Money and Payments in the Digital Age: Innovations and Challenges

François R. Velde
Federal Reserve Bank of Chicago

ÖNB - SUERF economics conference, Vienna 2017

Usual disclaimer

The views expressed do not necessarily represent those of the Federal Reserve Bank of Chicago or the Federal Reserve System

1. Money in the past
2. Bitcoin and all that
3. DLT or Blockchain
4. Money in the future

Money in the Past

- The barter problem
  - I want what you have but you don't want what I have
- A problem only if society lacks record-keeping
  - Solution: use secure tokens (as in a poker game)
- How to make them secure?
  - Solution: use tokens that are costly to counterfeit (gold, silver)
  - typically certified by a central authority (mint)
- How to economize on cost?
  - Find cheaper tokens
    - fiat (but still valued; counterfeiting must be prevented)
    - claims on assets (banks' demandable deposits, goldsmith notes, government debt)
  - improve record-keeping
    - reduce need for tokens through netting
    - centralized record keeping (early central banks from 1400, clearing houses)
  - none of this was easy to achieve (legal and theoretical innovations)

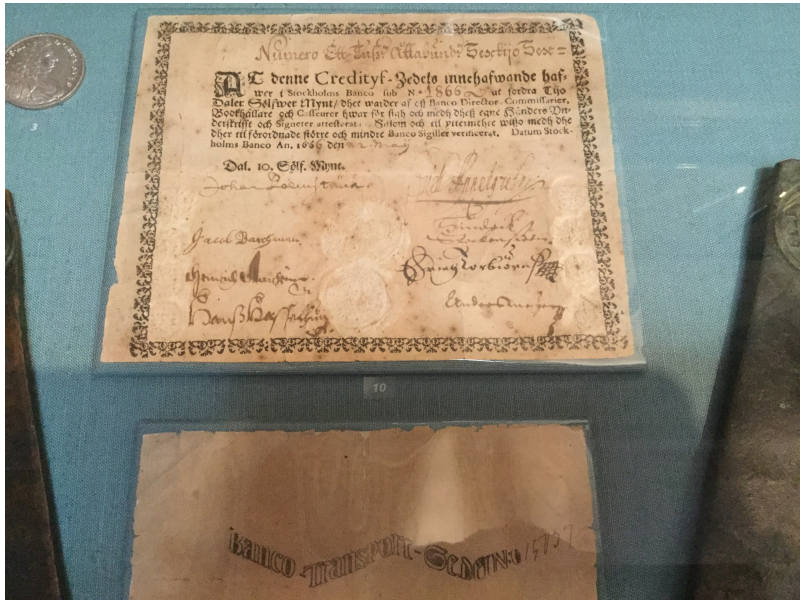
Money across the ages

costly token (ca 625 BC)

Money across the ages

ledger money (Amsterdam, 17th c.)

Money across the ages



cheap token (1666 AD)

Recurring themes in monetary history

- trust (i.e., lack of information and/or enforcement) has always been at the core of money
  - tokens: counterfeiting (as old as money)
  - ledgers: who guards the guardian?
- threats
  - self-interested attackers (counterfeiters)

Recurring themes in monetary history

Recurring themes in monetary history

- trust (i.e., lack of information and/or enforcement) has always been at the core of money
  - tokens: counterfeiting (as old as money)
  - ledgers: who guards the guardian?
- threats
  - self-interested attackers (counterfeiters)
  - malicious attackers

Recurring themes in monetary history

Recurring themes in monetary history

- trust (i.e., lack of information and/or enforcement) has always been at the core of money
  - tokens: counterfeiting (as old as money)
  - ledgers: who guards the guardian?
- threats
  - self-interested attackers (counterfeiters)
  - desperate governments (debasement/inflation = legal counterfeiting)
- intervention of a central authority
  - ranges from simple certification (minting) to central control
  - money is (also) a unit of account, hence need for setting standards

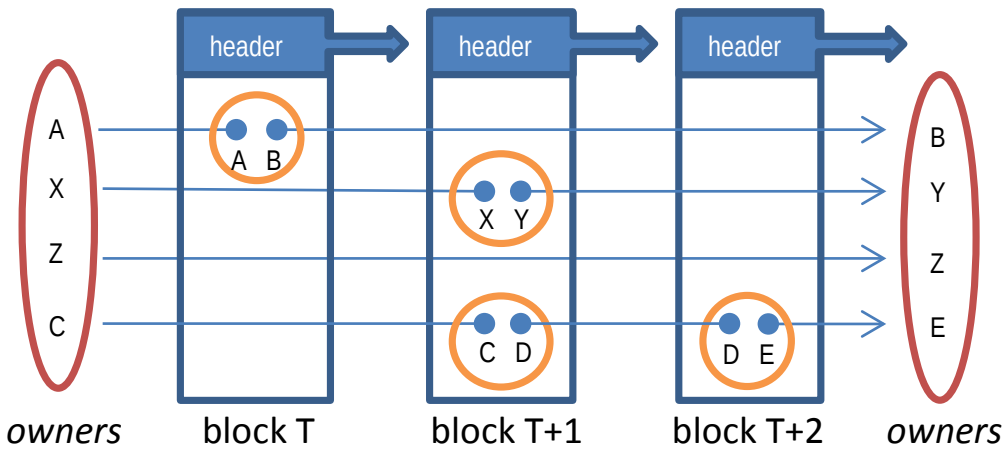
BTC and DLT

- 2009: bitcoin (BTC) described and launched
- 2012-13: catches the world's attention
- Using long-standing tools and clever design, it solves a particular problem:
  - how to issue and manage a monetary online token with no authority
- It is unique in monetary history:
  - intrinsically worthless yet valued (albeit with high variance)
  - dematerialized (no physical token)
  - neither inside nor outside money (no one's liability)
- It uses/exemplifies Distributed Ledger Technology (DLT)
  - potential applications outside the monetary/payments context

Design Elements

- Ownership: I own X because everyone knows/agrees that I do
  - information + consensus
- Recursive structure:
  - everyone agrees on a state of the world at time T (who owns what) = ledger
  - process for moving from T to $T + 1$
- Three elements:
  1. State of the ledger
  2. Language for transactions (ceding ownership)
     - cryptography verifies identities of sender/receiver
  3. Protocol for updating the ledger with validated transactions
     - in a decentralized, asynchronous system, how do we reach consensus?
- Essential value of ownership: the ability to transfer it
  - this is what makes BTC money (example of "on-chain asset")
  - can be applied to off-chain assets, but the link to real-world has to be ascertained

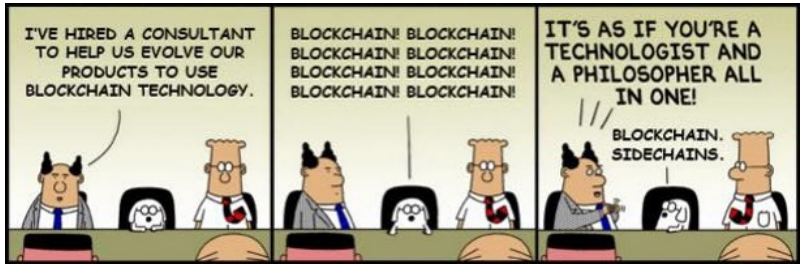
A blockchain



Consensus Protocol

- Decentralized system: who gets to update the ledger?
- Two broad methods:
  1. The updater is chosen at random, but from which set?
     - Proof of work: from those who pay to enter the lottery (BTC)
     - Proof of stake: from those who put up collateral (Ethereum?)
     - In both cases, altering the ledger is made costly
  2. We vote:
     - The voters are vetted (permissioned system) and rely on voters they trust
     - Algorithm reaches consensus even with unreliable or malicious participants (Byzantine generals): Ripple
- Key point: trust is never eliminated, it is displaced
  - you don't have to trust counterparties, but you have to trust the protocol
  - the ledger is only as immutable as the protocol!

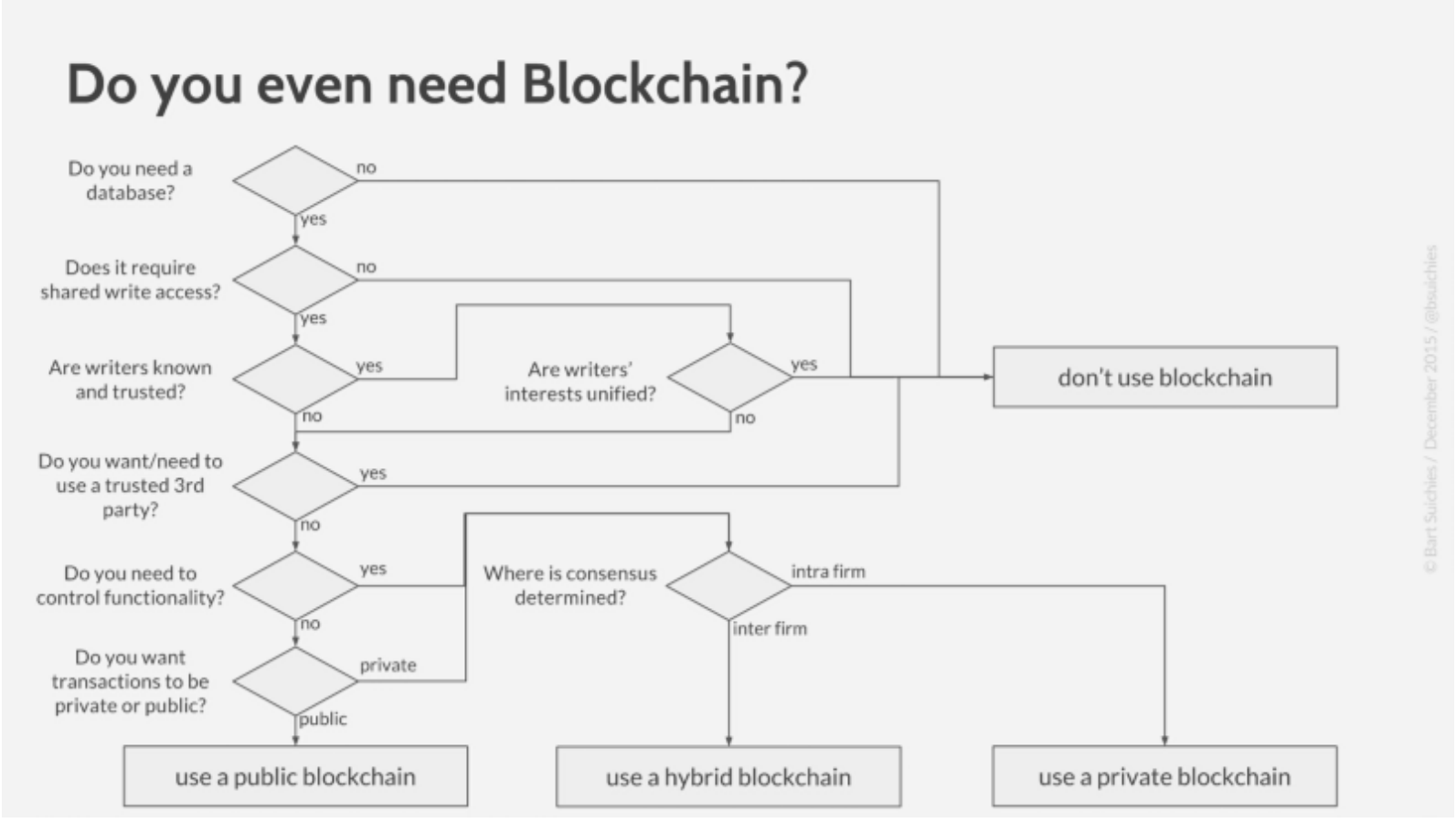
Is DLT a solution in search of a problem?



Is DLT a solution in search of a problem?

- Many have been taken with the desirable properties of blockchain
  - resilience, speed, decentralization, immutability
- Caveats: these properties
  1. stem from the solution to a particular decentralized problem
     - are decentralization and lack of trust key features of your problem?

Is DLT a solution in search of a problem?



emphasizing the **D** in **D**LT

Is DLT a solution in search of a problem?

- Many have been taken with the desirable properties of blockchain
  - resilience, speed, decentralization, immutability
- Caveats: these properties
  1. stem from the solution to a particular decentralized problem
     - are decentralization and lack of trust key features of your problem?
  2. involve tradeoffs

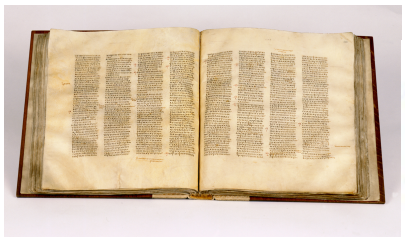
     scale/latency full histories and multilateral interactions imply increasing amounts of data

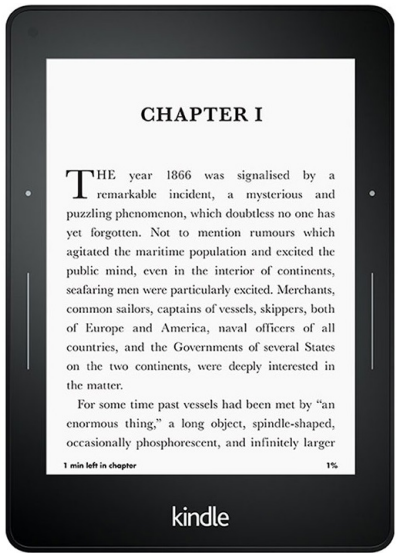
     information/privacy DLT builds ownership on (massive) public disclosure

     governance/control more openness means less control and more difficult governance

     resilience/vulnerability multiple nodes/copies of the ledger, but the protocol is a single point of failure
  3. only obtain once transition costs are paid
     - $1 \succ 2 \not\Rightarrow$ it's worth moving from 1 to 2

The future of money?





from 4th c. AD to 21st c. AD technology

from 7th c. BC to 21st c. AD technology?

Why digitize money?

- new technologies enable us to do the same things better, or to do new things
- DLT as a payment technology
  - better payments
    - faster/safer settlement and payment
    - broader access/fewer intermediaries
  - new payments
    - micro-payments
    - smart contracts
    - payments across asset classes
  - may not replace physical cash entirely
  - would it replace private money entirely?
    - it has been with us for a long time, as have its problems
- are these advantages unique to DLT?

Who will digitize money?

- historically the State and money have never been far apart
  - money as a regalian right (fiscal tool) or a public good entrusted to the State
  - legal tender underlies all payments
- but much innovation has come from the private sector or "trade groups"
  - first public banks founded in merchant cities, later ones were private corporations
  - legal and technical innovations arose bottom-up
- today Central Banks
  - issue and manage outside money/legal tender
  - (often) manage large-value payments (LVP) systems
  - regulate financial actors and protect financial stability
- BTC/DLT pose challenges
  - BTC: who/what do you regulate?
  - DLT: may create new actors/change risk profiles of existing actors/create new systemic risks
- Reasons why CBs might become involved in DLT
  - to set standards and ensure safety
  - improve LVP systems – or even SVP systems a.k.a. physical currency
  - provide legal tender for private sector DLTs
  - improve monetary policy: pay interest (perhaps negative) on digital money

Conclusion

- a lot of FinTech is about new ways to acquire and use private information
- perfect information (and enforcement) obviates money
- BTC has redefined ownership based on consensus and created a new form of liquidity (transferability)
  - but DLT solves a particular, decentralized problem
- if DLT does come into broad use, central banks will be drawn in
  - they can stay ahead or catch up