closed
public vs. private

identity
money

sovereignty
property

PARADIGMS
questioned

security
governance

law
regulation

RETHINK

REDEFINE

REINVENT

Risks & Rewards

Santander: Blockchain Tech Can Save Banks $20 Billion a Year

Yessi Bello Perez (@yessi_kbello) | Published on June 16, 2015 at 12:15 BST

NEWS

684 310 31 244 0

Blockchain technologies could reduce banks' infrastructural costs by $15-20bn a year by 2022, a new report from Santander InnoVentures claims.

The FinTech 2.0 Paper, produced in collaboration with Oliver Wyman and Anthemis Group, says distributed ledger technology could save banks money by eliminating central authorities and bypassing slow, expensive payment networks.

Beyond payments, its authors identify other areas of potential for distributed ledgers, noting:

Potential **Benefits**

- *Reduced* ***physical infrastructure***
- *Coordination via* ***one distributed database***
- *Fewer front and back office inefficiencies*
- ***Real-time Settlement*** */ No commitment Risk*
- ***Real-time auditing***
- *Some uses*: settlement, custody, IPO & debt issuance, OTC collateral, margining, repo

Blockchain **R&D**

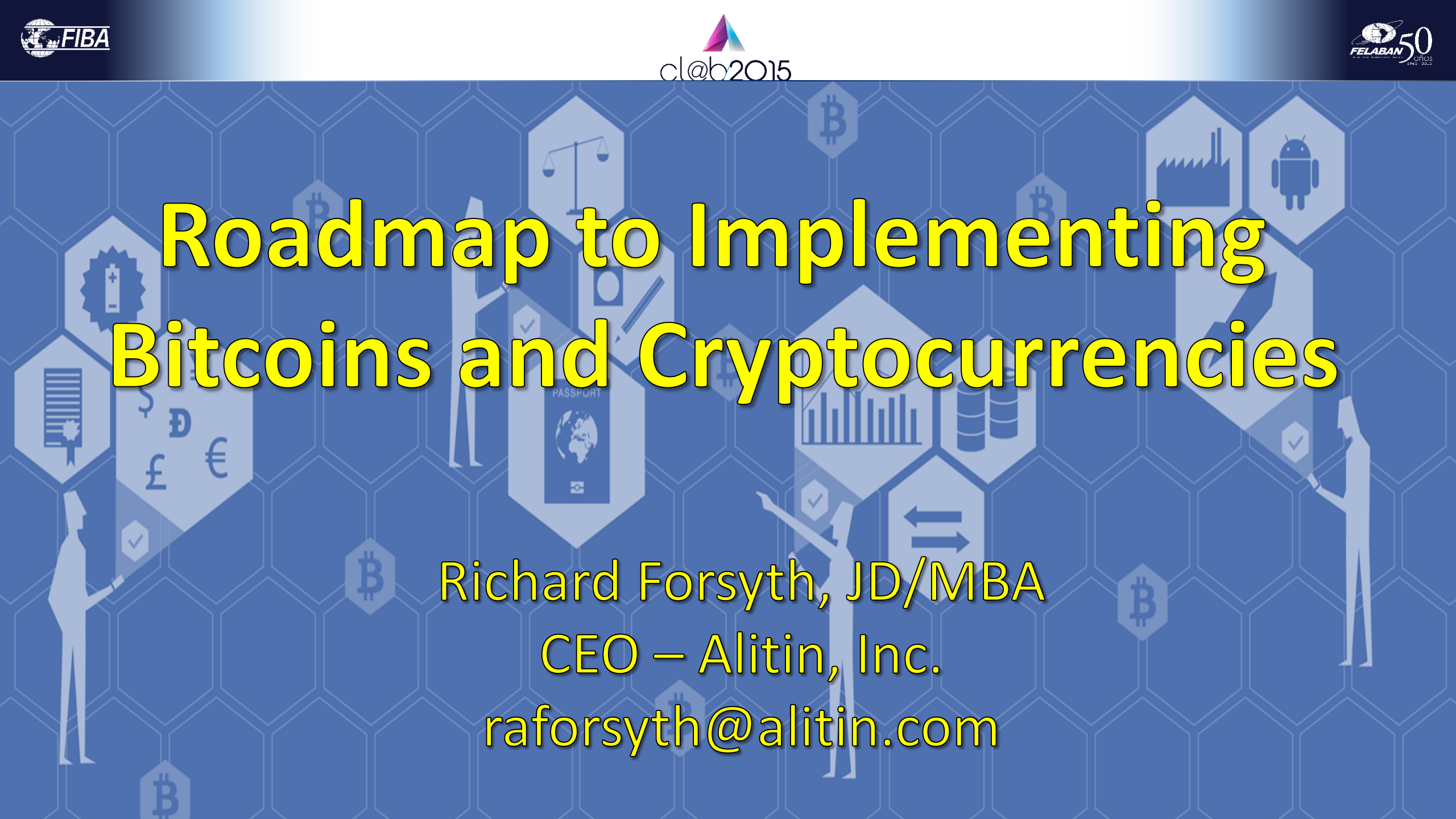
RBS **&** CBA *Ripple trial*
Citi *Blockchain Initiative*
UBS *Blockchain initiative*
Barclays *Lab + partnership with Safello*
LHV Bank (Estonia) *issuing receivables via colored coins*
HSBC *Innovation Lab*
SWIFT *Blockchain research challenge*
NASDAQ
IBM *Blockchain Initiative*

IBM-Samsung *IoT Partnership*
ING, ABN Amro, Rabobank
Deloitte, EY, PwC
Fidor Bank *Ripple integration*
CIBC *pilot projects*
Honduras *real estate records*
Greek Island *gold-backed crypto-currency*
UK *research and state support*
NYSE, USAA, BBVA *investments*
USAA *blockchain research*

Source: Constance Choi

"You should be taking blockchain technology as seriously as you should have been taking the development of the Internet in the early 1990s."

Roadmap to Implementing Bitcoins and Cryptocurrencies



Richard Forsyth, JD/MBA
CEO – Alitin, Inc.
raforsyth@alitin.com

Regulatory Environments

amazon

facebook

Google

coinbase

CIRCLE

EST 2011
BITSTAMP
SECURE TRADING AND MONEY PAYMENT


A DIGITAL ARMS RACE


SOCIETE
GENERALE


UBS


BARCLAYS

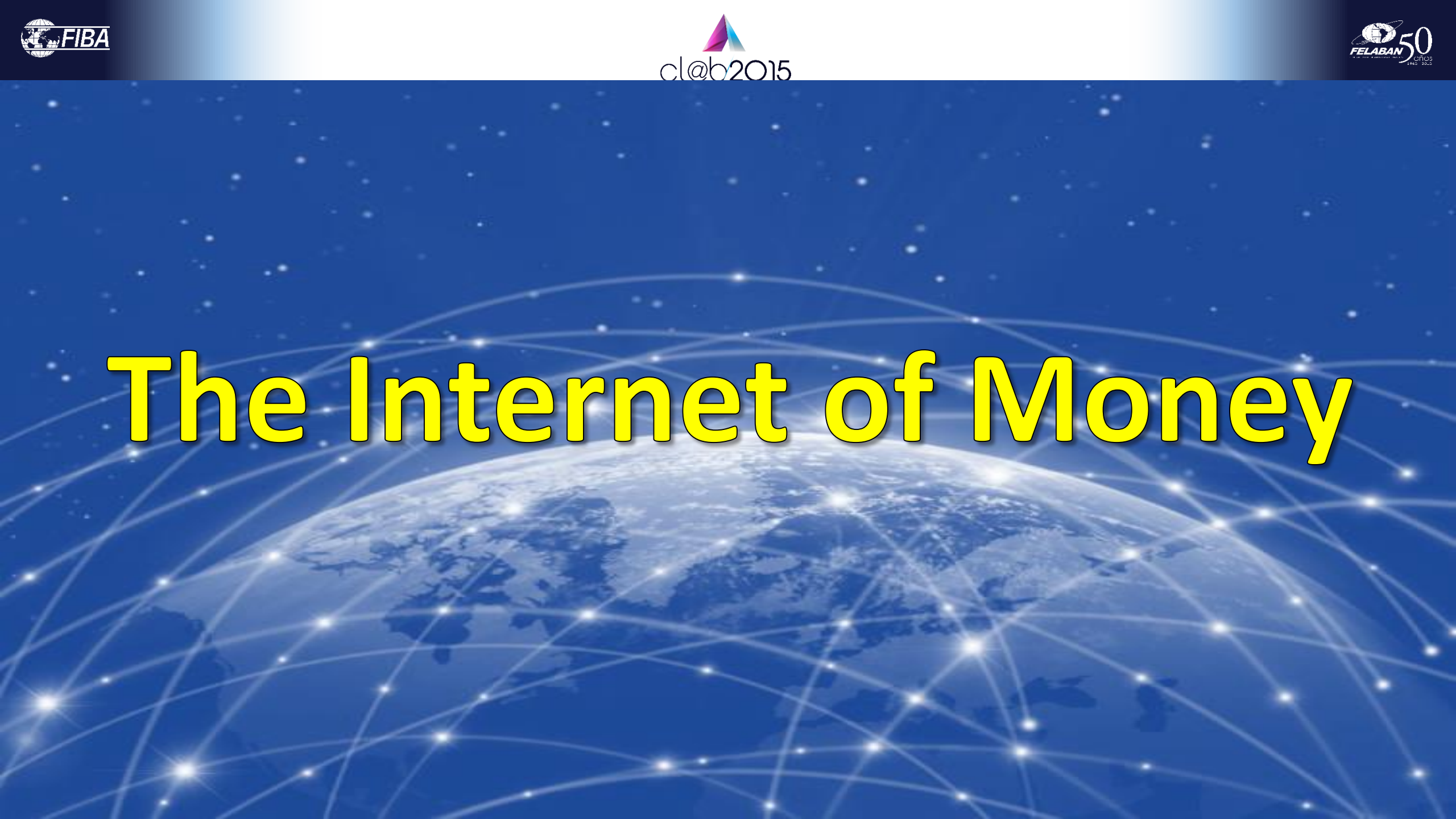

Goldman
Sachs


citibank


BNP PARIBAS


Standard
Chartered


Banco
Santander


FIBA
cl@b2015
FELABAN 50 años
The Internet of Money

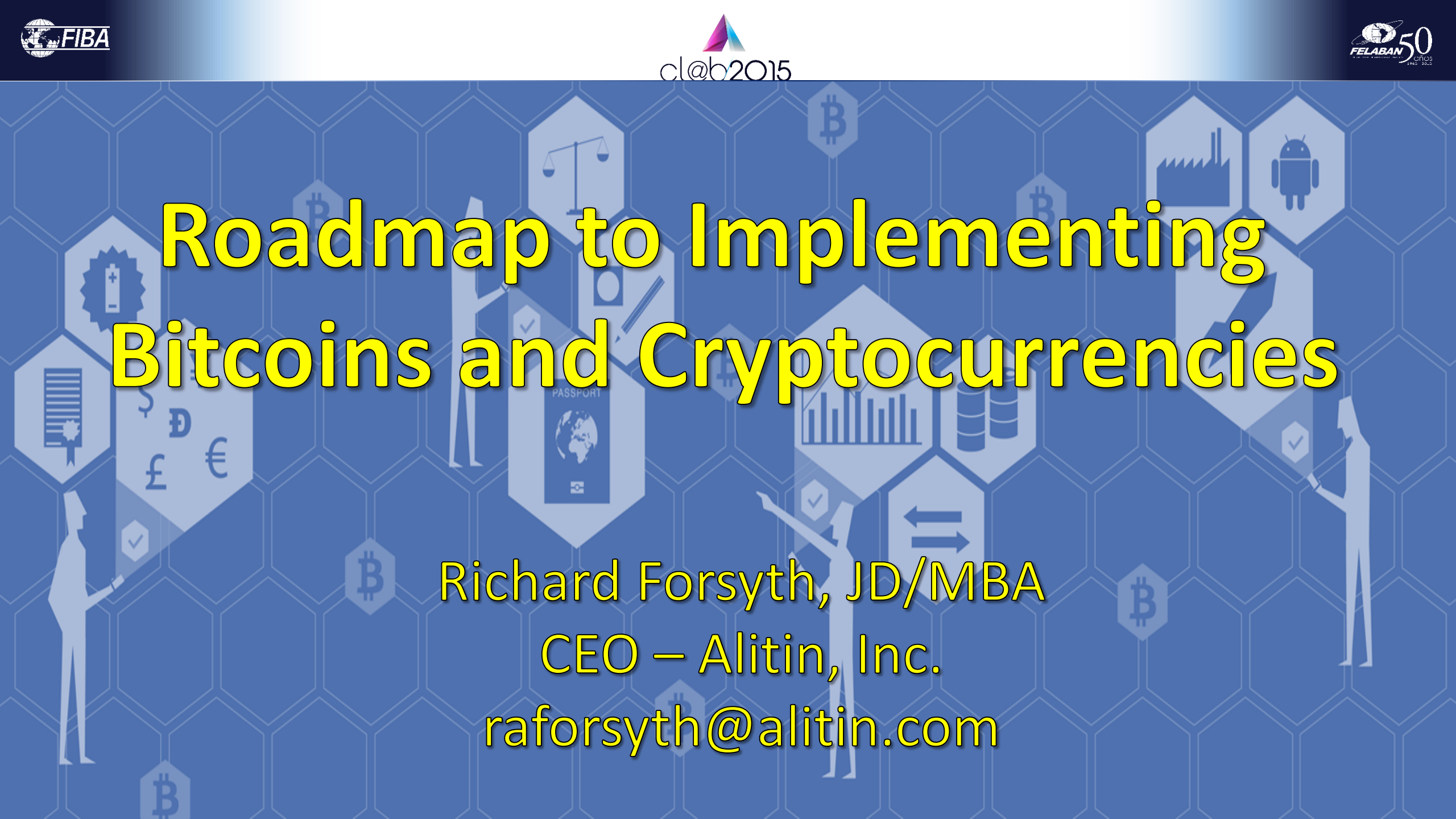
The Great De-Banking

How Can a Bank Keep Up?


Change is Hard.
So what?


THE UNITED STATES OF AMERICA
K43057691C
WASHINGTON, D.C.
ONE
DOLLAR

Roadmap to Implementing Bitcoins and Cryptocurrencies



Richard Forsyth, JD/MBA
CEO – Alitin, Inc.
raforsyth@alitin.com

Opportunities

RISKS &

Regulation

of Bitcoin & Cryptocurrencies

digital currency

virtual currency

crypto-assets

Risks & Stakeholders

Risk Areas	Stakeholders	Goals
• operational	• federal agencies	• safety
• credit	• state agencies	• soundness
• money laundering	• investors	• security
• terrorist financing	• consumers	• privacy
• information loss	• employees	• crime prevention
• Liquidity	• society	• health
• fraud		• integrity
• identity theft		

Regulation → Inevitable, yet **valid**

Compliance → Onerous, yet **valuable**

Smart Entrepreneurs
Enlightened Policy-makers, Regulators, Leaders

KNOW IT
WORK TOGETHER
FOCUS ON THE GOALS

Reasons for Regulating **Financial Intermediaries**

CONSUMER PROTECTION

ML & TF PREVENTION

SYSTEMIC RISKS

TAXATION

Bitcoin → Regulated Before Born

"transmission of money *or value*"

"cash *or* monetary *equivalent*"

"value that substitutes for currency"

Financial Intermediaries
Risk Areas

Anti-Money Laundering (**AML**)

Countering the Financing of Terrorism (**CFT**)

Privacy and Information Security (**InfoSec**)

Safety and soundness (**S&S**)

Consumer disclosures & support (**CP**)

Anonymity = Anathema

- Anonymous **identification**
- No **value limits**
- Anonymous **funding**
- No transaction **records**
- **Wide** geographical **use**
- No **usage limits**

Cash features

*FATF Report on New Payment Methods (**2006**)*

Myths

Anonymous

Untraceable

“Invisible to law enforcement and the taxman”

enhanced **surveillance** and **control**

Consumer “Advisories”

Lebanon, **Germany**, Hong Kong, **Belgium**, Indonesia, **UK**, Russia, **Estonia**, US-WI, **Greece**, Israel, **Brazil**, Philippines, **US-TX**, Germany, **US-CA**, US-NV, **Canada**, US-ID, US-SEC, **US-IN**, US-NM, **Europe-CB**, Argentina, **US-ME**, Netherlands, **Russia**, US-MI, **France**, Japan, **Australia**, UK, **Serbia**, Portugal, **Norway**, France, **Canada**, Ireland

2014 EBA Opinion

Regulatory **Arbitrage**

conservative vs. progressive
aggressive vs. permissive
formal vs. substantial
restrictive vs. expansive
misguided vs. enlightened

Thank You

@JuanLlanos