Bitcoin and other digital currencies: opportunities and threats

Dr. Frank Braun

April 15, 2015

areas of conflict

we'll look at current technological developments and future trends in the "money space" which pose

- opportunities
- threats

$\Rightarrow$ which is which?

$\Rightarrow$ please make up your own mind!

areas of conflict:

- control of the money supply
- traceability and the power to tax
- anonymity and the power to enforce laws
- control over financial participation (sanctions)

what is money?

definition:

- medium of exchange (3 Euro exchanged for Döner)
- unit of account (your total balance is 2,56 Euro)
- store of value (Krugerrand under mattress)

features:

- portability (cattle are not portable)
- divisibility (cattle are not divisible)
- durability (tea is not durable)
- rarity (sand is not rare)
- fungibility (diamonds are not fungible)

commodity money

historically commodities emerged as money *in the market*, e.g.:

- gold
- silver
- copper
- salt

using money has efficiency advantages over a *barter system*

state issued commodity money

Münzregal was the sovereign right of coinage:

- specification of *currency*
- right to mint
- right to use coins and the profit from minting

legal tender has advantages for issuer (government / sovereign):

- he can perform *debasement*:
  - reduce the purity of coins (e.g., put more copper into gold)
  - reduce the size of coins
- no competition

commodity backed paper money and fiat money

issue *paper notes* which are *redeemable* $\Rightarrow$ gold standard

Bretton Woods system established in 1944

US terminated convertibility of the US dollar to gold in 1971

$\Rightarrow$ world-wide fiat money system: "paper as money" (no backing)

Germany 1914 – 1923

Zimbabwe 2006 – 2009

inflation

- inflation is **not** an increase in the general price level
- inflation is an increase of the money supply

$\Rightarrow$ leads to increase in the general price level

- control of the money supply is **huge** power
- allows for hidden taxation:
  - inflation reduces worth of savings
  - inflation pushes people in higher tax brackets (progressive tax)

greatly varying opinions exists for:

- what is proper money and the role of interest rates
- the cause of business cycles and how to deal with them

pointers:

- Keynesian economics
- Chicago school of economics (monetarism)
- Austrian school (Austrian economics)

digital money

developed economies need money transfer *over distance*

- mailed check
- wire transfer
- credit card payments
- *digital money*

digital money: important concepts

- traceability (wire transfers)
- pseudonymity (numbered bank account)
- anonymity (cash)
- finalization vs. chargeback risk (Bitcoin vs. credit cards)
- central ledger vs. distributed ledger (bank vs. Bitcoin)

e-Gold (1996 – 2009) / 1mdc

- digital gold currency: digital currency **backed** by gold
- instant and final transfer of digital grams of gold (+ fractions)
- central ledger / accounting system
- peak 2006: e-Gold processed $>$ US$ 2 billion spends / year
- monetary base of only US$ 71 million worth of gold ($\approx 3.5t$)
- *overlay* currency 1mdc allowed for pseudonymous accounts
- mid 2000s: US stretched the definition of a *money transmitter* and pressed AML charges against e-Gold
- e-Gold was ultimately shut down by the US government
- judge: the founders of e-Gold "had no intent to commit illegal activity."
- founders vowed to continue operations under new KYC regulations, but failed to implement them

PayPal (1998 – today)

- original idea: a digital **currency**
- later: easy way to send USD and other currencies (via email)
- US: PayPal licensed as money transmitter, state-by-state basis

$\Rightarrow$ **very high** barriers to entry

- 2014: 203 markets, 152 million active, **registered** accounts
- PayPal allows to send, receive, and hold funds in 26 currencies
- follows all AML and KYC regulations

$\Rightarrow$ it is easy to get an account frozen

- chargeback risk

David Chaum / DigiCash (1990 – 1998)

cryptographer David Chaum:

- Untracable electronic mail, return addresses, and digital pseudonyms, *Comm. ACM*, 24, 2 (**Feb. 1981**); 84-90

$\Rightarrow$ groundwork for anonymous communications research

- **1983**: Blind signatures for untraceable payments, *Advances in Cryptology: Proceedings of CRYPTO 82*, pp 199-203

$\Rightarrow$ the foundation of **anonymous** digital money

founded DigiCash Inc. in 1990:

- produced "anonymous" micropayment system *ecash*

$\Rightarrow$ declared **bankruptcy** in 1998

Liberty Reserve (2001 – 2013)

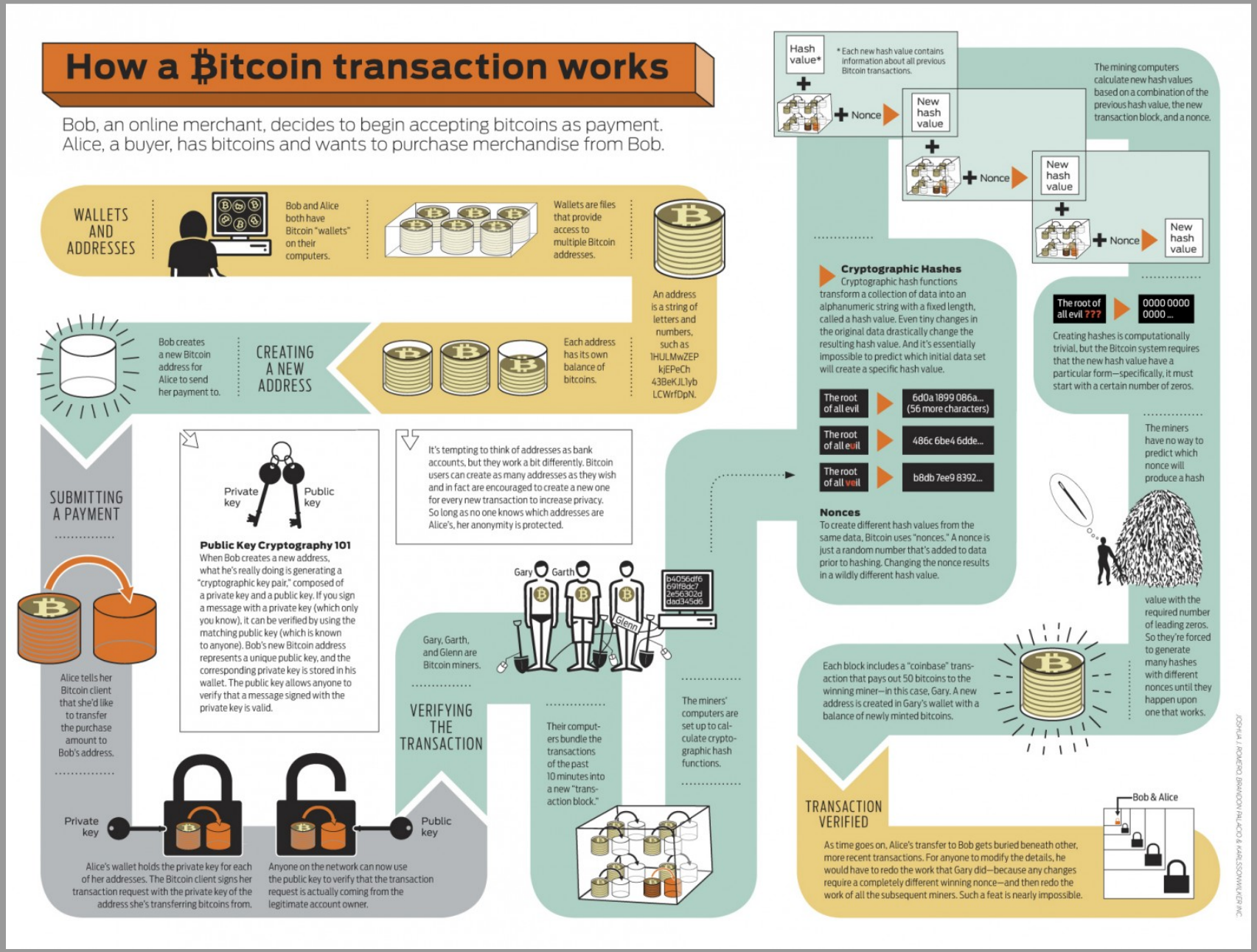
- centralized digital currency similar to PayPal
- was based in Costa Rica
- allowed to hold and transfer "Liberty" USD, Euro, and gold
- charged $\approx 1\%$ fee on each transfer (*finalized* transactions)
- followed AML and KYC regulations "liberally"
- 2013: shut down by US under the Patriot Act
- founders charged with money laundering and operating an unlicensed financial transaction company
- alleged to launder more than $6 billion in criminal proceeds during its history

M-Pesa (2007 – today)

- mobile-phone based money transfer in Kenya and Tanzania
- transfer of money via SMS, no smartphone required
- 2012: 12 million M-Pesa accounts in Kenya
- deposit and withdrawal money at banking agents ("Späti")
- gives people access to the formal banking system
- central ledger, fully traceable
- transfer and deposit/withdrawal fees $< 1\%$
- M-Pesa uses national ID cards to satisfy KYC requirements

Bitcoin (2009 – today)

- 2008: Satoshi Nakamoto publishes "Bitcoin: A Peer-to-Peer Electronic Cash System"
- 2009: Bitcoin network starts running with *genesis block*
- distributed ledger: *block chain*
- block contains all *transactions* since last block
- Bitcoin is a *consensus* mechanism
- Bitcoin *addresses* are *pseudonymous*
- transactions are fully *traceable* and public in the block chain
- transactions are *final*
- never more than 21 million Bitcoin ($\rightarrow$ fixed money supply)


How a ฿itcoin transaction works
Bob, an online merchant, decides to begin accepting bitcoins as payment.
Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.
WALLETS AND ADDRESSES
Bob and Alice both have Bitcoin "wallets" on their computers.
Wallets are files that provide access to multiple Bitcoin addresses.
An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.
CREATING A NEW ADDRESS
Bob creates a new Bitcoin address for Alice to send her payment to.
Each address has its own balance of bitcoins.
SUBMITTING A PAYMENT
Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.
Private key
Public key
Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.
It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.
Private key
Public key
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.
Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.
VERIFYING THE TRANSACTION
Gary, Garth, and Glenn are Bitcoin miners.
Gary
Garth
Glenn
b4056df6 69ff6dc7 2e563022 dad345d6
Their computers bundle the transactions of the past 10 minutes into a new "transaction block."
The miners' computers are set up to calculate cryptographic hash functions.
Hash value*
* Each new hash value contains information about all previous Bitcoin transactions.
Nonce
New hash value
The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.
Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.
The root of all evil
6d0a 1899 086a... (56 more characters)
The root of all evil
486c 6be4 6dde...
The root of all veil
b8db 7ee9 8392...
Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.
The root of all evil ???
0000 0000 0000 ...
Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.
The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.
Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.
TRANSACTION VERIFIED
As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.
Bob & Alice
JOSHUA J. ROMERO, BRANNON PALACIOS & KARL SCHWULKER/INC.

Bitcoin mining & current status

miners compete for new Bitcoin by solving mathematical puzzle to create next block:

- target rate: 1 block / 10 minutes
- difficulty adjustment every 2016 blocks
- reward: 25 Bitcoin
- reward halving: every 210000 blocks ($\approx$ 4 years)
- mining today mostly via *mining pools*

today:

- 6000 full Bitcoin nodes
- 1 Bitcoin $\approx$ 215 Euro
- 14 million Bitcoin in circulation

$\Rightarrow$ $\approx$ 3 billion Euro market capitalization

- Satoshi Nakamoto still unknown

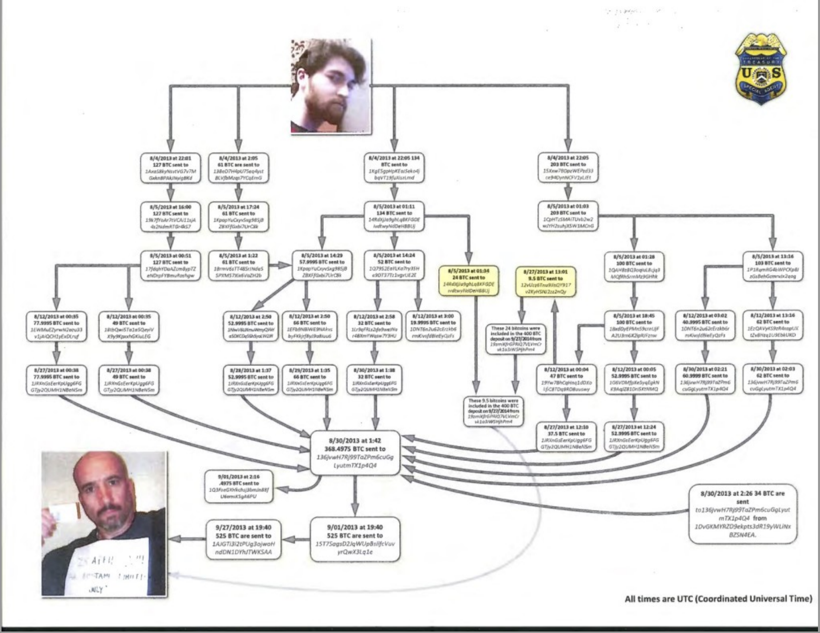
Bitcoin inspired many competing (alternative) *Altcoins*

Bitcoin case study: remittances

- remittance: transfer of money by a foreign worker to an individual in his or her home country
- 2013: $404 billion went to developing countries
- 2013: $542 billion overall global total
- Western Union and MoneyGram have large fees (up to 10%)
- Rebittance wants to reduce the fees to 1.1% by using Bitcoin
- e.g., Rebit allows to send money to the Philippines for free
- problem: exchangers in destination countries, regulations

Bitcoin case study: Silk Road

- Silk Road was an online black market mostly used for selling drugs
- launched February 2011
- website was a Tor hidden service
- Bitcoin was used as a payments system
- similar to Amazon Marketplace (with ratings for vendors)
- Silk Road provided Bitcoin *escrow* for fee
- FBI shut down the website in 2013 and arrested Ross Ulbricht
- FBI initially seized 26,000 Bitcoin, worth $\approx$ \$3.6 million at the time
- later FBI reported that it had seized 144,000 Bitcoin, worth \$28.5 million from Ulbricht personally


8/30/2013 at 1:42
368.4975 BTC sent to
136jvwH7Rj99TaZPm6cuGg
LyutmTX1p4Q4
9/01/2013 at 19:40
525 BTC are sent to
15T7SagsD2JqWUpBsiifcVuv
yrQwX3Lq1e
9/27/2013 at 19:40
525 BTC are sent to
1AJGTi3i2tPUg3ojwoH
ndDN1DYhJTWKSAA
8/30/2013 at 2:26 34 BTC are sent
to136jvwH7Rj99TaZPm6cuGgLyut
mTX1p4Q4 from
1DvGKMYRZD9ekpts3dR19yWLiNx
BZSN4EA.
All times are UTC (Coordinated Universal Time)

Bitcoin case study: WikiLeaks

- 2010: WikiLeaks released US diplomatic cables

$\Rightarrow$ donations to WikiLeaks were blocked by Bank of America, VISA, MasterCard, PayPal and Western Union

- it is believed due to political pressure by the US government
- example for control over financial participation (sanctions)
- WikiLeaks took Bitcoin donations and was able to stay afloat

Crypto Wars II

history:

- Cypherpunk movement started in the late 1980s
- crypto was export restricted, universal backdoor demanded

$\Rightarrow$ Cypherpunks won the first Crypto Wars

$\Rightarrow$ lead to WikiLeaks (among other things)

today:

- Edward Snowden
- Apple et al. pushing for stronger encryption

$\Rightarrow$ Crypto Wars II

the four horsemen of the information apocalypse

1. terrorists
2. drug dealers
3. money launderers
4. child pornographers

$\Rightarrow$ look out for these in public debates!

counter-economy in general (a.k.a. the black market)

- "Forget China: the $10 trillion global black market is the world's fastest growing economy – and its future. "
- "[If it] were an independent nation, united in a single political structure – call it the United Street Sellers Republic (USSR) or, perhaps, Bazaaristan – it would be an economic superpower, the second-largest economy in the world (the United States, with a GDP of $14 trillion, is numero uno)."
- "In the developing world, it's been increasing every year since the 1990s, and in many countries it's growing faster than the officially recognized gross domestic product (GDP)."

(The Shadow Superpower, *Foreign Policy*, October 28, 2011)

the fight over exchangers

exchanger: allows to exchange in and out of digital cash (for example, Bitcoin and e-Gold)

- similar to conflict regarding large cash deposits, withdrawals, and cross-border transport
- Know Your Customer (KYC) regulations
- Anti Money Laundering (AML) regulations

cashless society

- pro arguments: reduced costs and reduced crime rates
- Nordic countries are leading the way to cashless societies
- 2013: Nigeria starts to roll-out 13 million MasterCard branded national ID cards with electronic payment capabilities
- deployed systems are fully traceable

$\Rightarrow$ obvious privacy implications

Ethereum

- cryptocurrency crowdfunded with Bitcoin in 2014
- largest crowdfunding campaign at the time: US$ 18 million
- presale of *Ether*, the currency of Ethereum
- Bitcoin: simple scripts, e.g. 2-of-3 multi-sig transactions
- Ethereum: Turing-complete distributed virtual machine (VM)
- Ether is used to pay for executing code on the Ethereum VM

$\Rightarrow$ the same code is executed on each node in the network

$\Rightarrow$ protocol defines a consensus finding mechanism

$\Rightarrow$ not just currency, but allows to execute *smart contracts*

- example: virtual trust found, releases funds to address of child at certain date (or over time)
- cryptographically secured, non-changeable

recap

- development of money in general and the role of digital money

⇒ transfer over distance

- history: e-Gold, PayPal, DigiCash, and Liberty Reserve

⇒ most advanced solution failed, regulation killed innovation

- state of the art: M-Pesa and Bitcoin
- Bitcoin case studies: remittances, Silk Road and WikiLeaks

⇒ simple solutions (fully traceable) are astonishingly successful

⇒ crytocurrencies are here to stay (backing, consensus)

⇒ interesting DCs lead to interesting real world phenomena

conclusion

- trends: Crypto Wars II, developing counter-economy, fight over exchangers, cashless society, Ethereum

⇒ areas of conflict **remain**:

- control of the money supply
- traceability and the power to tax
- anonymity and the power to enforce laws
- control over financial participation (sanctions)

⇒ **technological** and **political** forces pull in two **extreme** directions:

1. transparent and cashless society, **everything** is taxable, **automatic** law enforcement, strong control of the money supply, **no privacy**
2. ubiquitous anonymous digital cash, non-traceable communications and financial transactions, metastasizing black markets, **states loose power** to tax and enforce laws

of course, more **moderate** scenarios in the middle are possible!

interesting future ahead!

links

projects:

- Mute: `http://mute.berlin` (register for beta invitation)

contacts:

- `frank@cryptogroup.net` (please use PGP, key on key server)
- `94CC ADA6 E814 FFD5 89D0 48D7 35AF 2AC2 CEC0 0E94`

slides:

- `http://mute.berlin/doc/touro.pdf`

thank you very much for your attention! questions?