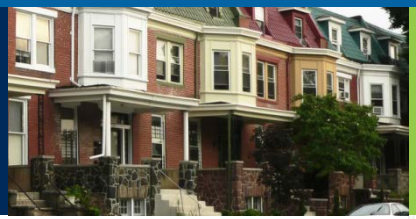
Blockchain 2.0

Mid-Atlantic Association of Financial Professionals
November 2016



Dave Beck

Senior Vice President & Regional Executive

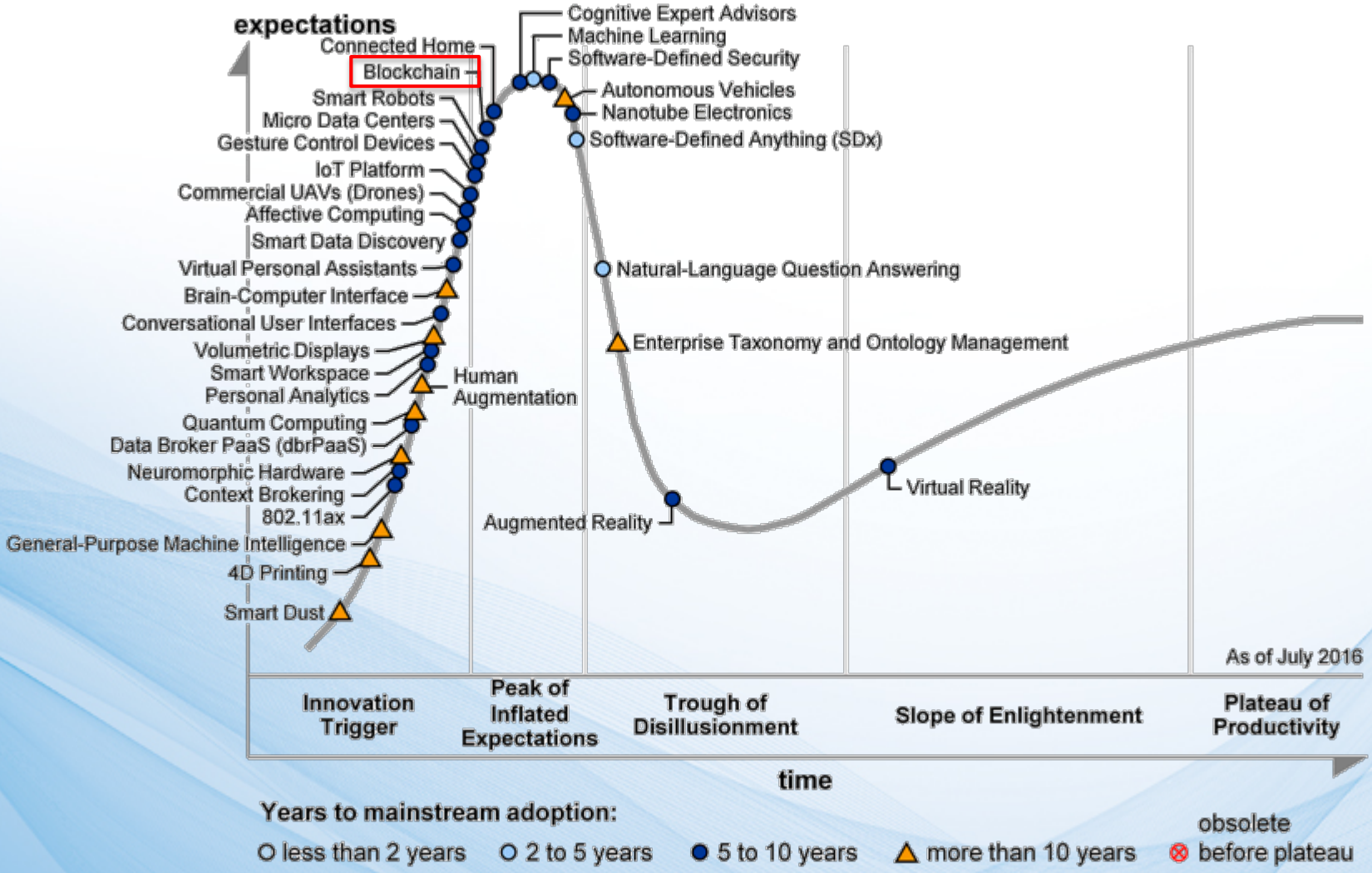
dave.beck@rich.frb.org

FEDERAL RESERVE BANK OF RICHMOND

Richmond ▪ Baltimore ▪ Charlotte

Blockchain and the Hype Cycle

Gartner's Hype Cycle for Emerging Technologies, 2016



Source: Gartner (August 2016)

It Started with a Whitepaper

The eight-page document described methods of using a peer-to-peer network to generate "a system for electronic transactions without relying on trust" and laid down the working principles of the cryptocurrency.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

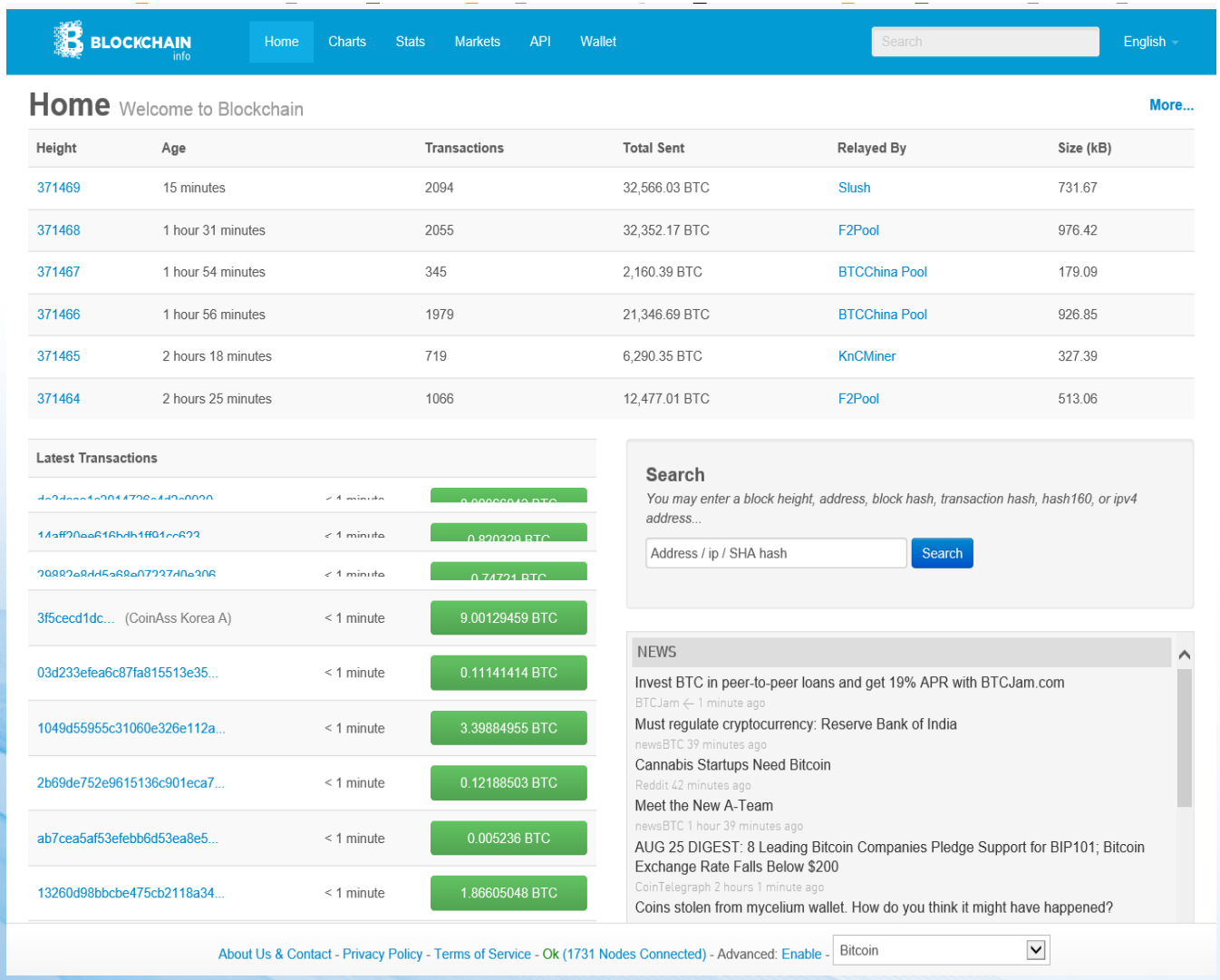
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

The “Double Spend” Problem

Early digital currencies had a problem preventing users from double spending a single digital unit of currency

Bitcoin solved this problem with lots of math!

Bitcoin and the Blockchain



Double spending is prevented using an extensive, decentralized network of computers, each holding a copy of the public ledger containing an audit trail of all bitcoin transactions. This is the “blockchain”.

Screen shot from blockchain.info

How the “blockchain” Gets Built

Start with a transaction between two bitcoin holders

To create a new block, miners must find a hash that meets specific requirements

- The hash requirement includes the header of the preceding block
- The hash must be less than or equal to the **target** number
- The hash must include a number called a **nonce**

Miners generate millions of hashes per second until the correct hash is found. If a miner generates a hash larger than the target number, then they increment a number called a **nonce** and try again. The new nonce will result in a new hash, and if still larger than the target, the nonce is incremented again and again until the target is reached.

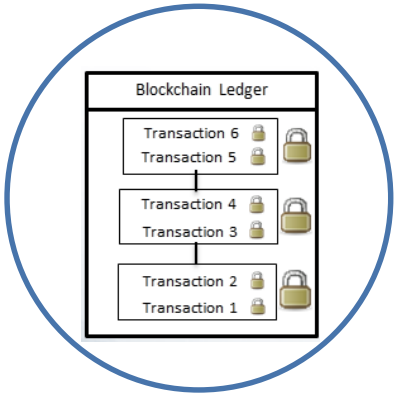
The target number is decided by every client connected to the Bitcoin network (ideally ever 2 weeks). It is lowered or raised in difficulty to make the next hash harder or easer to find. More miners results in a harder hash in order to maintain constant creation of a block every 10 minutes .

Since each block contains the hash of the previous block, they link together in a long chain (**blockchain**).

Bitcoins are **awarded** to the miner’s address that finds the hash and creates a new block. Initially every block solved rewarded the miner 50 **new Bitcoins**. This reward is halved approximately every four years. This slowly reduces the amount of coins released into the world over time. This controlled supply and release means that all possible 21 million Bitcoins will eventually be mined and that is all that will ever be available.

As Bitcoins are transferred from one wallet to another, these transactions are digitally signed and **stored publicly in the body of the block**.

Components of a Blockchain



Blockchain Ledger

- A transaction ledger where each transaction is tied to all of the previous transactions by making a cryptographic hash of the entire ledger every time there is a new transaction

Blockchain Distribution

- A system wherein all participants in the consensus model have a complete copy of the entire ledger
- Distribution can be public, or partial with security roles

Blockchain Consensus

- A process used with distributed ledgers that ensures that all parties can agree on the validity of transactions and of the entire ledger

The Blockchain

"Smart Contracts" are often considered a 4th Component

Note: "blockchain" and "distributed ledger technology" or "DLT" are not exactly the same, but are used interchangeably in most cases

Benefits and Challenges

Benefits

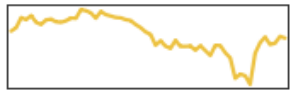
- **Cheaper, Relatively Faster Value/Ownership Transfer**
- **Real-Time Settlement**
- **Improved Data Auditability and Governance**
- **Provides Greater Resiliency by Minimizing Centralized Points of Failure**
- **Transparency and Immediacy**
- **Potential for Global Transaction Processing Systems**

Challenges

- **Scalability to Handle Large Transaction Volumes**
- **Security Issues When Private Key is Shared**
- **Confidentiality of a Public Blockchain**
- **Exception Processing**
- **Potentially Large Conversion Costs**
- **Enforceability in Existing Law**
- **AML/KYC Considerations**

Further Reading:
"The Great Chain of Being Sure About Things"
"The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the cryptocurrency."
The Economist (October 2015)
www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

Market Caps for Top Ten Cryptocurrencies

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$9,519,748,757	$599.36	15,883,296 BTC	$60,728,700	0.26%	
2	Ethereum	$1,120,639,356	$13.30	84,252,897 ETH	$22,911,600	1.69%	
3	Ripple	$244,094,572	$0.006884	35,458,607,580 XRP *	$1,382,870	-1.07%	
4	Litecoin	$181,118,832	$3.80	47,683,304 LTC	$1,342,360	-1.33%	
5	Monero	$133,878,427	$10.33	12,961,036 XMR	$3,249,040	1.19%	
6	Ethereum Cla...	$106,329,634	$1.26	84,206,819 ETC	$4,829,330	8.55%	
7	Steem	$79,283,915	$0.520271	152,389,648 STEEM	$486,582	11.67%	
8	Dash	$78,182,689	$11.57	6,757,830 DASH	$414,937	0.56%	
9	NEM	$47,564,640	$0.005285	8,999,999,999 XEM *	$48,781	-1.75%	
10	MaidSafeCoin	$38,569,413	$0.085226	452,552,412 MAID *	$98,746	-0.43%	

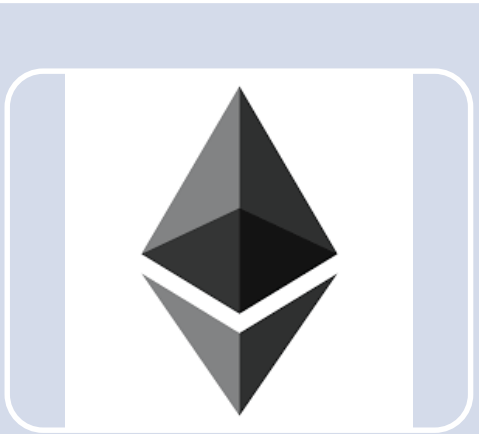
How Protocols Compare

Public

P2P & Business 2 Business

Simple program for one purpose

10 minute settlement



Public

P2P & Business 2 Business

Programmable Applications

14 second settlement

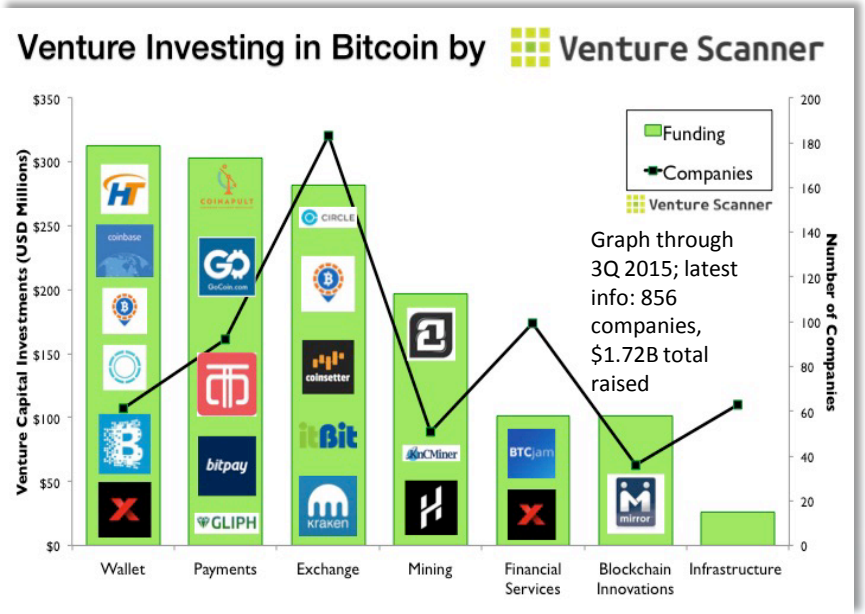
Permissioned

Bank 2 Bank

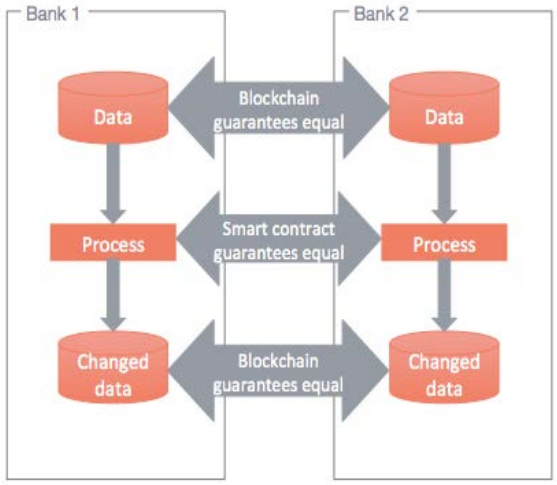
Simple program for one purpose

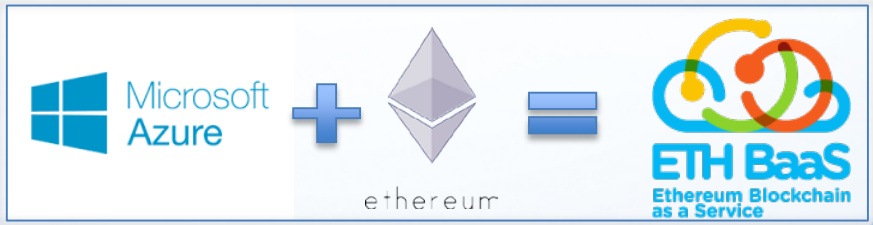
Near instant settlement

Continued Interest in Bitcoin & Ethereum



- Ethereum is a blockchain that can run "smart contracts"
- Runs on proof-of-work consensus model similar to Bitcoin but will switch to proof-of-stake
- The DAO hack resulted in the Ethereum blockchain splitting into two different blockchains





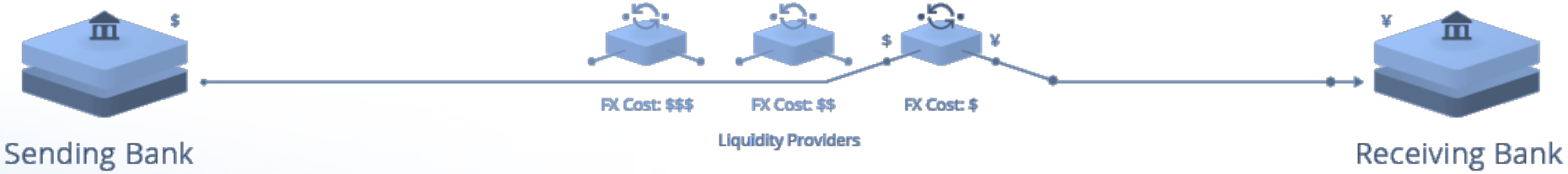
- Companies such as Abra and Circle use Bitcoin as a payments rail - users don't know they're using Bitcoins
- Bitcoin is starting to be seen by some as a safe haven investment due to global uncertainty, as well as an escape from failing economies.

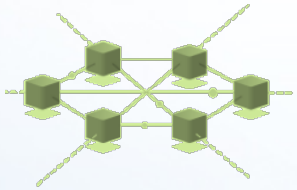
- Microsoft is providing developers resources to work on Ethereum
- UBS, Santander and other banks are using an Ethereum based blockchain to test a "settlement coin," as is the Bank of Canada [continued on slide 8]

Further Reading:
"Ethereum, a Virtual Currency, Enables Transactions that Rival Bitcoin's" New York Times, March 2016
http://www.nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enables-transactions-that-rival-bitcoins.html?_r=2

Disruptive FinTechs (Ripple)

Ripple's distributed financial technology allows for banks around the world to directly transact with each other without the need for a central counterparty or correspondent.





Ripple Network

The Ripple network contains the Ripple Consensus Ledger (RCL), a secure distributed ledger that uses the consensus process to settle transactions. Because of its distributed nature, it does not require a central operator, and offers transaction immutability and information redundancy. RCL holds the order book with bid/ask offers from payment initiators and market makers. Its path-finding algorithm enables it to find the lowest foreign exchange rate across all order books and currency pairs.

- Ripple has focused lately on the Interledger Protocol (ILP); marketing claims include:
  - Ripple's implementation of ILP connects bank and non-traditional payment networks to make sending payments "just as easy as sending emails"
  - At its core, Interledger is a web protocol for routing payments across independent networks
  - ILP provides the same benefits as other blockchain systems, including the certainty and auditability of transactions, but adds (theoretically) unbounded scalability with no transaction limits to meet customer demand

Images from Ripple
https://ripple.com/technology/

Banks and Financial Services

- Nearly every global bank is involved in at least one distributed ledger/ blockchain related initiative
  - Current strategy is to experiment and learn, rather than launch specific applications or place singular large bets
  - R3 working with over 50 global banks https://r3cev.com/
- According to the World Federation of Exchanges, 84% of world's trading venues and clearing counterparties are exploring/implementing a distributed ledger
- Much of the interest is in private ledgers
- Projects (and press announcements) are numerous
- Key areas being explored:
  - Global Payments
  - Trade Finance
  - Property and Casualty Claims Processing
  - Syndicated Loans
  - Automated Compliance
  - Proxy Voting
  - Asset Rehypothecation

Santander: Blockchain Tech Can Save Banks $20 Billion a Year

Yessi Bello Perez (@yessi_kbello) | Published on June 16, 2015 at 12:15 BST

NEWS

21 31 253 0

Blockchain technologies could reduce banks' infrastructural costs by $15-20bn a year by 2022, a new report from Santander InnoVentures claims.

The FinTech 2.0 Paper, produced in collaboration with Oliver Wyman and Anthemis Group, says distributed ledger technology could save banks money by eliminating central authorities and bypassing slow, expensive payment networks.

Beyond payments, its authors identify other areas of potential for distributed ledgers, noting:

> *"In time, distributed ledgers will support 'smart contracts' – computer protocols that verify or enforce contracts. This will lead to a wide variety of potential uses in securities, syndicated lending, trade finance, swaps, derivatives or wherever counterparty risk arises."*

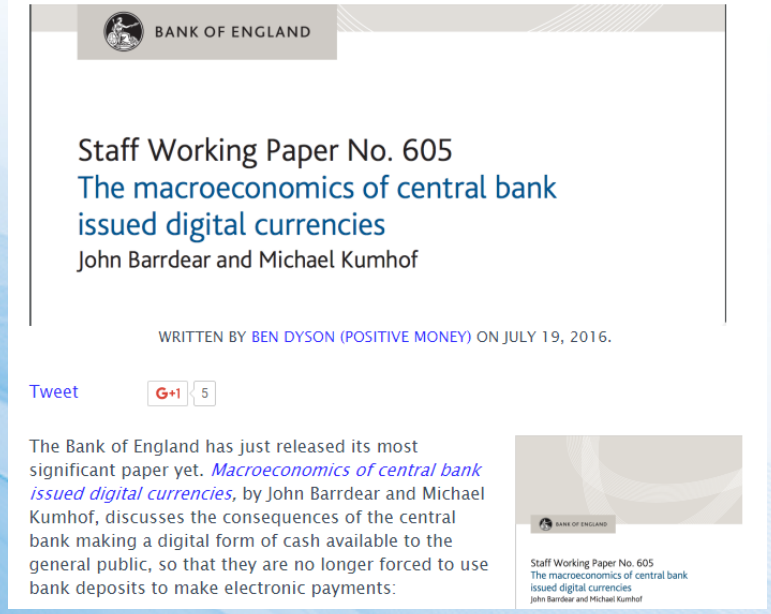
CoinDesk
http://www.coindesk.com/santander-blockchain-tech-can-save-banks-20-billion-a-year/

Further Reading:
"The Future of Financial Infrastructure"
"An ambitious look at how blockchain can reshape financial services"
World Economic Forum
http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

Possible Directions

Central Bank Explorations

Further Reading:
Staff Working Paper No. 605
The macroeconomics of central bank issued digital currencies
Bank of England (July 2016)
http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf



BANK OF ENGLAND

Staff Working Paper No. 605

The macroeconomics of central bank issued digital currencies

John Barrdear and Michael Kumhof

WRITTEN BY BEN DYSON (POSITIVE MONEY) ON JULY 19, 2016.

Tweet G+1 5

The Bank of England has just released its most significant paper yet. *Macroeconomics of central bank issued digital currencies*, by John Barrdear and Michael Kumhof, discusses the consequences of the central bank making a digital form of cash available to the general public, so that they are no longer forced to use bank deposits to make electronic payments:

Last updated: June 16, 2016 5:06 pm

Canada experiments with digital dollar on blockchain

Philip Stafford

Share Author alerts Print Clip Gift Article Comments

Brussels had agreed the deal with Ottawa, above, in 2013 but national parliaments have protested

Canada is exploring the creation of a digital version of its currency as central banks examine whether modern technology can create a new medium of exchange.

The Bank of Canada, the country's central bank, revealed in a private presentation in Calgary on Wednesday that it was working with the country's biggest banks to develop an electronic version of the Canadian dollar.

It is examining how to put a government-backed, or fiat, currency on blockchain, the digital ledger that underpins cryptocurrency bitcoin. Full adoption would mark a significant advance for the emerging technology.

More

ON THIS TOPIC

- "Project Jasper" involves issuing, transferring and settling central bank assets on a distributed ledger via a token named CAD-Coin
- Carried out with several of Canada's biggest banks, including Royal Bank of Canada, CIBC and TD Bank, as well as Payments Canada
- Uses intellectual property developed by R3, a New York blockchain consortium of more than 50 of the world's biggest banks
- Platform is Ethereum

Possible Directions

Central Bank Explorations

NEWS

The US Federal Reserve is 'Paying Close Attention' to Blockchain

Stan Higgins (@mpmcsweeney) | Published on October 7, 2016 at 21:30 BST

NEWS

419 133 2

Federal Reserve governor Lael Brainard delivered a speech on blockchain today, remarking that the technology could have a major impact on the financial system.

Brainard's speech, delivered to at the Institute of International Finance in Washington, D.C., represents what may be the US central bank's strongest words on blockchain to date. She detailed developments from a Federal Reserve-guided working group that is focused on financial innovation, an effort that, in part, is looking at the question of using the tech in next-generation payment and settlement systems.

http://www.coindesk.com/federal-reserve-paying-attention-blockchain/

- Cross-border payments and trade finance are some of the most promising areas to see the benefits of the technology
- "A smart contract would automatically execute payments on the specified schedule to the assigned owner over the life of the bond."
- "The industry may still be several years away from an application that is ready to fully implement."
- Different participants in the industry are working together to look for common approaches

- March 2016: Governor Brainard speech on "The Use of Distributed Ledger Technologies in Payment, Clearing, and Settlement" https://www.federalreserve.gov/newsevents/speech/brainard20160414a.htm
- June 2016: Fed hosts Blockchain and FinTech conference in DC; 90 central banks in attendance
- October 2016: Governor Brainard speech on "Distributed Ledger Technology: Implications for Payments, Clearing, and Settlement" https://www.federalreserve.gov/newsevents/speech/brainard20161007a.htm

Possible Directions

Other Developments / Use Cases

Further Reading:
Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World
Don Tapscott and Alex Tapscott (May 2016)

symbiont
Smart Securities, Intelligent Markets

Delaware is open for blockchain business

- Delaware, the state that incorporates the most companies, is exploring the use of blockchain technology to make its paperwork cheaper and more efficient
- Delaware's Blockchain Legal Ambassadors are collaborating with the Delaware Corporation Law Council to develop amendments to Delaware law
- New legal framework will be ready as early as the summer of 2017

Blockchain as a Service

- Providers like IBM and Microsoft are offering Blockchain as a Service with other Cloud offerings

https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business?language=en

Prosperity/Consumer Related Use Cases

- **Land Registry** - 70 percent of the people in the world who have land have a tenuous title to it
- **A Real Sharing Economy** - The big sharing-economy disruptors in Silicon Valley should be disrupted
- **Remittances** - Paying 2percent rather than 10 on moving money internationally
- **Protecting Personal Data** - The virtual you is not owned by you -- that's the big problem
- **Intellectual Property** - The money should flow back to the creative artists, and they should control the industry, rather than powerful intermediaries

Possible Directions

Summary of Use Cases