

Breaking the Bank

Stable asset-backed cryptocurrencies

Alexander Lipton

jointly with Sandy Pentland, Thomas Hardjono
MIT Connection Science & Engineering

Stanford

08 February 2018

*"But money has been introduced by convention as a kind of substitute for need or demand; and this is why we call it money (νομισμα), because its value is derived, not from nature, but from law (νομοζ), and can be altered or abolished at will."
Aristotle, The Nicomachean Ethics*

Milton Friedman Quote

"I shall depart from the original 'Chicago Plan of Banking Reform' in only one respect, though one that I think is of great importance. I shall urge that interest be paid on the 100% reserves. This step will both improve the economic results yielded by the 100% reserve system, and, also, as a necessary consequence, render the system less subject to the difficulties of avoidance that were the bug-a-boo of the earlier proposals. ... This problem of how to set the rate of interest is another issue that I feel most uncertain about and that requires more attention than I have given to it."

Milton Friedman, A Program For Monetary Stability

"I. The outbreak of the crisis and its spillover to the entire world reflect the inherent vulnerabilities and systemic risks in the existing international monetary system."

"II. The desirable goal of reforming the international monetary system, therefore, is to create an international reserve currency that is disconnected from individual nations and is able to remain stable in the long run, thus removing the inherent deficiencies caused by using credit-based national currencies."

"III. The reform should be guided by a grand vision and begin with specific deliverables. It should be a gradual process that yields win-win results for all."

*Dr. Zhou Xiaochuan, Governor of the People's Bank of China,
23 March 2009*

Contents

- Recent technology advances
- Why blockchain can potentially be useful?
- How to choose a ledger?
- Some potential applications
- Monetary circuit
- Bitcoin setup
- Ripple setup
- Global payments
- Should governments issue digital cash?
- Chaum vs Nakamoto
- Utility Settlement Coin
- Digital Trade Coin
- Conclusions



TECHNOLOGY

BREAKING THE BANK

NEW FINANCIAL NETWORKS COULD STOP
THE CONCENTRATION OF WEALTH AND
INCREASE PARTICIPATION IN THE ECONOMY,
BUT ONLY IF USED WITH CARE

BY ALEXANDER LIPTON AND ALEX PENTLAND

IN BRIEF

The modern financial system has introduced some fundamental problems into society. In order to increase transparency and minimize risk, the supercomplex monetary circuit has to be modeled in sufficient detail—a task that our current technology is unable to handle.

New technologies such as digital currencies are now making it possible to simulate every trade and transaction. These tools could build more efficient financial networks and decentralize the control of money. People could exchange directly with each other instead of relying on banks.

Although the potential for sweeping change is sparking fervent innovation, many variables remain. How these digital networks get built and used are critical factors in ensuring that they promote equity and accountability. Extreme levels of centralized control are possible too.



Subject Areas:

Digital currency, blockchains, reserve banks, cryptocurrency

Keywords:

Blockchain technology, cryptography, electronic cash

Author for correspondence:

Thomas Hardjono

e-mail: hardjono@mit.edu

Digital Trade Coin (DTC): Towards a more stable digital currency

Alexander Lipton¹, Thomas Hardjono² and
Alex “Sandy” Pentland³

¹MIT Connection Science

²MIT Connection Science

³MIT Media Lab & Connection Science

We study the evolution of ideas related to creation of asset-backed currencies over the last two hundred years and argue that recent developments related to distributed ledger technologies and blockchains gives asset-backed currencies a new lease of life. We propose a practical mechanism combining novel technological breakthroughs with well-established hedging techniques for building an asset-backed transactional oriented cryptocurrency, which we call the digital trade coin (DTC). We show that in its mature state, the DTC can serve as a much needed counterpoint to fiat reserve currencies of today.

1. Introduction

This paper describes the concept of the asset-backed *Digital Trade Coins* (DTCs), currently under development at MIT [1]. It outlines an approach to building a consortium of sponsors, who contribute real assets, a narrow bank handling financial transactions involving fiat currencies, and an administrator, who issues the corresponding digital token in exchange for fiat payments and makes fiat payments in exchange for digital tokens. In short, our proposal is to apply distributed ledger technology to give a new lease of life to the old notion of a sound asset-backed currency, and to use this currency as a transactional tool for a large pool of potential users, including small and medium enterprises (SME) and individuals. We intend to build a currency, which encourages legitimate commerce, but makes illegal activities difficult.

Digital Trade Coin (DTC) in a Nutshell

- Today, for the first time ever, there is the possibility of a digital currency that combines the best features of both cash and digital currencies.
- This currency is largely immune to policies of the central banks that control the worlds' reserve currencies.
- Such a currency has enormous potential to improve the stability and competitiveness of trading and natural resource producing economies.
- We propose to develop a trade-oriented asset-backed digital currency, aimed at facilitating international trade and making it as seamless as possible.

- This currency will be based on proprietary framework combining the most recent advances in blockchain and distributed ledger technology, cryptography, and secure multi-party calculations, together with time-tested methods for preventing double spending.
- Unlike Bitcoin, it will be fast, scalable, and environmentally friendly.
- It will also be transaction friendly because of its low volatility vs fiat currencies.

Digital Trade Coin (DTC) in a Nutshell

- Coins: Roman, Iranian; used in Silk Road
- Coins: Spanish, Austrian: used in Age of Sail
- Coins: Sterling: reserve currency driven by the British Empire
- Dollar: used as reserve currency for 20th Century
- Euro, Yen: added to reserve currency basket in late 20th Century
- ...and now the Yuan and a revived Silk Road

The Nabataean Kingdom

Nabataean Kingdom (400 BC – 100AD)



Figure: Nabataean Kingdom.

The Old Silk Road

Trade Coins on the Silk Road:

silver *drachm* of Sasanian Iran and gold *solidus* of Byzantine empire

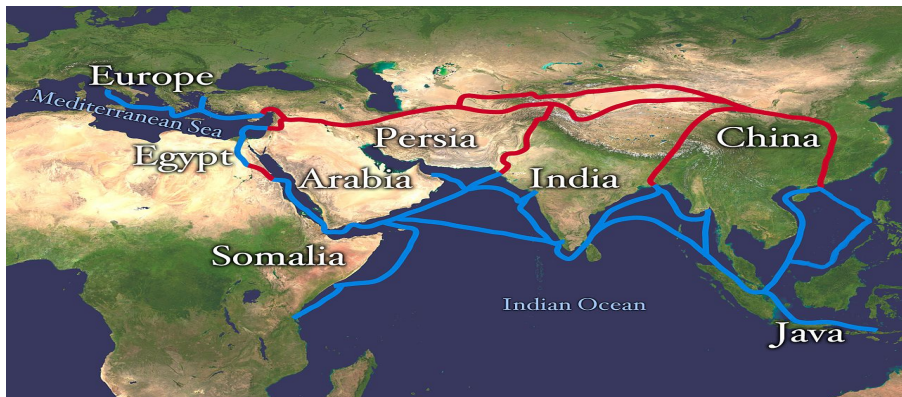
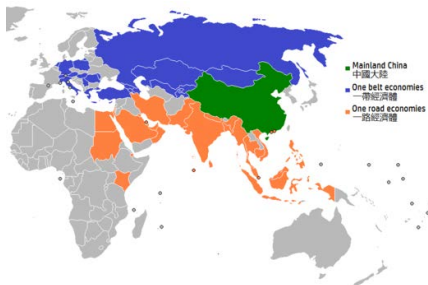


Figure: Old Silk Road.

A New Silk Road

Chinese One Road Countries (In Orange Color)



CONCLUSION:

PROSPERITY COMES FROM CONNECTIONS

Figure: New Silk Road.

Pieces of Eight

Trade Coins: Spanish Piece of Eight, Austrian thaler,

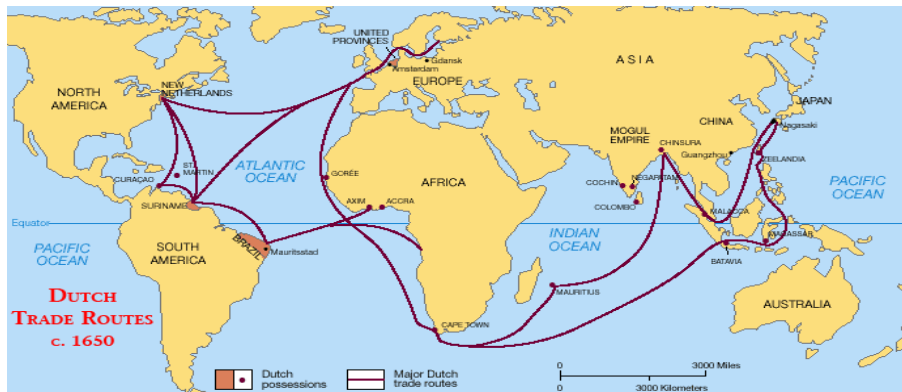


Figure: Spanish Pieces of Eight

Recent Technology Advances

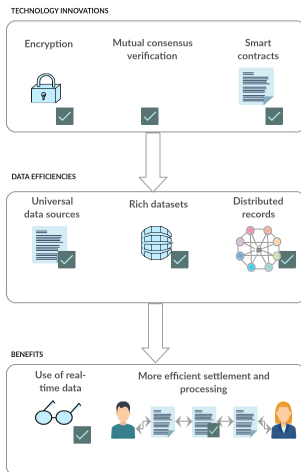
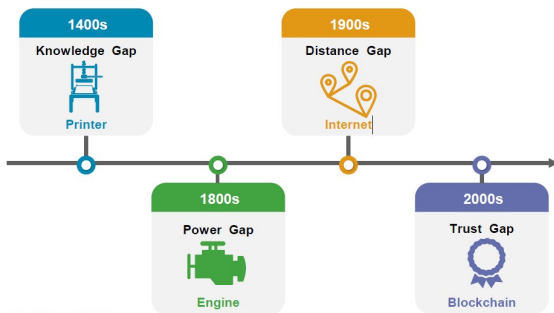


Figure: Recent distributed ledger technology and data science innovations

Innovations

Every century there has been a major innovation that has close existing gaps; Blockchain will play a key role in the Gap of the 21st century



Source: Richie Etwaru, TEDxMonticello

Figure: Important innovations. Source: Richie Etwaru.

Why Blockchain Can Potentially be Useful?

- Distributed ledgers come in several flavours:
 - A Unpermissioned public ledger (Bitcoin, Ethereum, and the myriad others)
 - B Permissioned public ledger (Ripple, etc.)
 - C Permissioned private ledger (R3 CEV and other similar projects)
 - D Traditional centralized ledger
- Mechanisms for controlling distributed ledgers:
 - A proof of work (pow)
 - B proof of stake (pos)
 - C third party verification, etc.

How to Choose a Ledger?

- What ledger is needed?
- Is there need to joint writing access?
- Who are the writers (are they known, are their interests aligned, can they be trusted)?
- Are there trusted third parties (one or several)?
- Do you want (need) to make transactions public or private, etc.?
- Think carefully before deciding which ledger to use!

Some Potential Applications

- Finance / Banking / Insurance:

- A Title deeds

- B Cryptocurrencies / Central Bank Digital Cash

- C Post-trade Processing

- D Local Payments / Global Payments

- E Trade finance

- F Rehypothecation

- G Syndicated loans

- Law / Government / Corporate Government

- Digital Identity / Cyber Security / Verified Data

- Health Care:

- A Records

- B Research

- Internet of Things

Sketch of Monetary Circuit

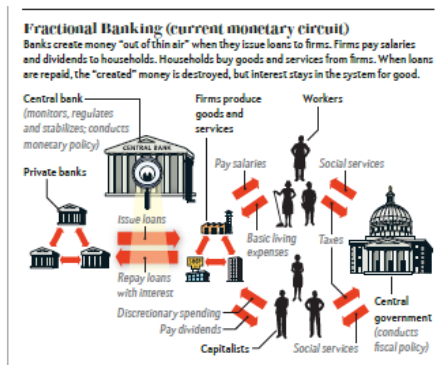


Figure: Sketch of monetary circuit. Source: Scientific American, vol 318, no 1.

Sketch of Monetary Circuit (cont.)

Bitcoin Setup

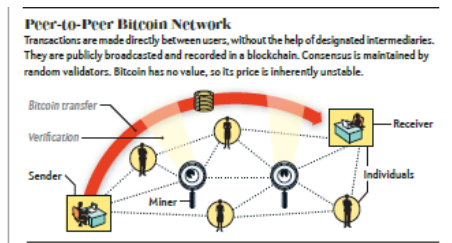


Figure: Bitcoin setup. Source: Scientific American, vol 318, no 1.

Bitcoin Deficiencies

- Bitcoin has no value
- Accordingly, its price vs a fiat currency or a representative basket commodities excessively volatile
- As a result, it cannot be used as a transaction currency (think of a mortgage taken in bitcoin in 2014)
- No can it be a unit of account or a store of value (it goes up and down massively)

Bitcoin is NOT Money

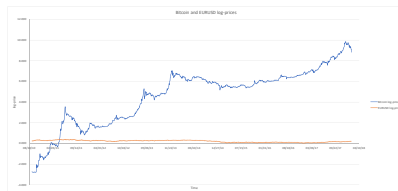


Figure: Bitcoin and Eur log-price. Sources - blockchain.info and FRED

Bitcoin is NOT Money

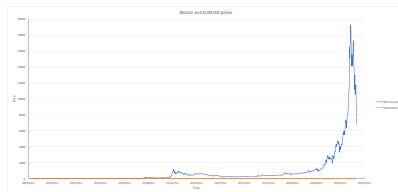


Figure: Bitcoin and Eur price. Sources - blockchain.info and FRED

Ripple Setup

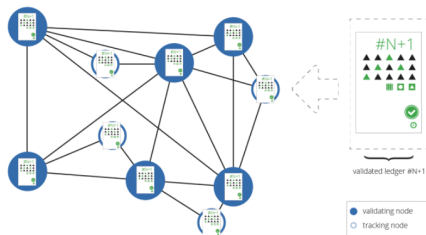
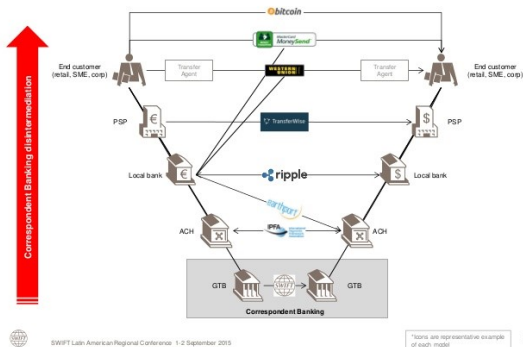


Figure: Ripple setup. Source: Ripple Labs.

Local Payments

Correspondent banking disintermediated at origination



SWIFT Latin American Regional Conference 1-2 September 2015

7

Global Payments, Current

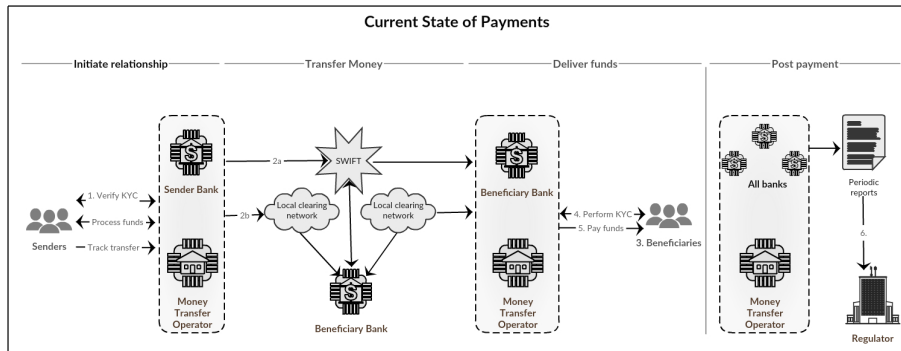


Figure: Global payments current (after WEF). Although existing payment system IS NOT broken (for instance, Gross Real Time Settlement works well), it is expensive

Global Payments, Future

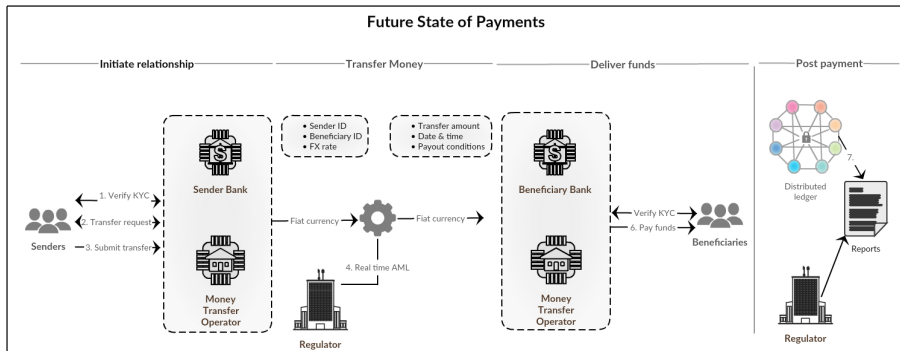


Figure: Global payments future (after WEF)

Central Bank Issued Digital Cash (CBDC)

- Potentially, central banks could issue digital cash
- CBDC opens way to a better monetary policy
- But also a possibility of pushing interest rates into a seriously negative territory and other controversial policies
- On the one hand, increasing tax collection, fighting crime, etc.
- On the other hand, excess control over ordinary citizens
- In principle, it would be possible to open a checking account at central bank directly, thus making retail banks obsolete
- In practice, it is more convenient to do by issuing licenses for narrow banks

Utility Settlement Coin (USC)

- CBDC is technically possible but politically complicated
- Hence several alternatives have been proposed
- One promising venue is USC, which is developed by a consortium of banks and a fintech startup called Clearmatics
- Initially, USC can be an internal token for a consortium of participating banks
- These coins have to be fully collateralized by electronic cash balances of these banks, which are held by the Central Bank itself
- Eventually, these coins can be circulated among a larger group of participants
- However, in this case, issuance of USCs has to be outsourced to a narrow bank

Narrow Bank

- In a nutshell, a narrow bank is a bank which cannot default for credit and liquidity reasons
- The main characteristic of a narrow bank is its assets mix which includes solely marketable low-risk securities and central bank cash in the amount exceeding its deposit base.
- As a result, such a bank can only be affected by operational failures, which can be minimized, but not eliminated, by using state-of-the-art technology, thus providing a maximally safe payment system.
- Accordingly, narrow bank deposits would be equivalent to currency, thus abolishing the need for deposit insurance with all its perverse effects on the system as a whole.
- We need a 100 percent Reserve Bank (C-PeRB). Assets: central bank reserves and currency; liabilities: demandable deposits and shareholder equity. C-PeRB is financed by a combination of deposits (debt) and shareholders' equity.

Historical Approaches to Asset-backed Currencies

- The idea of anchoring value of paper currency in baskets of real assets is old
- Gold and silver as well as bi-metallic standards have been used for centuries
- Two approaches are common:
 - A A redeemable currency backed by a basket of commodities;
 - B A tabular standard currency indexed to a basket of commodities.

Historical Approaches to Asset-backed Currencies

- Joseph Lowe (1822) was the first to explain how to use a tabular standard of value to the price inflation
- Poulett Scrope (1833) developed a similar plan based on a basket of 50 commodities
- William Jevons (1877) developed these ideas (much) further and proposed an indexation scheme based on a basket of a 100 commodities
- Alfred Marshall (1887) proposed a similar tabular standard
- Ever inventive Irving Fisher (1911) developed a mixed tabular/gold standard which he called 'compensated dollar' proposal

Historical Approaches to Asset-backed Currencies

- Frank Graham (1933), inspired by developments during the Great Depression developed an automatic countercyclical policy based on 100 percent backing of bank deposits by commodities and goods
- Benjamin Graham (1933) proposed backing the USD with a commodity basket at 60% and gold at 40%
- Friedrich Hayek (1943) extended proposals by Grahams to establishing a universal basket of commodities, which every country would use to back its currency
- John Maynard Keynes (1941-1943) proposed the bancor, an international currency defined in terms of a weight of gold. The bancor is supposed to be a multilateral transaction currency

Historical Approaches to Asset-backed Currencies

- Nicholas Kaldor (1963) proposed a new commodity standard, which he also called bancor, a commodity reserve currency
- Robert Hall (1982) wanted to define the USD in terms a basket of four commodities: ammonium nitrate, copper, aluminium, and plywood (ANCA)
- Xiaochuan Zhou (2009) proposed a new international reserve currency anchored to a stable benchmark

The Oil Market vs the Metals Market

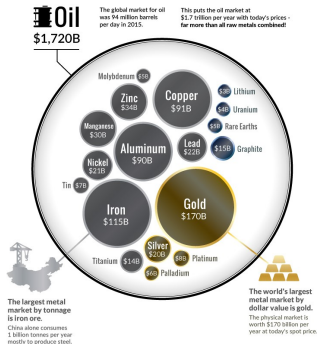


Figure: The oil market vs the metals market. Source: <http://www.visualcapitalist.com/size-oil-market/>

- USC is helpful from a technical perspective, but it does not solve issues of monetary policy.
- We wish to address this issue by building a counterweight for fiat currencies by backing the DTC by a pool of real assets
- We start with oil, but eventually expand to metals, crops, mooring rights, etc.
- Sponsors bring their oil to the pool administrator, who issues DTC in one-to-one ratio
- DTCs are sold to the public
- The corresponding fiat currencies are deposited with the affiliated narrow bank
- The proceeds are passed through to sponsors

- As a result, the administrator is in possession of real assets, sponsors with fiat currency, general public with DTCs, which can always be converted into fiat at the current market price
- The price P_{DTC} of DTC will be close to (but not exactly at) the market price of the corresponding asset pool, P_M
- Indeed, if P_{DTC} falls significantly below P_M , economic agents will put DTC back to the administrator, who will have sell a fraction of the pool's assets for cash and pass the proceeds to these agents
- If P_{DTC} increases significantly above P_M , sponsors will supply more assets to the administrator, who will issue additional DTC and pass them to sponsors, who will sell them for cash, just pushing the price down
- This mechanism ensures that $|P_{DTC} - P_M|/P_M \ll 1$, a very desirable feature, especially compared for conventional cryptocurrencies, habitually exhibiting extreme volatility
- At the same time, outright manipulation by central banks is not possible either

DTC Setup

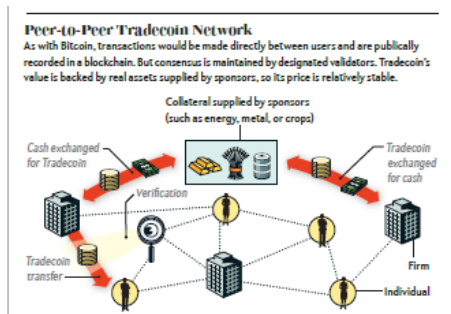


Figure: DTC setup. Source: Scientific American, vol 318, no 1.

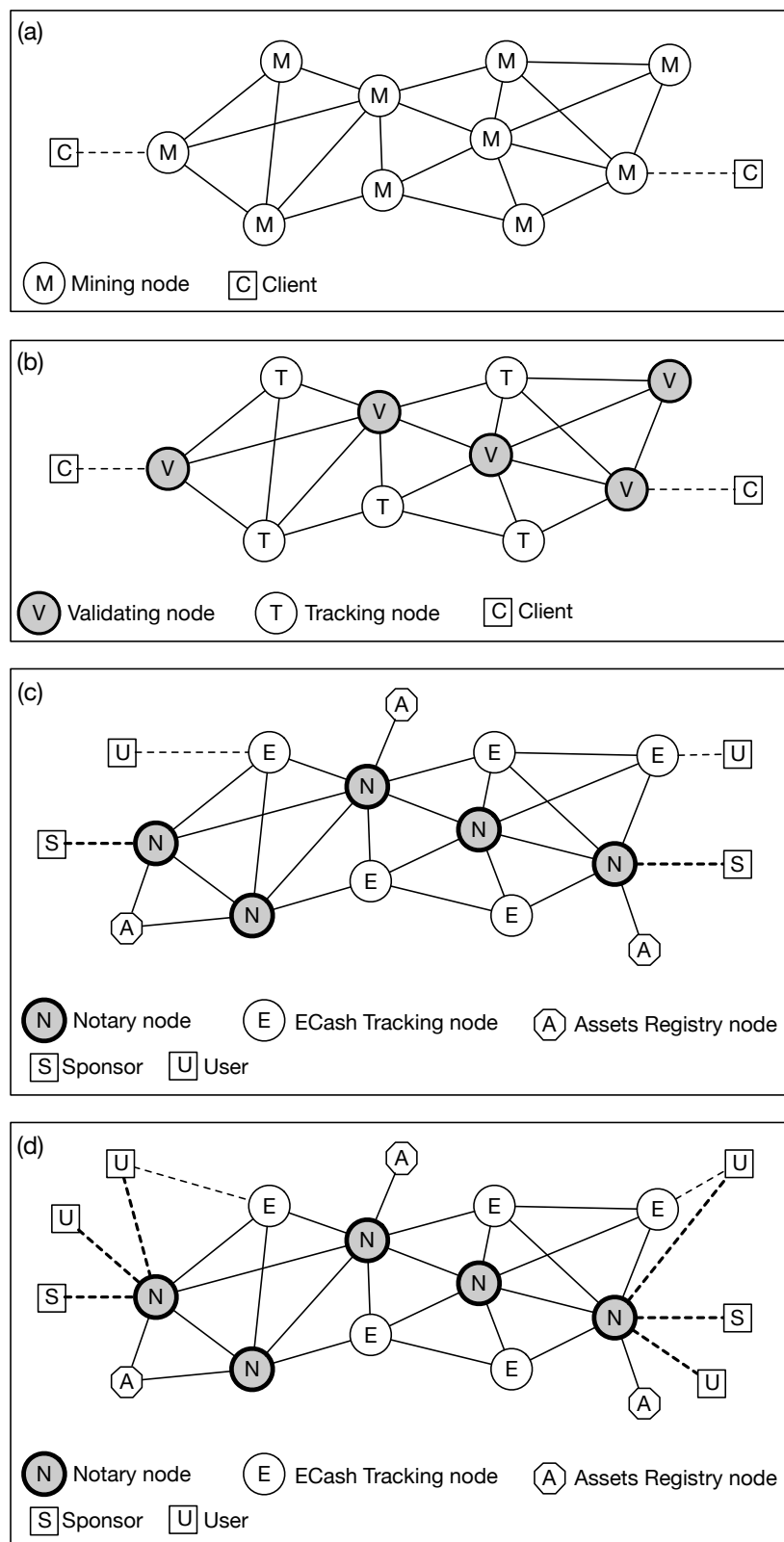


Figure 1. Comparison of different blockchain architectures: (a) Bitcoin; (b) Ripple; (c) DTC for Sponsors; (d) DTC for Sponsors and Users

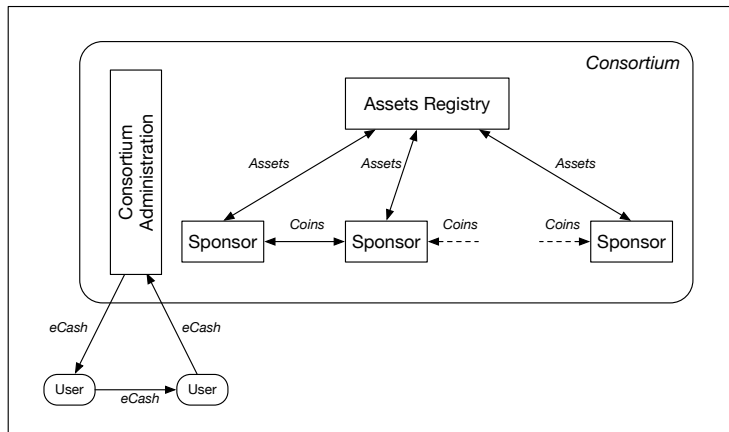
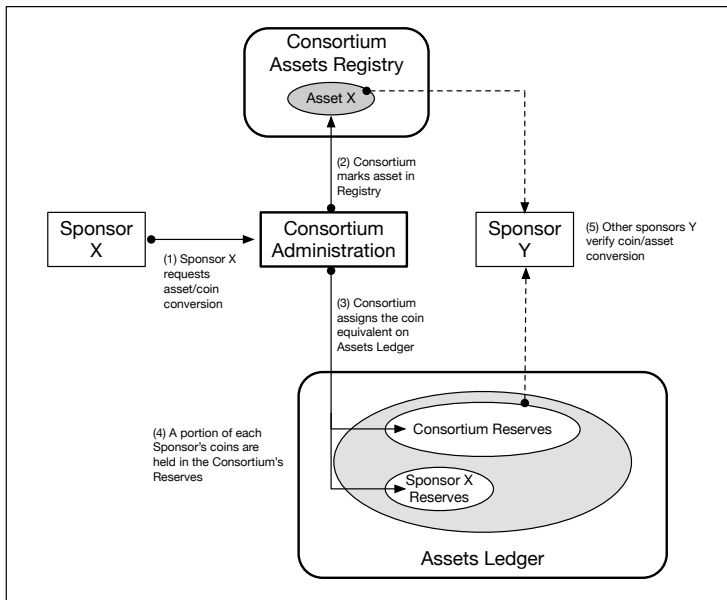
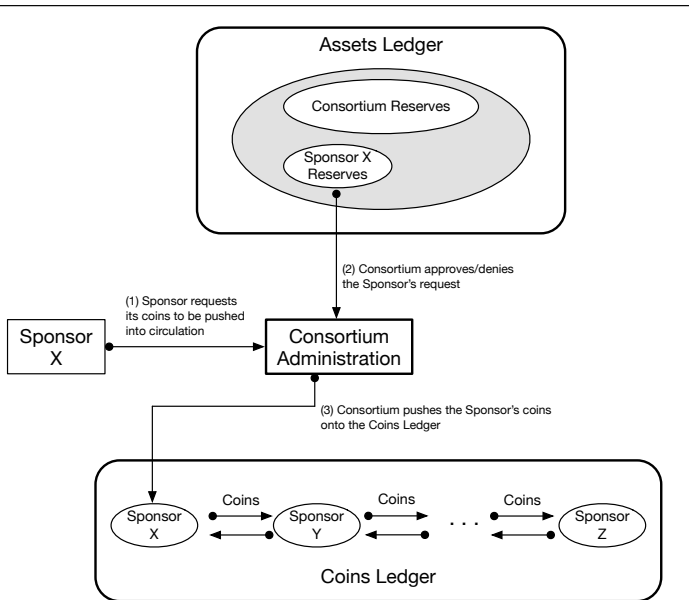


Figure: Tradecoin Entities

Converting Assets to Coins



Coins Ledger



DTC Setup

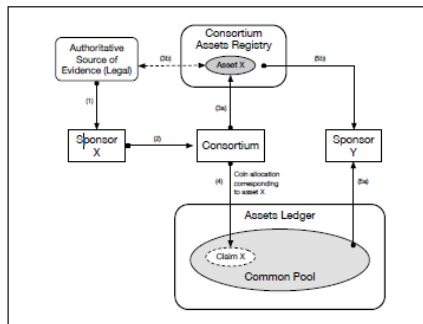


Figure: Conversion.

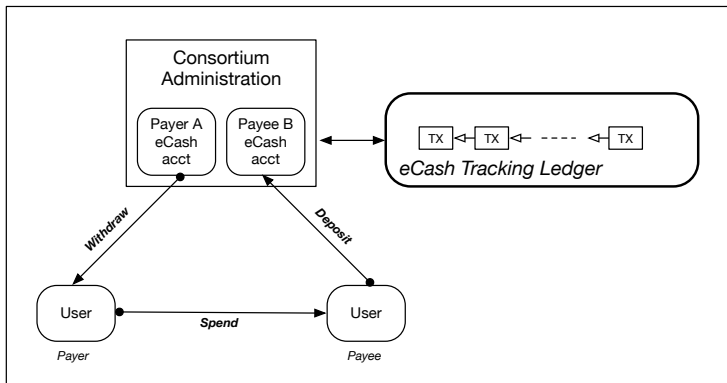


Figure: eCash Ledger

DTC Advantages

- DTC has real value
- Accordingly, its price vs a representative basket commodities has very low volatility
- The price of the DTC vs a fiat currency is more volatile but still much lower than the price of bitcoin.
- As a result, it can be used as a transaction currency (think of a mortgage taken in DTC in a country which is naturally aligned with some of the major constituent commodities)
- DTC can be used as a unit of account and a store of value (as much as gold or oil, say, can)

Conclusions

- The idea of distributed ledgers is not new
- Modern technology gives it a new lease of life
- Potentially, distributed ledgers have numerous applications in finance
- Cryptocurrencies are the best known but not the only ones
- Digital cash is very promising avenue
- If physical cash disappears, it is possible to imagine a future where everyone has direct access to central bank cash, albeit indirectly
- Retail banks may bifurcate into narrow banks and investment pools
- Asset-backed cryptocurrencies can serve as a much needed counterpoint for fiat currencies