Cryptocurrency and Blockchain as Agents of Social Change

Bebo White

SLAC National Accelerator Laboratory/
Stanford University

bebo@slac.stanford.edu

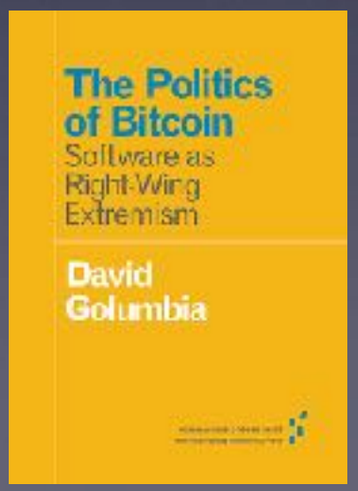
Some caveats (1/2)

- I am
  - a technologist and not an economist or sociologist
  - fascinated by the technological and mathematical underpinnings of cryptocurrencies and blockchain
  - primarily focussed on Bitcoin and Ethereum
  - convinced that there can be great social benefit from the technology
  - never going to try and convince anyone to purchase cryptocurrencies
  - always open to brainstorming and discussion
  - ….an owner of cryptocurrency

Some caveats (2/2)

- when I tell people that I research/discuss/advocate(?) cryptocurrency/bitcoin and blockchain, they usually think that
  - I'm a techie/computer nerd/idealist academic, etc.,
  - I'm a hacker or criminal
  - I am unaware (or willing to overlook) the social and/or environmental issues
- why do people think this?

Why do they think this?



HKU March 2018

Here's a weird one -

"Speaking of gold and cryptocurrencies, the LBMA conducted several interesting polls on which of the two assets would benefit the most in certain scenarios. In one such poll, **attendees overwhelmingly said the gold price would skyrocket in the event of a conflict involving nuclear weapons. Bitcoin, meanwhile, would plummet, according to participants—which makes some sense.** As I pointed out before, trading bitcoin and other cryptos is dependent on electricity and WiFi, both of which could easily be knocked out by a nuclear strike. Gold, however, would still be available to convert into cash."

LBMA = London Bullion Market Association

And even weirder…

The Telegraph HOME | NEWS | S

Technology

News | Reviews | Opinion | Internet security | Social media | Apple | Google | New

Technology

Steven Seagal becomes face of new cryptocurrency Bitcoiin2Gen

share 0

Steven Seagal has endorsed new cryptocurrency Bitcoiin2Gen. CREDIT: AP

By Mark Molloy

21 FEBRUARY 2018 • 4:37PM

Steven Seagal's multifarious career has taken him from Hollywood to promoting Russian firearms, but his latest move into the world of cryptocurrency may be his most surprising to date.

"[We] can best interpret the different forms money takes – the money commodity, coins, convertible and inconvertible paper currencies, various credit moneys, etc. – as an outcome of the drive to perfect money as a frictionless, costless and instantaneously adjustable 'lubricant' of exchange while preserving the 'quality' of money as measure of value"

David Harvey

A view of money by a cryptocurrency enthusiast (1/3)

- money is a set of shared rules within a community for exchanging value
- these rules are historically defined and regulated for governments and banks and the bounds within which communities communicate with one another
- rules are subject to change due to historical and social phenomena
- cryptocurrencies are simply rules (software) that are relevant to the global online community

A view of money by a cryptocurrency enthusiast (2/3)

- as long as all parties in a community share and abide by the agreed rules, *money* can take on a rich and diverse range of characteristics
- cryptocurrency to/from fiat currency bridges multiple communities where rules might overlap or be inconsistent
- p*rogrammable money* involves rules which define how and when value can be exchanged according to how the parties want to interact

A view of money by a cryptocurrency enthusiast (3/3)

- so, according to these definitions, *BTC is money* even though it
  - is intangible (just a collection of bits stored in an online ledger)
  - is not backed by something tangible, e.g., gold, silver
  - is not controlled by some central authority, e.g., requires no intermediary

What exactly is Bitcoin?

- "Bitcoin" is the protocol; "bitcoins" are the units (BTC)
- designed for an "networked society" using network technologies e.g., mobile telephones
- decentralized and independent of "state/fiat currencies"
- can be used for anonymous transactions like fiat currencies - unlike credit cards, PayPal, etc.
- potential to revolutionize E-commerce - online exchange, no specific currency, micro payments
- easily convertible to "state/fiat currencies"

Satoshi Nakamoto saw a way

- "The network is robust in its unstructured simplicity. Nodes work all at once with little coordination"
- A distributed, peer-to-peer network of payments ledgers (non-centralized)
  - Impossible (?) to forge/modify - based on rigorous technology and techniques
  - Doesn't allow double-spending and provides proof-of-payment (non-repudiation)
  - Supported by "the power of the crowd"
- Not based on dollars, euros, pounds, etc., but a currency "for the digital age" - bank-free, government-free, empowering

Bitcoin/cryptocurrency

- is not science fiction
- is not a computer science fantasy
- is not strictly the domain of criminals and hackers
- is perfectly suited for a digital, networked, mobile world
- has disrupted the financial establishment and contributed to the birth of FinTech
- frightens some and/or threatens the status quo - “Bitcoin and blockchain are a flawed solution to a problem that does not exist” (Izabella Kaminska, FT Alphaville)

“Technology is amoral. It is neither good nor bad. It is up to all of us - not just scientists, government officials, and people fortunate enough to lead foundations - to think hard about these new technologies and how they should and should not be used.” - Bill Gates

and so it is for cryptocurrencies

A little tech - how Bitcoin works (addresses/keys)

- Bitcoin (BTC) is based on public/private key encryption
  - well-established method; mathematically robust; used in many common applications, e.g., https
  - a secret passphrase is used to mathematically generate a public address and a private address (key pair)
    - deriving one address from the other is mathematically unfeasible
- address might look something like this: 1BBsbEq8Q29JpQr4jygjPof7F7uphqyUCQ
- to send/spend BTC, user specifies the recipient's public address and amount of BTC
- to receive BTC, provide the payer your public address
- your BTC wallet (or some other storage device) knows your private address
- addresses are not registered to users; a user can have a different address for every transaction

- consider all the horror stories we hear about cryptocurrencies…
- what about some good stories?…and not just ones about people who have made a lot of money

Cryptocurrencies are more than just about payments

- Empowerment
- Transparency

HKU March 2018

We talked about exchange of value within communities

- suppose those communities were
  - the disenfranchised/unbanked
  - those with “dead capital”
  - those who are victims of failed national financial systems
  - those where the “chain of value” is subject to theft or corruption
  - those in desperate need of value following natural or man-made disasters
  - those who are part of “the micro-economy”
- **money is power!**

Disintermediation

- third parties are no longer needed to
  - establish identity or prove creditworthiness
  - distribute media
  - mediate communication between parties
  - mediate transfers of value

The disenfranchised/ unbanked (1/2)

- it is estimated that 2.5 billion people are unbanked - why?
  - qualifications/restrictions
  - regulations
  - trust/fear
- they are therefore
  - limited in their financial transactions
  - potential victims
- cryptocurrencies **may** be one of many possible solutions

The disenfranchised/ unbanked (2/2)

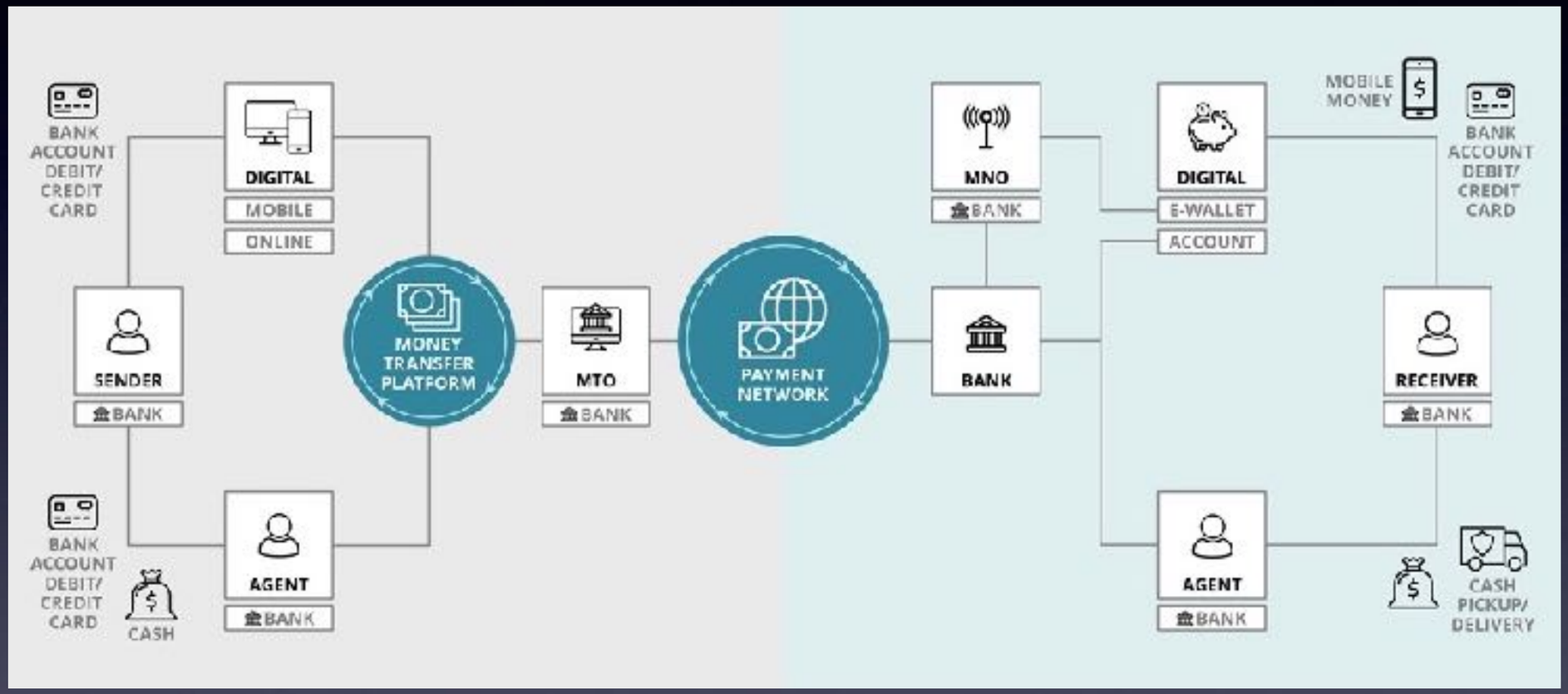
- a means to facilitate low-cost remittances for those seeking to transfer small amounts of money internationally
- a means for an otherwise excluded individual to have a decentralized global bank account accessible by downloading an open source wallet from the Internet vs. having to set up an account with a financial institution
- does require conversion mechanisms for fiat currencies at both end points
- the basis for a richer set of financial services

Cryptocurrencies are a part of a social financial revolution

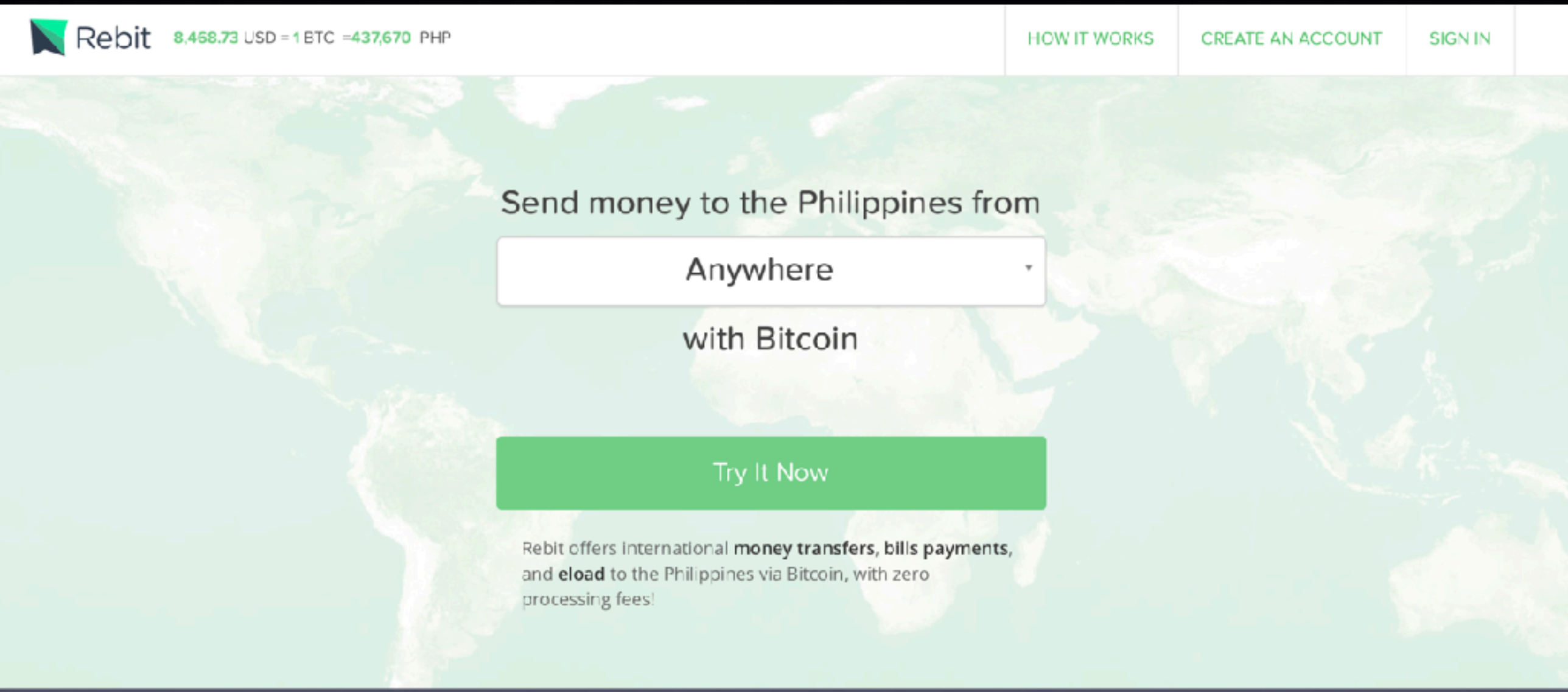
- "Some people are fed up with the centralized banking system"
- "Paying with bitcoin makes moving money across borders easy and with low transaction fees and some degree of anonymity"

Claudio Orlandi
Aarhus University

For example - the cross-border remittance ecosystem



Ref: The Aite Group



HKU March 2018

Disaster relief

- immediate and direct transfer of financial support when banks are inaccessible or aid agencies and/or governments are too slow to respond

- tracking of donations to insure that they are received by the intended recipients

- may have infrastructural issues

- empowering a “relief economy”

GSMA Mobile Money Program

GSM *(Groupe Spéciale Mobile)* Association

HKU March 2018

All it really takes

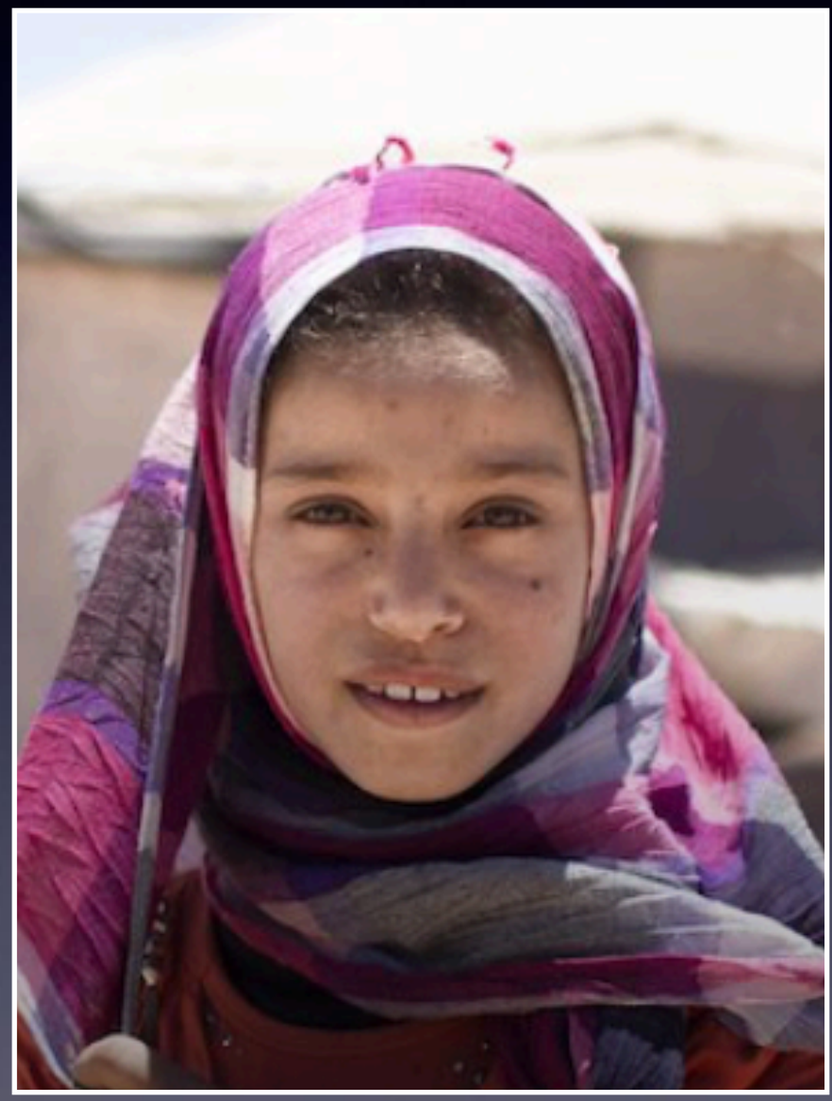
HKU March 2018

UN test - refugees in Jordan

- cryptographically unique coupons/retinal-scanning support distribution of local currency to individuals with multiple refugee camps

- allows for greater assurances that value is being provided to those in actual need

- reduces overhead in disbursement while at the same time increases transparency



Failed financial systems

AMERICAS

Venezuela Launches Virtual Currency, Hoping to Resuscitate Economy

Leer en español

By [redacted] and NATHANIEL POPPER FEB. 20, 2018

President Nicolás Maduro of Venezuela spoke at a news conference in Caracas on Tuesday about the launch of an oil-backed digital currency called the petro. Federico Parra/Agence France-Presse — Getty Images

RELATED COVERAGE

Russia and Venezuela's Plan to Sidestep Sanctions: Virtual Currencies JAN. 3, 2018

As Venezuela Collapses, Children Are Dying of Hunger DEC. 17, 2017

White House Raises Pressure on Venezuela With New Financial Sanctions AUG. 25, 2017

MEXICO CITY — With Venezuela suffering one of the most severe economic collapses of modern times, the beleaguered administration of President Nicolás Maduro announced on Tuesday that it had begun a presale of virtual currency backed by the nation's vast petroleum reserves.

TECH

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

Cash is useless in Venezuela thanks to hyperinflation — so people are turning to bitcoin

- To survive Venezuela's hyperinflation, many have taken to mining bitcoin to afford basic necessities, according to the Atlantic
- It is also made affordable due to the low cost of power in the country's heavily-subsidized electricity market
- Bitcoin miners can make as much as $500 a month, which is enough to afford things such as baby diapers and insulin from overseas

Saheli Roy Choudhury | @sahelirc

Published 1:36 AM ET Thu, 24 Aug 2017 | Updated 11:40 AM ET Thu, 24 Aug 2017

CNBC

Entrepreneurship in developing countries

- unbanked residents of developing countries are often unable to enter the import or export business because they have no way to convert their currencies into more widely accepted money
- it may be impossible for them to process payments, pay for supplies and equipment, and receive loans or lines of credit
- the mobile telephone can provide access to a global market independent of the local banking infrastructure

Or an independent financial future

- Republic of Marshall Islands (RMI)
  - is poised to become the first sovereign nation to issue a cryptocurrency that will be legal tender - the SOV
  - the SOV will be distributed alongside its current local currency, the US$
  - dependence on the US$ should diminish
  - the SOV will be distributed to the public via an ICO so the public becomes stakeholders

5 other key cryptocurrency issues/challenges

- micropayments - difficult with fiat currency
- inflation - safeguards in the algorithm
- mining - or more specifically POW/POS
- volatility - speculation? investment?
- forks/clones - other cryptocurrencies - ICOs/ITOs, FinTech

Perhaps one of the lasting disruptive legacies of the cryptocurrency discussion is *blockchain*

What is the Blockchain? (1/3)

- the platform model for most cryptocurrencies
- a distributed database/ledger that provides an unalterable, (semi-) public record of digital transactions
- each block aggregates a timestamped batch of transactions to be included in the ledger (blockchain)
- each block is identified by a cryptographic signature

What is the Blockchain? (2/3)

- blocks are all back-linked, i.e., they reference the signature of the previous block in the chain (kind of like a linked list)
- that chain can be traced all the way back to the very first block created
- this provides an un-editable/immutable (compromised) record of all transactions made - why?
- the chain can be controlled by any single entity
- the chain has no single point of failure

What is the Blockchain? (3/3)

- most importantly (perhaps) - it is very hard to add blocks to the blockchain e.g., mining
- its strengths are in
  - distribution
  - technical robustness
  - lifespan
  - non-modifiability/immutability
  - unquestionable provenance via strong encryption

Cryptoeconomics or "Blockchain voodoo"

- the 3rd part of Satoshi's vision
- "past is provable, future is predictable"
- uses cryptography to prove actions occurring in the past (presence on the blockchain)
- predicts that economics can ensure that actions occur in the future (contracts/ programmable money on the blockchain)

(Ref: Justin Poirier)

Cryptoeconomics - why does it work?

- works because people trust math and people like money, privacy, etc.
- establishes trust, even between pseudoymous parties
- makes trust in a person or third party optional
- reduces the cost of an intermediary to only the actual transaction cost

(Ref: Justin Poirier)

Why Blockchain?

- just because we can, should we?
- "The idea that everyone (and their descendants) has to have a copy of THE ledger of all transactions in the universe (now and future) has always smelled fishy to me"
- the idea that people could have computers in their homes…
- the idea that people have all the world's knowledge at their fingertips…

A blockchain is “a technology that allows people who don’t know each other to trust a shared record of events”

- Bank of England

It doesn’t just have to be about money

"Of the 7.3 billion people in the world, only 2 billion have a title that is legal and effective and public regarding their control over an asset…When something is not legally on record as being owned, it can therefore not be used as collateral to get credit, as a credential that you can be able to transfer part of your property to invite investment in. Things are owned, but when they're not adequately paperized or recorded, they cannot fill the functions of creating capital and credit" - Hernando De Soto

"Although their incomes are low, the poor of the world have a surprisingly large amount of property. The problem is that this property is not legally recognized as theirs." - Niall Ferguson

"The majority of countries in our world have the following issue: people just losing properties because of someone changing records in a database." - Valery Vavilov (CEO of BitFury)

Blockchain and land registry

- people in many countries suffer when unclear ownership makes it hard to sell or borrow against real estate
- poor documentation can make it easier for corrupt officials to redistribute land to their cronies
- registry data stored on a blockchain would ideally make fraudulent land transfers by any corrupt future governments more difficult

bitland

Land Title Protection Ghana

HKU March 2018

Diamond blockchain

- diamonds represent emotional attachment, an illegal liquid means of exchange, a potential source of human suffering
- in January 2018 De Beers Group announced the establishment of a diamond blockchain to maintain immutable records of
  - quality and the value chain
  - ownership/exchange
  - provenance - conflict-free (no “blood diamonds”)

Identity

- 2 billion people in the world have a government-issued ID; more people have IDs on social media
- 5 billion in the world have no government-issued ID perhaps making them vulnerable to:
  - identity theft
  - access to services
  - mobility
  - reputation
  - even human trafficking

Suppose your ID resided on a blockchain?

- it would be immutable
- you could control
  - content
  - credibility
  - visibility
  - would identity theft be a problem or would this be a true online identity?
  - could you use your personal information bits like coins/ tokens of value?

Remember your public address?

- suppose you think of your public/private address/key as an identity (maybe, but not necessarily, the only kind of identity)
- in order to "speak for" your identity, your corresponding private address/key would be used
- suppose your passphrase/key pairs were associated with a biometric parameter, e.g., fingerprint, retinal scan, etc.

Democracy

- March 7, 2018 electronic voting using biometric data and personalized cryptographic addresses
- permissioned blockchain validated by authorized persons
- transparency
- no results manipulation
- no printing costs
- reduces electoral violence
- powered by Swiss foundation Agora


TRANSPARENT

The world's first blockchain-powered elections just happened in Sierra Leone

Conclusions and take-aways

- we need to look beyond the technologies of cryptocurrencies and blockchain as just being another form of money or banks
- these technologies have opened up a new discussion of how we might benefit the human condition
- there remain numerous challenges (maybe some unsolvable) associated with these technologies that should be addressed/explored
- these challenges are not just technical

I encourage you to get onboard - your ideas are needed!

HKU March 2018

Thank You!
Questions? Comments?

bebo@slac.stanford.edu

HKU March 2018