



Blockchain

Technical Principles and Practical Use Cases

The blockchain changes the entire equation of trust for everything

The Economist

The real innovation is not the digital coins themselves, but the trust machine that mints them—and which promises much more besides.

Goldman Sachs

Silicon Valley and Wall Street are betting that the underlying technology behind the Blockchain, can change... well everything.

IBM

"Blockchain, as a technology, is extremely interesting and intriguing," said Arvind Krishna, senior vice president of IBM Research.

ANDREESSEN HOROWITZ

"In 20 years, we'll talk about Bitcoin like we talk about the Internet today" - Marc Andreessen, Andreessen Horowitz

Governments afraid to fall behind on blockchain technology



China

周小川: 区块链技术是一项可选的技术, 人民银行部署了重要力量研究探讨区块链应用技术

11/09/2016



UK

UK Chief Scientist Report to UK Government - Government should establish trials of distributed ledgers to assess the technology's usability within the public sector."

Jul 18, 2016



US

The US Securities and Exchange Commission (SEC) has approved Overstock's plans to issue stock via the blockchain.

Dec 16, 2016



Japan

Japan's Financial Services Agency (FSA) considering legislation to classify digital currencies as currency.

11/02/2016



Hong Kong

John Tsang (HK Financial Secretary) Government will encourage exploring applications of Blockchain technology in financial services. US\$2.5Bn Fin-Tech investment in 2016-2017 budget.

11/06/2016



Korea

The Korea Exchange (KRX) to create an over-the-counter (OTC) trading platform using blockchain tech.

11/01/2016



Singapore

The Monetary Authority of Singapore, the city-state's central bank, has funded a blockchain system as part of a five-year US\$225m Fin-Tech investment plan.

10/18/2016

The blockchain will reshape entire industries' operating models



What is the blockchain

A block is created when multiple nodes agree and validate the transactions. "Distributed ledger" comes from the fact that there is no need for a centralized party to validate a transaction.



Centralized



Distributed



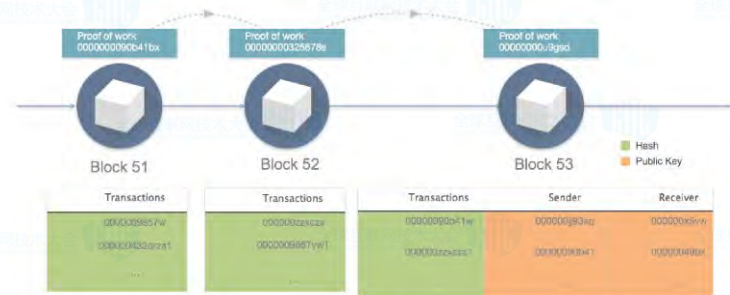
Decentralized

Most secure distributed ledger consensus mechanism:

PROOF OF WORK (PoW) – An economic measure to deter ledger hacking by requiring work from the service requester, usually in the form of computer power over a period of time.

How blockchain transactions work

Blockchains solve two major challenges for digital transactions, controlling the information and avoiding duplication.



- ID referred to as a "hash" called "proof of work." This is a random set of encrypted digits.
- Public key identifies the sender and receiver
- Transactions numbering from one to many thousands are included in each block.

Flow of a transaction on the blockchain

• Counterparty A sends funds to Counterparty B



• The transaction is configured into a block.



• The transaction is broadcast across the entire network which validates it



• Counterparty B receives funds from Counterparty A



• The block is then added to the chain which records the entire non-reversible history of transactions in a public ledger



Myths and Truths about the Bitcoin Blockchain



Myths about the Bitcoin Blockchain

Many hold the incorrect view that Bitcoin is outdated, slow, first gen. prototype technology

Myth 1

Bitcoin can only handle ~ 7tps

?

Myth 2

Bitcoin is slow, transaction confirmations take 10-60 minutes

?

Myth 3

Bitcoin is expensive, micro-transactions cannot use Bitcoin

?

Myth 4

Bitcoin code is not turing complete, cannot do smart contracts

?

Where does this number come from?

One 1MB size block every 10 minutes. Basic transaction size is 250 bytes.

$1,000,000 \text{ bytes} / 10 \text{ min} / 60 \text{ sec} / 250 \text{ bytes} = 6.6 \text{ tps}$

Two camps have solutions to these problems.
Who and what are they?

What is the Bitcoin Blockchain?



Camp 1

“Bitcoin is a
censorship resistant
settlement network”

Focus: Ensure on-chain
decentralization

Solution: Build layer 2 solutions
on top of decentralized
Bitcoin i.e. Lightning
Network , Sidechains.



Camp 2

“Bitcoin is a
peer-to-peer currency”

Focus: Ensure on-chain
transaction
throughput

Solution: Increase block size to
allow more on-chain
Bitcoin transactions
at low fees.

Different outlooks on the future of Bitcoin Blockchain

🚩 Camp 1

"Can scale - Build layers on top of Bitcoin (Eg. Lightning, Sidechains) "

- 7 billion people roll 2 payment channels per year
- 133 MB blocks – unlimited transaction amount
- 3 Mbits/sec with IBLT

🚩 Camp 2

"Does not scale - Increase the block size"

7 billion people making 2-blockchain transaction per day

Bigger blocks = Centralization

-24 GB blocks

-3.5 TB / day

-1.27/PB / year

Very few full nodes

Very few miners

Default inability to verify the blockchain

Bitcoin Lightning Network - Solves speed, block size

- Payment channels between multiple parties in a multi-hop hub and spoke model (similar to internet routing)
- Minimally trusted intermediaries (cannot take your coins)
- With a malleability soft fork, Bitcoin can scale to billions of transactions per day

The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments

Joseph Poon Thaddeus Dryja
joseph@lightning.network rx@awsonet.org

January 14, 2016
DRAFT Version 0.5.9.2

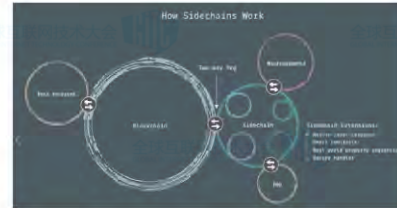
Abstract

The bitcoin protocol can encompass the global financial transac-

Bitcoin Sidechains - Solves innovation with multiple blockchains

"Conceptually, we would like to transfer an asset from the (original) parent chain to a sidechain, possibly onward to another sidechain, and eventually back to the parent chain, preserving the original asset. Generally we can think of the parent chain as being bitcoin and the sidechain as one of many other block chains."

Example Sidechain:
Rootstock to bring Ethereum smart contracting language to BTC



Enabling Blockchain Innovations with Pegged Sidechains

Adam Back, Matt Corallo, Luke Dashij,
Mark Friedenbach, Gregory Maxwell,
Andrew Miller, Andrew Poelstra,
Jorge Timón, and Pieter Wuille¹
2014-10-27 (revision 5523e43)

Abstract

©2014-2015 by the author(s). All rights reserved. This work is licensed under a Creative Commons License.

Global exchanges CEOs recognize blockchain opportunity



ASX

"We're having a very close look at this. The timing is almost perfect. Where blockchain can make an enormous difference, we're having a look at whether this is a way to transform our equity markets." — ASX CEO Elmer Funke Kupper

Goldman
Sachs

Silicon Valley and Wall Street are betting that the underlying technology behind the Blockchain, can change... well everything.

NASDAQ

"Blockchain applied to the private market is innovation built on top of innovation, and carries with it the opportunity to forever alter the future of financial services infrastructure."
— Bob Greifeld, CEO, Nasdaq



UBS

"I believe that blockchain technology will not only change the way we do payments but it will change the whole trading and settlement topic," — Oliver Bussmann, CIO of UBS

Timeline of major projects taken by institutions and exchanges

J.P.Morgan

JPMorgan Partners With Digital Asset for Blockchain Trial



ASX now actively working to employ blockchain (distributed ledger) technology to potentially replace its equities settlement systems.



Opening a technology lab in London to explore using blockchain technology in financial services.

NASDAQ

Implementing the bitcoin blockchain technology in its Nasdaq Private Market, a marketplace for pre-IPO trading, to expand and enhance the equity management capabilities it offer.



The Korea Exchange (KRX) South Korea's lone securities exchange, is reportedly moving to create an over-the-counter (OTC) trading platform using blockchain tech. Aims to help its OTC traders reduce the cost of transactions. Help off-board dealers to trade more easily by saving their costs and efforts in seeking trade partners."

Case Study: Nasdaq Linq solving Private Share trading

NASDAQ



- Individual shareholder certificate on the blockchain

What Nasdaq Linq does?

Digitize, integrate, control all equity-related functions

- Cap table management
- Shareholder liquidity
- Investor relations
- Capital raising



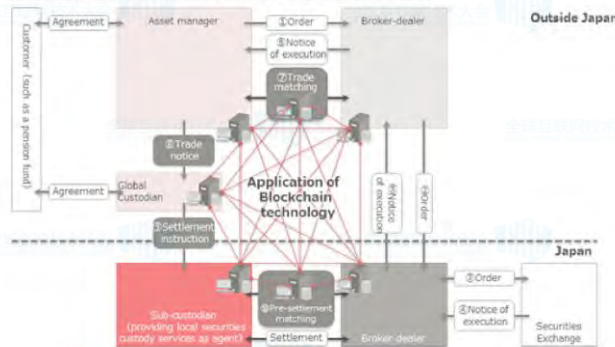
- Company ownership view on a blockchain

Case Study 2: Mizuho Bank - Cross-border trade settlement

MIZUHO

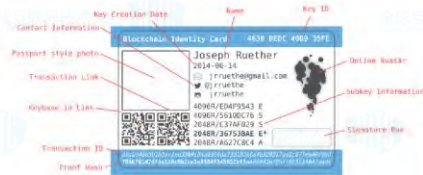
"The trade is the settlement."
Blockchain for international trade settlement

Flows in new post-trade settlement process for cross-border transactions



Case Study 3: Onename - Identity on Blockchain

onename



Choose a unique name

This is the name you share so others can find your blockchain ID. If you keep your password safe, no one can take this name from you.

Create and verify your profile

Link your blockchain ID and social media profiles together to prove ownership of your blockchain ID and verify it's really you.

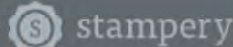
Start using your blockchain ID

Share your blockchain ID on your website, social media profiles, and business cards so people can easily find you online.

Case Study 4: 21 Inc - Micropayment on Blockchain



Case Study 5: Stampery - Notary on Blockchain




Proof of Ownership
Certify that a file or email is authored by you.


Proof of Existence
Certify that a file or email existed at a certain point of time.


Proof of Integrity
Certify that a file or email was not tampered with.


Proof of Agreement
Get 1-click agreements between parties without leaving your email.


Proof of Receipt
Certify that a specific recipient read your email at a certain point of time.

✓ **Total Accountability**
No more need of trust in insiders or third parties. We replace trust with mathematical proof.

✓ **Legally Valid**
Blockchain-based hashing and time stamping make for exceedingly strong evidence of the authenticity of a document.

✓ **Easier Auditability**
For the first time in human history, an immutable layer of transparency removes friction from your auditing needs.

✓ **Absolute Security**
All evidence and audit trails generated by Stampery are 100% counterfeit-proof and verifiable by independent third parties.

✓ **Secure Attribution**
Secure your data and mitigate risks with mathematical attribution that cannot be tampered with.

✓ **Infinite scalability**
Thanks to our technology, we can stamp exabytes of data on the blockchain. We also have an API.

Case Study 6: IBM - IoT on Blockchain



Figure 4. *To be safe, scalable and efficient, Internet of Things networks must be re-architected to gradually shift from managing billions of devices to hundreds of billions of devices*

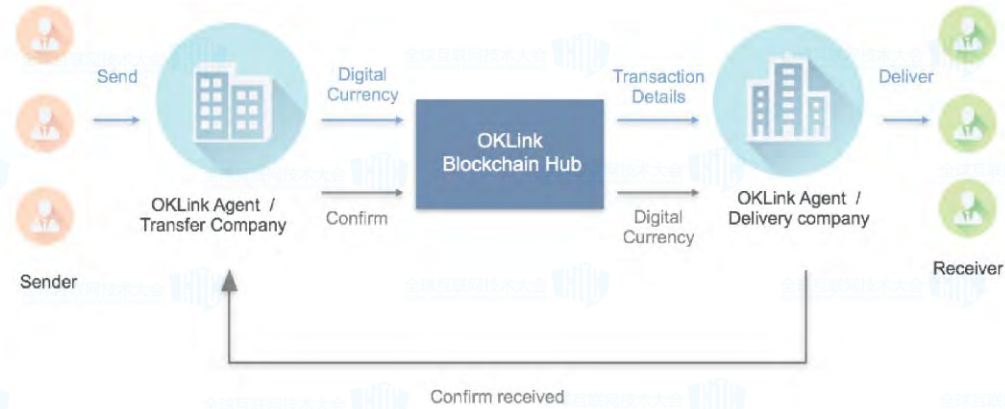


Figure 5

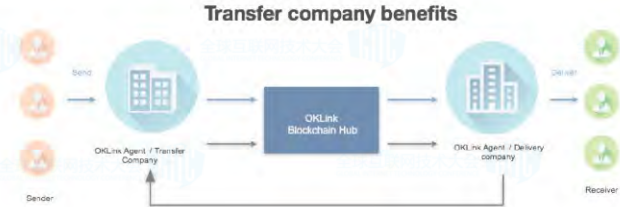
The blockchain functions as a universal digital ledger facilitating various types of IoT transactions between devices



Product -OKLink chain Network Flow



Offer improved experience for transfer companies



Access

At corners



Speed

Instant settlement



Cost

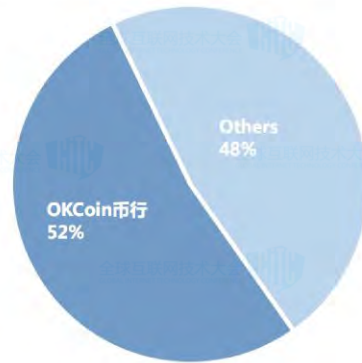
Capital efficiency
using digital currency



Reliability

Real-time confirmation
of receipt

Company performance -Market Share



Product -- OKCoin digital asset exchange





扫描二维码 获取更多区块链资讯