

Will the monetary system change?

Risks and privacy implications of digital currencies, and decentralized systems

#what_is_this_talk_about

- + Will the monetary system change?

- Yes, it already has.

- + How and why, and what drives the change is what we try to understand and research.

- We will talk about *economics*, and the *Internet*.

#whoarewe

- + I am glad I do not speak only for myself today, but also in the name of an excellent team called TSH
- + My name is Usema and I go by the nick of Nsb. (We just hate voyelles)
- + TSH is a team of Tunisian white hat hackers: Amine, Bayrem, Bilel, Youssef and Fahmi... (big up!!!)
- And they are great at what they are doing.
- + We are nerds who like economics, computers, opsec, staying up late and Signal. (except Fahmi)
- + Next year hopefully the TSH guys will come to talk about how they can deploy banking software, and harden it, on a hostile environment.
- And probably invite you to hack it.

#root

- + Our goal is to build a place where Internet is a tool for a more fair distribution of wealth.
- + In our understanding, wealth distribution is not taking from someone to give to someone else.
- + Wealth distribution would be fair if financial wealth can find its way, as far as it can reach out. In a frictionless manner.
- + It means for us conceiving new systems that can be as inclusive as connecting to the Internet. With fewer or no intermediaries.
- + We can use computers to do that. In very imaginative ways.

#let's_manage_expectations

- + There will be five parts in this presentation.
- + We are here to provide the results of a research project that started back in July 2015.
- + This is not an exercise where we reply to questions, but rather ask more of them, and provide theories that we can apply.
- + You are invited to be critical, because anyways you will be:
 - Nothing gives back better than a constructive and objective audience.
- + It is a thought process:
 - We start from the systems that are immature and complex to grasp and appreciate.
 - We end up with a system that even grandparents can understand and use.

Monetary systems

#monetary_systems

+ The birth of money in the system:

- To create wealth, Central banks can tweak interest rates, print money, or throw it from a helicopter, to inject it in a given economy.



[https://en.wikipedia.org/wiki/Helicopter_money]

#monetary_systems

- + The birth of money in the system:

- Central banks issue debt that few selected financial institutions in a given economy are eligible to buy. Other banks.

- These banks repackage the debts and sell them to smaller banks, etc, etc...

- The more this money is exchanged, the more it provides the market with fresh financing resources.

#monetary_systems

- + The birth of money in the system:
 - Banks are also eligible to create money out of thin air, through issuing debt via loans and other products...
 - The money circulates in the given economy so people can get income, deposit it in bank accounts, and pay their taxes.
- + This newly created money is backed by: Trust (governance), regulations and security.
 - Too big to fail == Feel free to cheat

Bankless monetary systems

#bankless_monetary_systems

- + Bankless systems. Who started this thing?
- Bitcoin is the first operating bankless monetary system built on the Internet.
- + What did Bitcoin do?
- Bitcoin replicated the monetary role of Central Banks: Currency creation, distribution and settlement.
- Moreover Bitcoin made untrusted participants agree on a single version of data set, solely relying on connected machines.
- (and incentive engineering).
- To achieve this, Bitcoin adopts a set of unorthodox, known and fixed rules.

#bankless_monetary_systems

- + It's safe to say that Bitcoin is:
 - An experimental piece of software,
 - A network,
 - And potentially a payment protocol, that can replace/reshape legacy monetary systems.
 - With no banks involved (required) at all.

#bankless_monetary_systems

+ What are Bitcoin related risks (assuming that no one ever uses hard cash to commit crimes)?

- Same drivers as classic banking: Toxic environment and greed.

- Weak Governance and exposure to attacks by economic players.

- Energy consumption: No replication of proof-of-work for new decentralized/centralized systems.

- Bitcoin - Die Technik und ihre Ökologische Auswirkung – Jaseg: [<https://media.ccc.de/v/dg-71>]

- Mining centralization: 71% of the mining power is based in China.

- It is better than having them attacking the network.

- Unequal distribution of coins: Satoshi ~900k BTC, FBI ~174kBTC...

#bankless_monetary_systems

+ What role a Bitcoin would play?:

- Bitcoin would be for banking institutions what a “hardened” SMTP would be for emails servers.

- Error 402 - Payment required:

> Reserved for future use. The original intention [of error 402] was
> that this code might be used as part of some form of digital cash
> or micropayment scheme, as proposed for example by GNU Taler, but
> that has not yet happened, and this code is not usually used.

[https://en.wikipedia.org/wiki/List_of_HTTP_status_codes]

#bankless_monetary_systems

+ What role a Bitcoin would play?:

- If two banks, or two payment systems, have different currencies and different architectures and designs, they still can exchange with each other, using bitcoin as transfer and settlement protocol...

-- ...in a relatively secure and valid manner.

- Transfer of financial data, with nominal settled value.

#bankless_monetary_systems

+ Bitcoin is here:

- Large and active community of cryptographers, developers, investors and entrepreneurs
- Resiliency and resistance to censorship: Bitcoin fibre, Satellite...
- Innovation: Diverse implementations
- Reached a critical security mass:
 - Provides security and mitigation against identified attacks: 51% attack, double-spend attack, Sybille attack, DoS...

#bankless_monetary_systems

+ Questions:

- What happens if connected machines can perform the same operations as humans, in a more efficient and predictable way?
- What are the implications of switching to a bitcoin-centered monetary system?

Financial systems

#financial_systems



The financial system

"To a computer programmer the financial systems looks like a lot like untested code with weak debugging..."

Tim Wu, Law professor

#financial_systems

+ What is the financial system now?

- A financial system is the system that covers financial transactions and the exchange of money between investors, lenders and borrowers.

- Financial systems can also be defined as models that portray financial services, institutions and markets that link depositors with investors.

[Investopedia]

#financial_systems

+ Questions:

- Trust in software and computer networks, or trust in bankers as individuals?
- Can banking ignore the new bankless systems?
- Wait a minute let's think about the bank as a business (which it is): What kind of skills would the new bankers be required to have?
- Who cares about banks? What would be their role? Will they adapt to binary currencies?
- What would binary currency bring to the industry?

Currency technology

#currency_technology

**...because everyone
needs a Swiss bank
account in their pocket**

#currency_technology

- + What does binary currency bring to the monetary system?
- Kein papier: New architectures
- *Micro* transfers
- Programmability, Automation, and other buzz words...
- Infinite inclusiveness
- More risks, thus a need for *regulation*

#currency_technology

- + The technology and security underlying the payment systems will bring more value to the currency:
- As if a dollar made out of better paper would be preferred and more valued by the user.
- Incentive for banks and financial institutions to implement competitive technology:
- The more private and secure, the more attractive the currency will be for a technology-elastic user.

#currency_technology

+ Risks and privacy implications of binary currency:

- It keeps (nasty) logs of every transaction you do.

- Richad Stallman on Bitcoin – London 2012: [<https://youtu.be/FN6Q--zqroM>]

- All the time: examples of Scandinavia and India

- Electronic payments for liberal society - Sva: [https://media.ccc.de/v/EH2017-8471-taler_-_talk]

- It depends of the technology providers and their will to **not** use the data for an evil purpose.

- It is an excellent tool for dictators and totalitarians to set up a dystopia by the book.

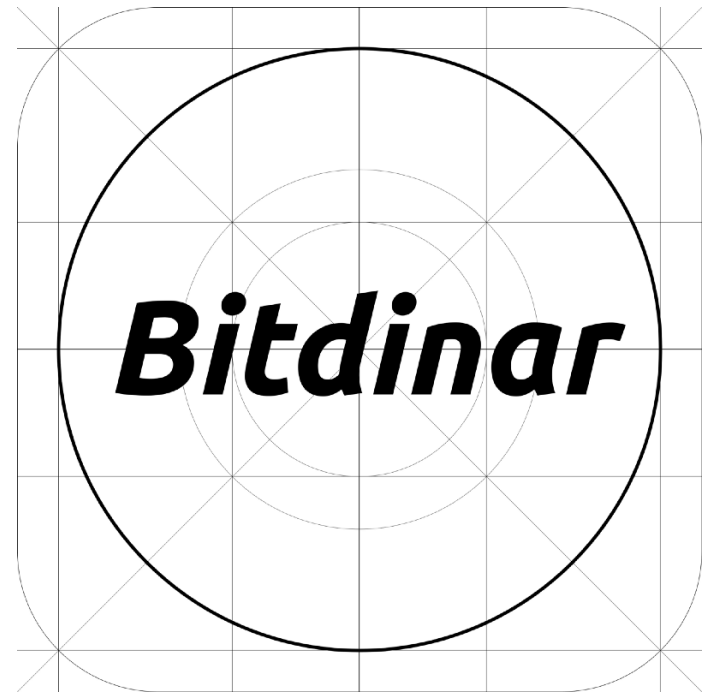
#what_now

- + New monetary systems with new rules.
- + It is not gonna stop.
- + Risks of proliferation of monetary chocks, and radical tactics.
- + Adoption of invasive financial technology by authoritarian individuals.
- + Is it the end of the world? No!

Implementation

#implementation

- + So we came up with a proposition of a simple payment system called Bitdinar.
- + The project started somewhere around summer 2015.
- + The first Bitdinar coin ~~mined~~ mined in September 2016, as an early prototype.



#implementation

- + Bitdinar is a centralized payment system: A digital fiat currency
- + We designed Bitdinar so there is the smallest number of "features" to hack.
- + "Send" and "Receive" Bitdinar tokens, in a server-client architecture.
- + Bitdinar is a fork of taler.

#implementation



Abhishek Balaji

Jan 2 · 10 min read

GNU Taler—‘Digital Cash’ that is socially responsible

A Technological Option to Save our
Democracy and Economy from
“Cashless” Totalitarianism

<https://blog.50p.in/taler-98604e2e0094>

#implementation

+ Then we found a bank willing to let us deploy Bitdinar as a payment system for them.

+ Somewhere around fall 2016.



#implementation

- + La Poste Tunisiennes is a public bank. The equivalent of public Postbank, more or less.
- + La Poste Tunisienne uses Bitdinar as a gateway to their existent eDinar payment framework.
- + La Poste Tunisienne is headed by Moez Chakchouk.
- He founded 404Labs, a safe space located now in the same building that used to host the local Internet censorship infrastructure (under Ben Ali's dictatorship).

#implementation

+ Then the Tunisian Central Bank decided to officially research and develop a digital money strategy. Nearly 2 months ago.

> ...this action is part of a national strategy to promote
> financial inclusion, consolidate the resources of the
> banking system...

[<https://www.tap.info.tn/en/Portal-Top-Slide-EN/9485689-meeting-at-bct-on>]

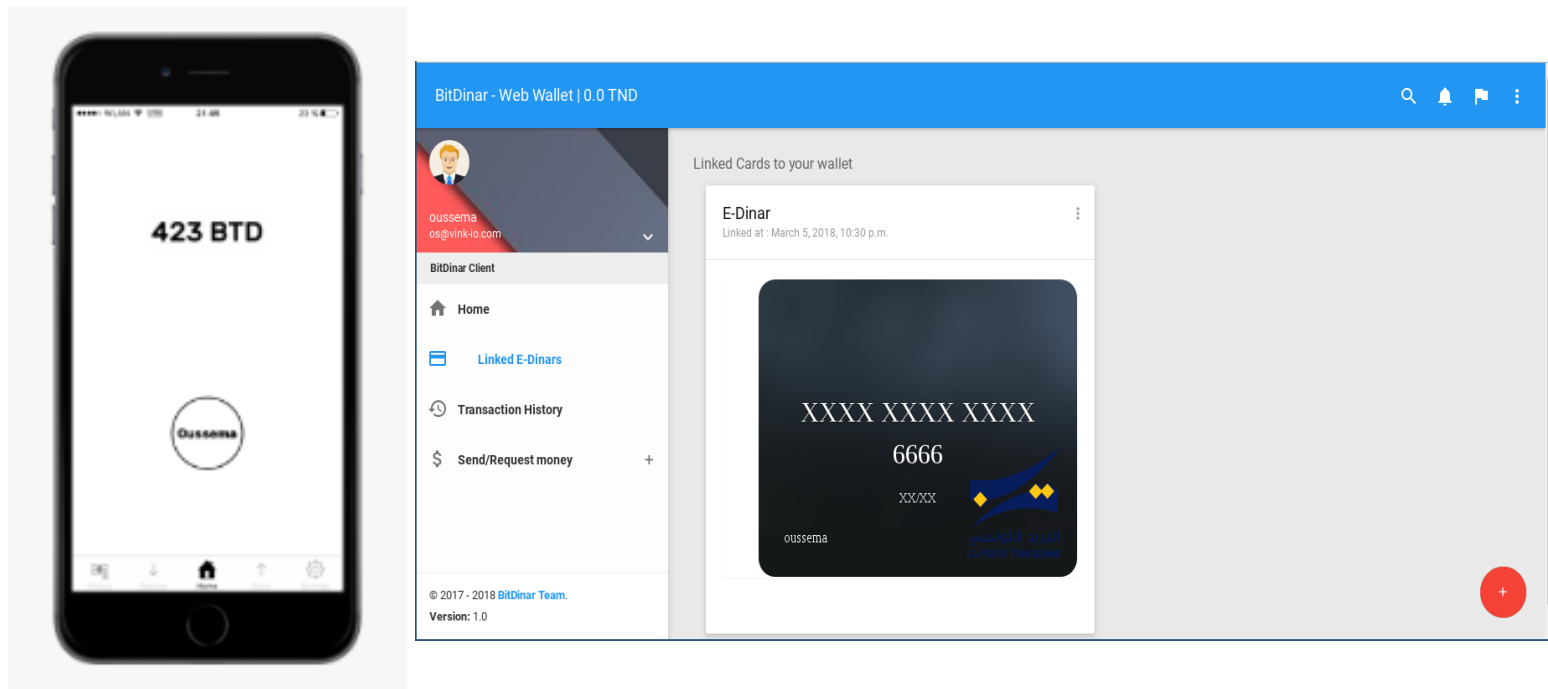
+ They decided it was time to reduce cash, on which the local economy relies heavily, and boost the "digital" economy.

+ We have applied even though they did not specify when and how companies can apply.

#implementation

+ Then I asked TSH to take pictures of themselves excited about C++ code, and dreaming of fountains of bitcoin while changing the world.

+ Instead they decided to share with you a snapshots of their implementation.



Books and links

Books:

- Capital in the 21st century: Piketty
- The banker's new clothes: Anat Admati & Martin Hellwig
- From bitcoin to Burning man and beyond: John Clippinger David Bollier
- Mastering bitcoin: @aantonop: <https://github.com/bitcoinbook/bitcoinbook>

Links:

- Workshop on standards for digital Fiat currency: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/dfc/201710/Documents/Outcomes_DFC_Workshop.pdf
- How banks create money: <http://positivemoney.org/how-money-works/how-banks-create-money/>
- The libbitcoin maifesto - Amir Taaki: <http://nakamotoinstitute.org/libbitcoin-manifesto/>

Videos:

- Bitcoin - Die Technik und ihre Ökologische Auswirkung - Jaseg: <https://media.ccc.de/v/dg-71>
- Electronic payments for a liberal society - Sva: https://media.ccc.de/v/EH2017-8471-taler_-_talk
- How the economic machine works - Ray Dalio: <https://www.youtube.com/watch?v=PHe0bXAIuk0>
- Don't Panic facts about populations - Hans Rolsing: <https://youtu.be/FACK2knC08E>
- The 4 horsemen of the apocalypse - the renegades: <https://youtu.be/5fbvquHSPJU>
- Rise and rise of bitcoin: <https://youtu.be/gcwnpv0Dd-8>

Propaganda:

- World Web Forum in zurich: <https://www.iso-20022.ch/info-to-go/news/artikel/world-web-forum-oussema-settala-ueber-die-demokratische-seite-der-blockchain/>
- Enpact interview: <http://www.enpact.org/digital-currencies-as-a-tool-for-financial-inclusion/>

That's it fnords!!



1GG8rNnFMePJL1Jh1EhJm2F9wJ1v5PhhUh

Donations in btc