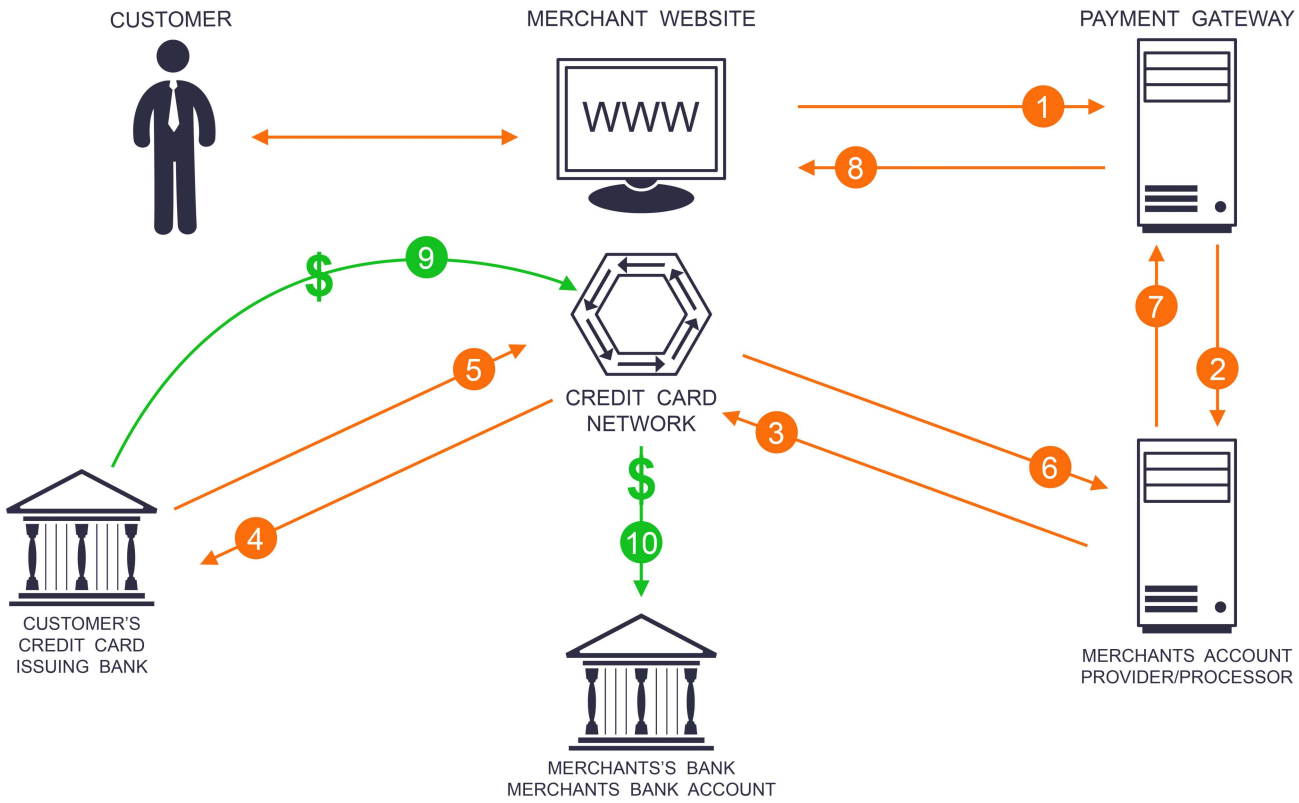
Bitcoin & Blockchain

Agenda

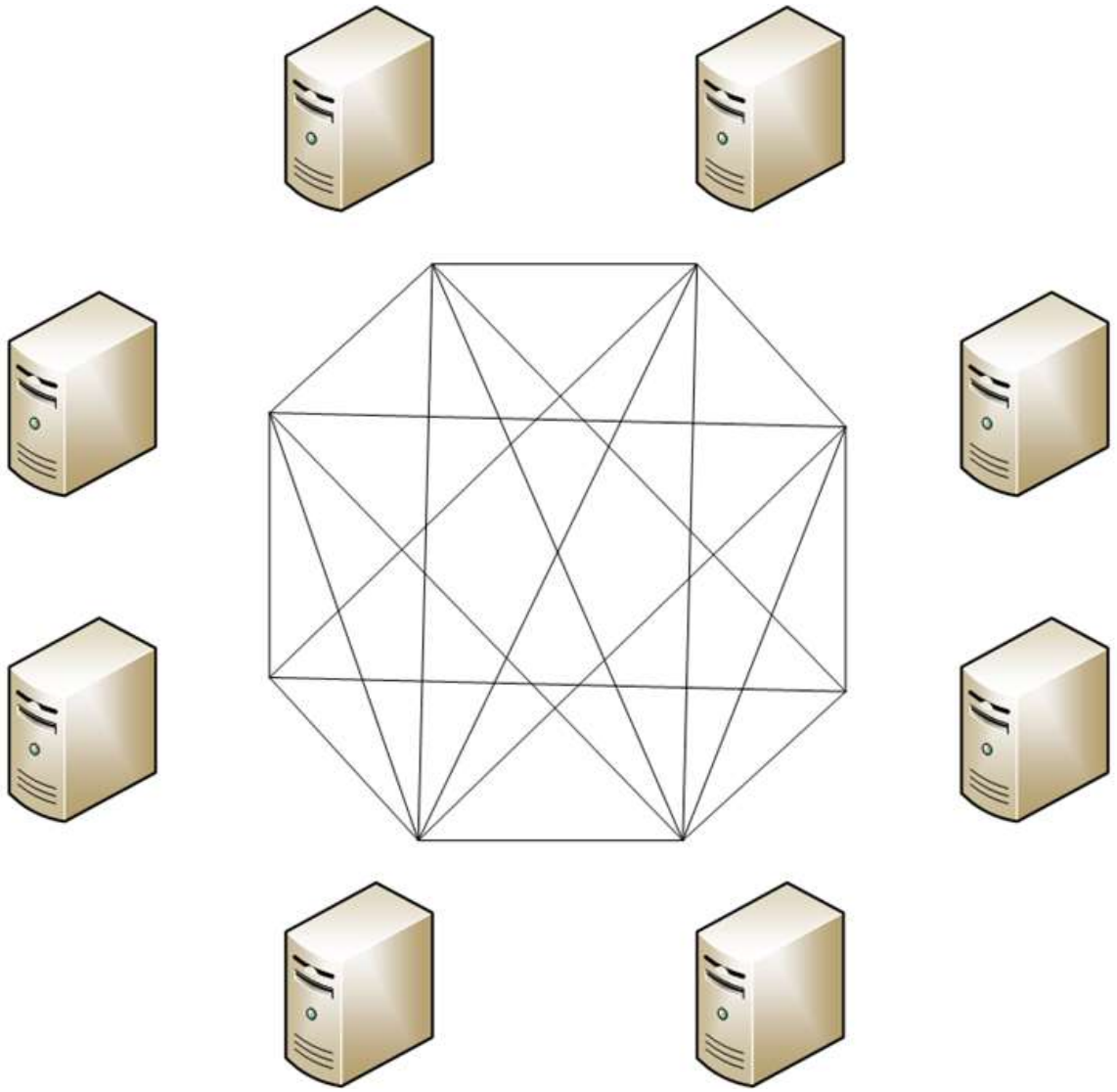
1. Financial Services Landscape
2. Bitcoin
3. Blockchain
4. Beyond Bitcoin

Financial Services Landscape

Credit Card Payment Process



Mesh of Servers



Centralized System

Bitcoin

Bitcoin

Was invented by an unidentified one under the name of `Satoshi Nakamoto`.

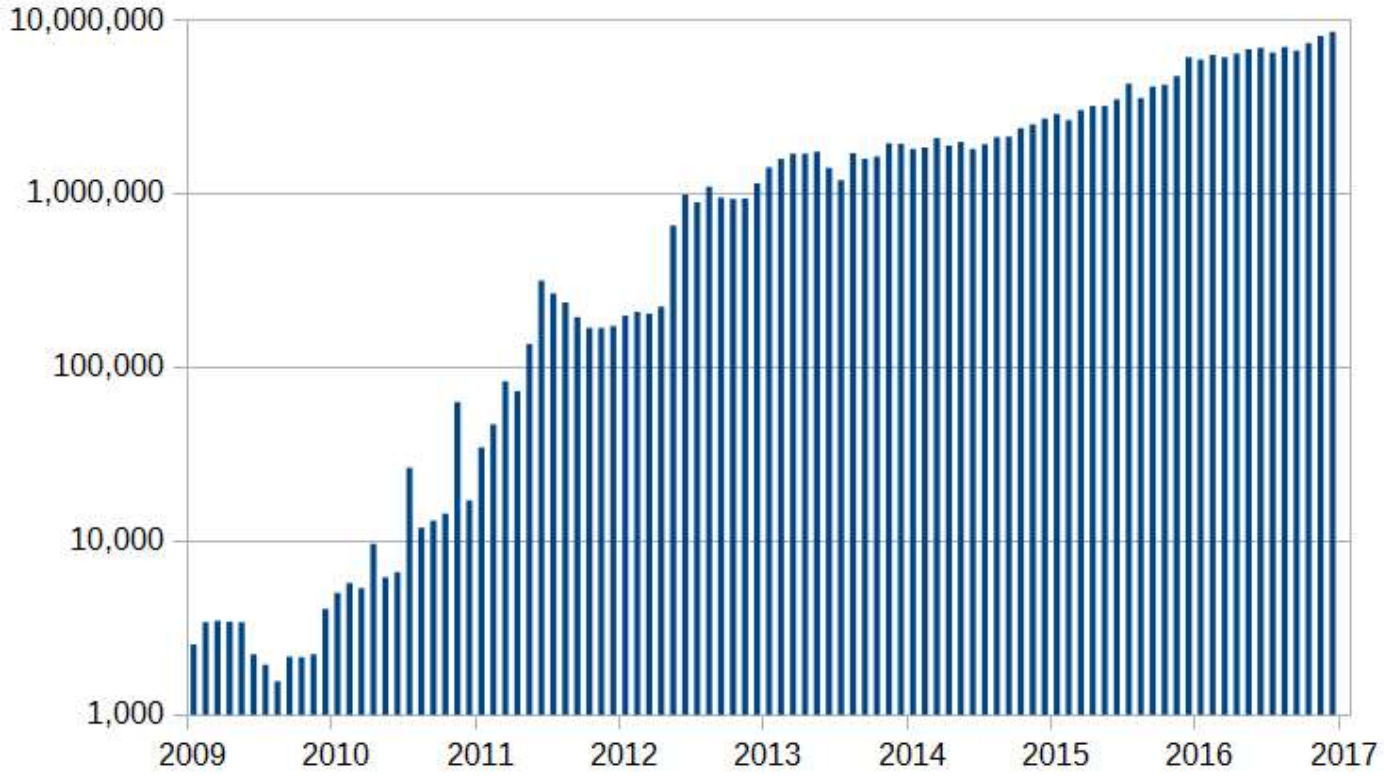
- Bitcoin was introduced on 31 October 2008 to a cryptography mailing list
- and released as open-source software in 2009.

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

Number of Bitcoin transactions per month

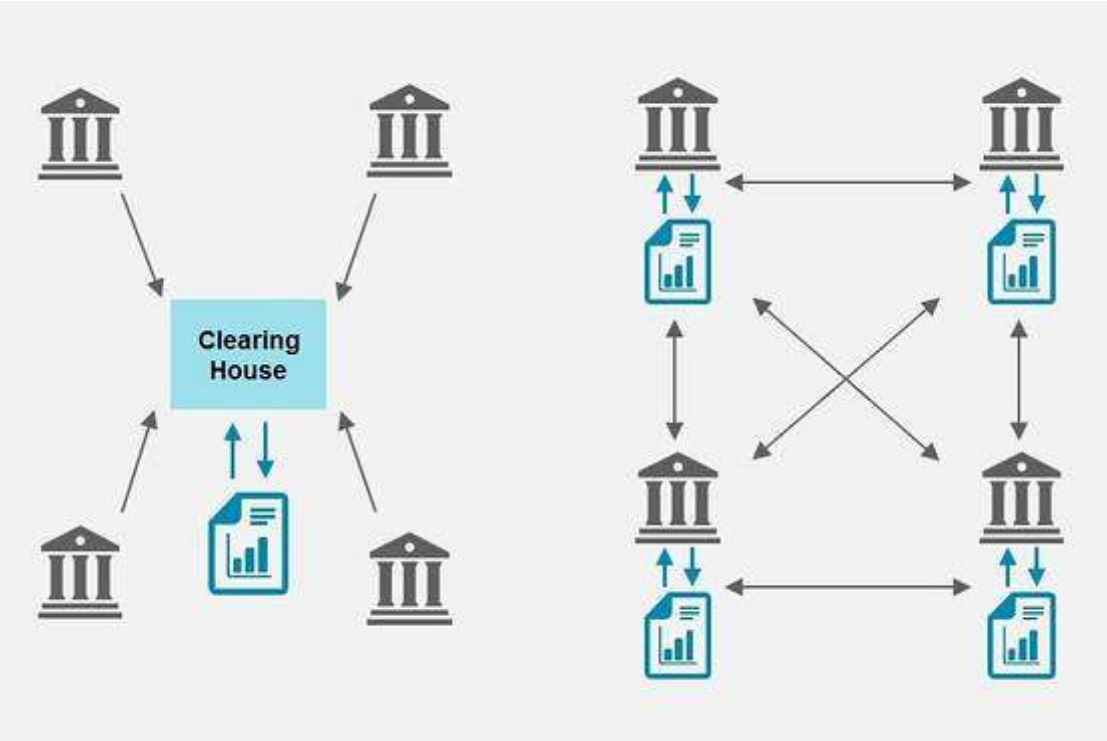


Using Bitcoin

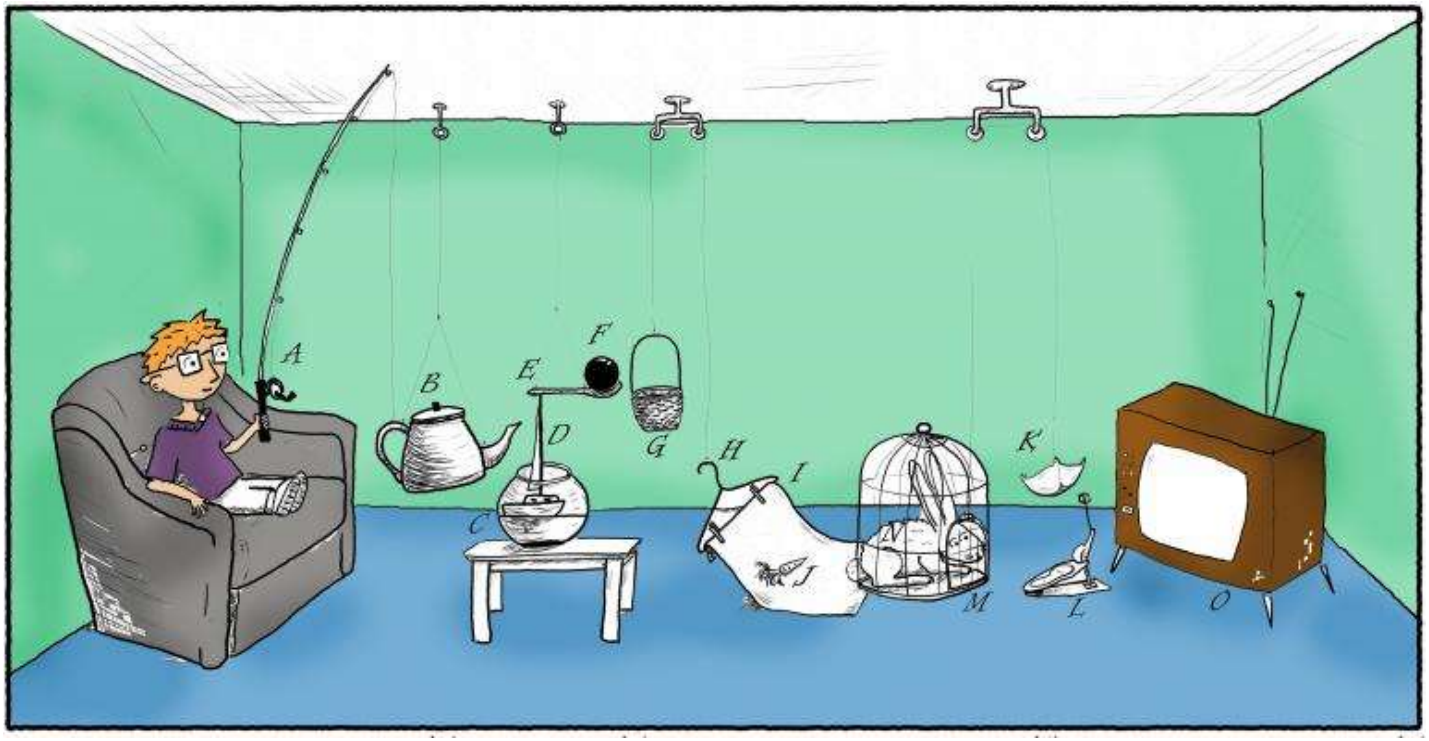
Source:
https://en.wikipedia.org/wiki/Bitcoin

Rethinking Financial Services

BTC challenges the Centralized Systems!



Rube Goldberg Machine?



Financial Systems face BTC pressure

- The monetary system of Bitcoin challenges the banks' role
- More researches on digital currencies are expectedly conducted
- The technology's potential capability in solving the challenge of 'how to establish trust – the essence of money – in a distributed network'.

Source: http://fintechnews.ch/blockchain_bitcoin/central-banks-face-bitcoin-pressure/3819/

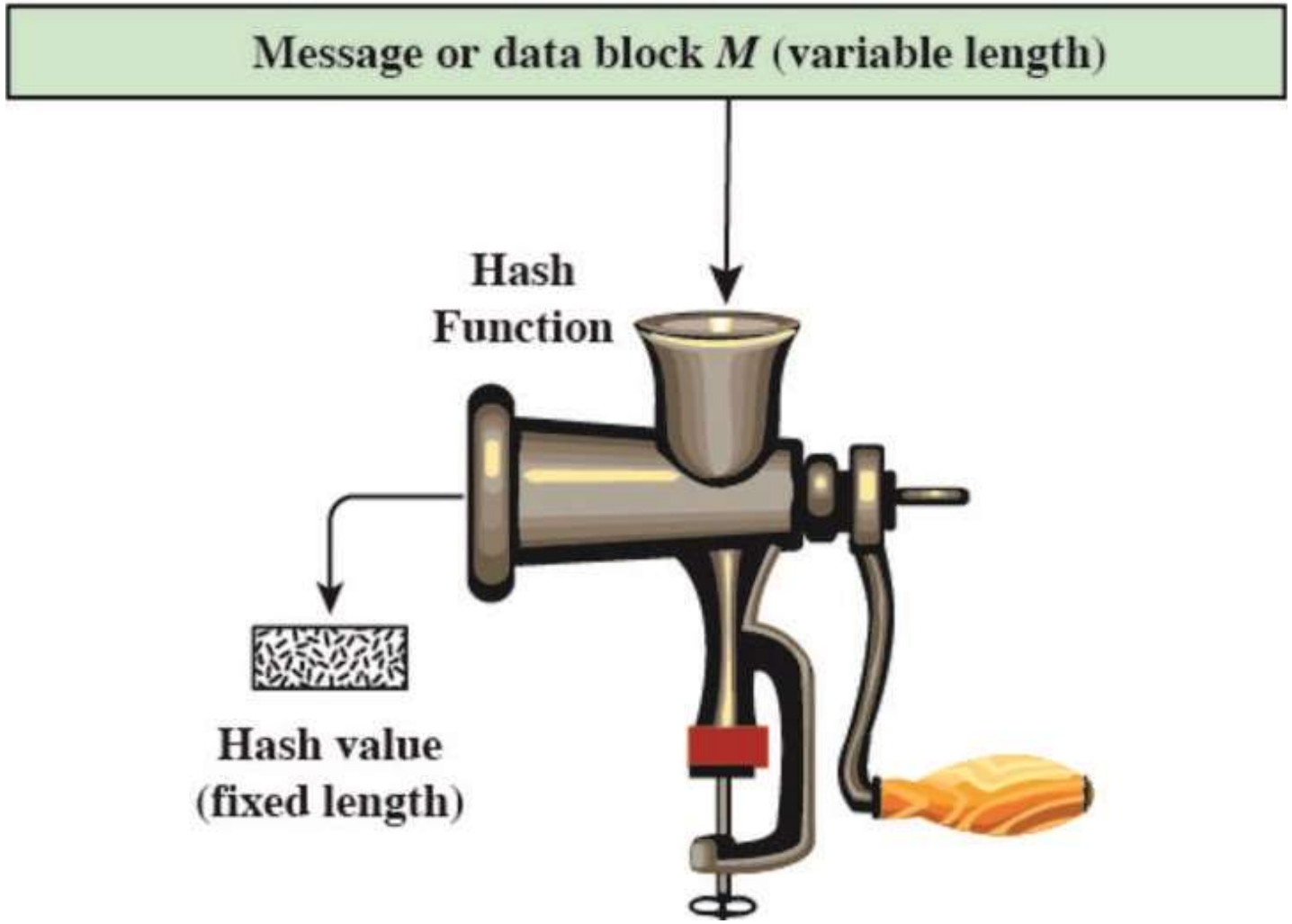
Blockchain

- Bitcoin concepts show us the potential capability to many systems.
- Algorithm behind bitcoin is the `Blockchain`.
- The Blockchain shows us how to solve the trust problem using `Mathematics`, especially in the subject of `Cryptography`.

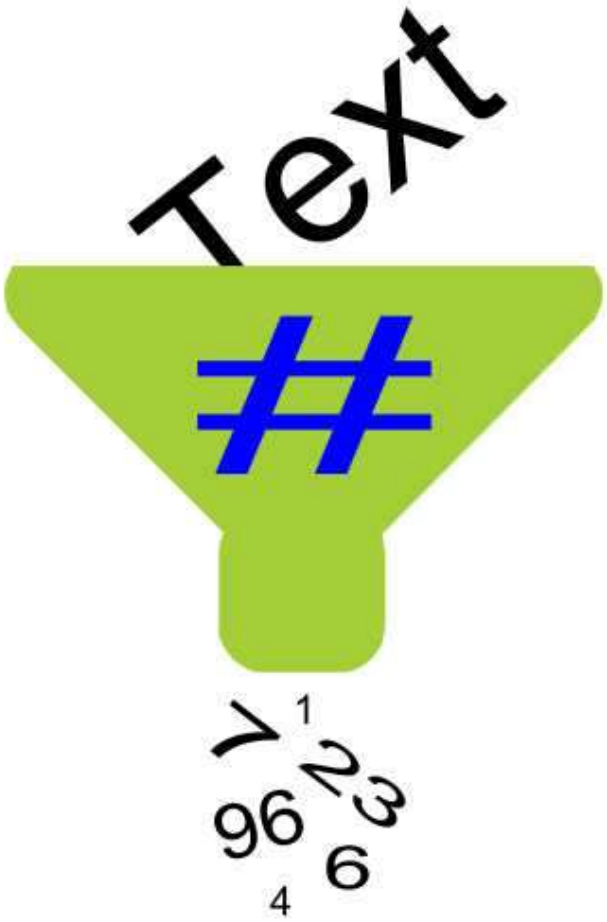
Establishing Trust in Legacy System

- OTP
- 3-D Secure
  - Verified by Visa
  - MasterCard SecureCode
  - J/Secure
  - American Express SafeKey

Cryptography



Digital Fingerprint



Hashes are a bit like fingerprints for data.

A given hash uniquely represents any arbitrary collection of data.
At least in theory. This can represent unique items

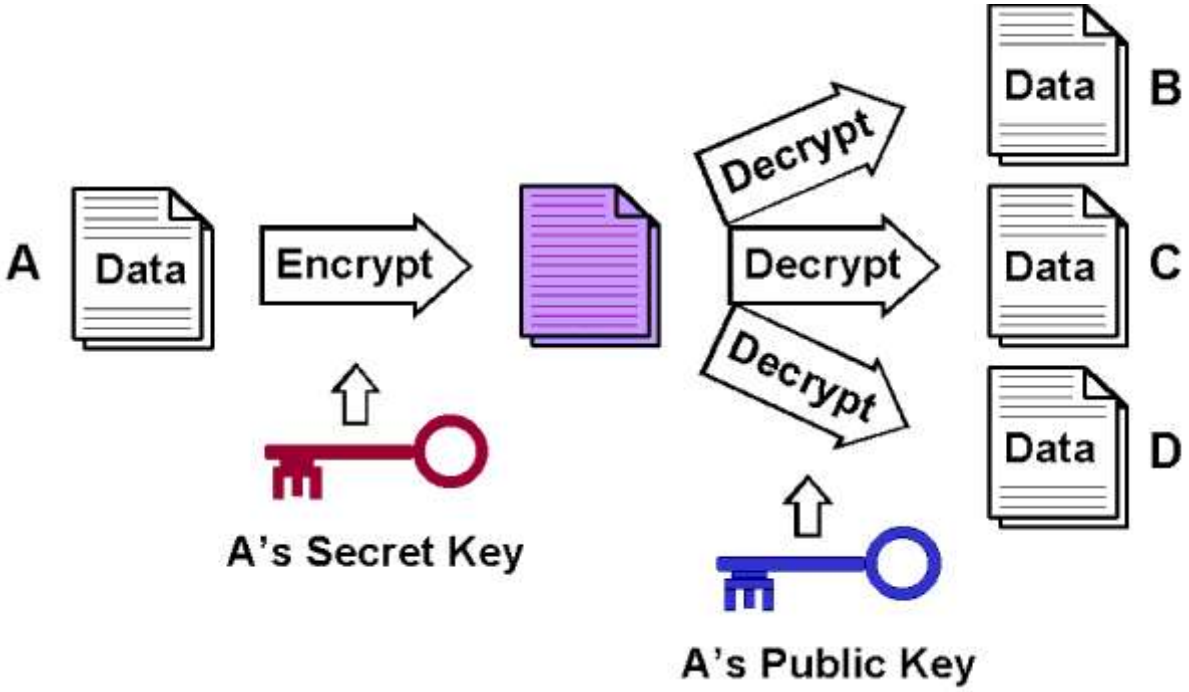
=

```
79054025
255fb1a2
6e4bc422
aef54eb4
```

Number as a Key

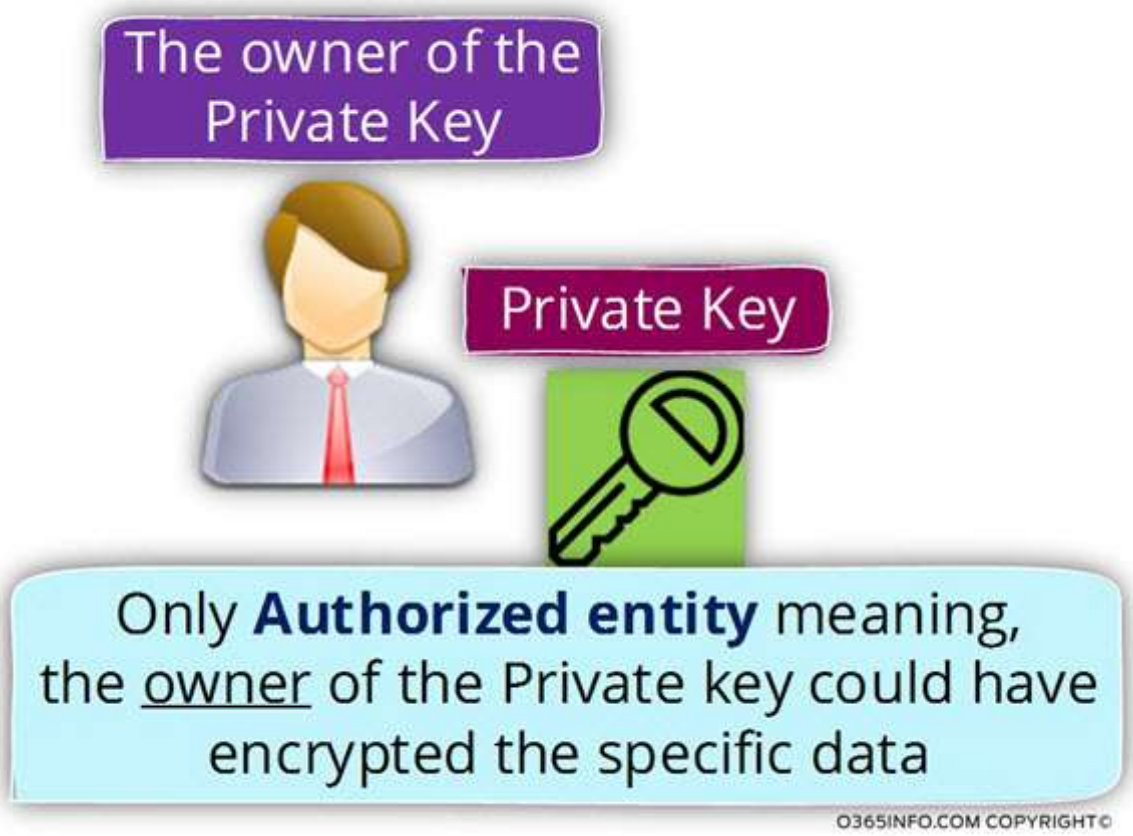
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (GNU/Linux)

mQGiBEKD9XwRBAC0h4q4ueWr0skKkTDP+XKwZ6HSTYFkfxjAUlITyZpGBajYZuXO
y/u7HTAkggS/eSX0VErNFrIUIkdXh0ED/FQxE7tq5tBQv22i/ehoakeww9RNYy0e
yUSYrpCFh4Ktszo2LXIAD5HfEmKI8ow6pHT8PKBn2oqZyYo/nFvTzG7GlwCghzKt
mUJ6dds7ONZvpGbMBeI/0JsEAIY7dPb9lM1Xzauk1o9cmKrnL2P7SK8vsQZUvcZL
7X7dI4J0TWYK19ShOXjQNA7CJbbvlOuKJuXwLsH/VzX+MD3P9l0ZbDEQeAtu4mLG
kxcYMU/rPOjuC7erPDmL47+N/sS/2qHO21lKf2SuIkry57ikcZxdt5czLztWFc9l
fXwF3ICIbZHA3i8An1B9dLXBHfNNFajQIZrdwfw+gDktiEYEEBECAAYFAkZ3/9oA
CgkQlWQfayU+WOO05QCgqCrojF3nDPhcwGK+Ft0v9UmivRAAoK5c0okgf35eF034
LXOYpe0eT0omP8CJBQzqvN0jtUZ94Vux6tgV8eygEOKlQibSYodQSHTKq+WKKXIt
dGy+/kmj1LE9py8vkfioHOAFhHfVJyx8DuEXIzBnFwXr8E822hqN/qt5Mq9y9OBy
MrFaOfZ7YdcV1y/yYooTvQA78A3gyFle7vBsEJC7xo4eTdt2/9/kiSFZ3mGAsJKe
4dB61rhlCa5gtVQH0Z/HRRNmUC1PC8Wph/u2z8sgT6BYf59mX4q8gi60Ar30g3IF
XEWhWIhJBBgRAgAJBQJCg/W5AhsMAAoJEAMkDQZT2UAUWYMAn2NBNHIOJMcnj8Oo
FIgyxFGXBslCAJ4zcUz74RbQuP+UV/hPf2OlY7SeOA==
=q2SM
-----END PGP PUBLIC KEY BLOCK-----
```

How to keep it secret.

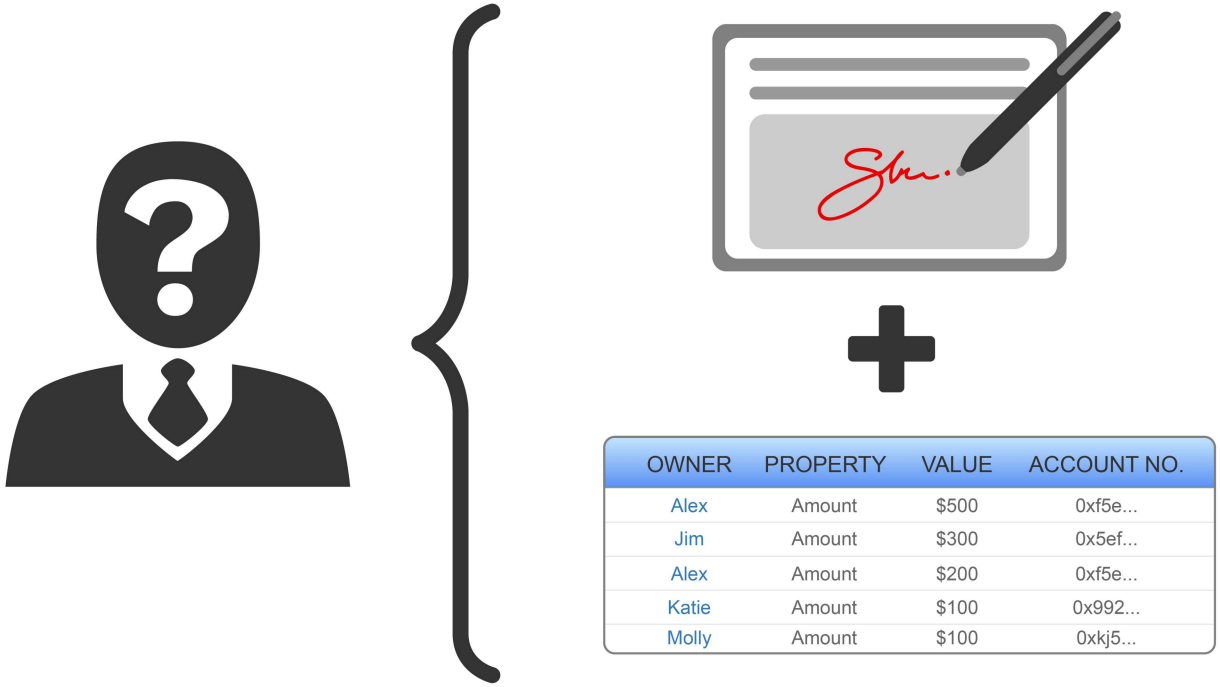


Who owns the key?

Only the key owner can signed the transaction.
Thus, the transaction can only be issued from the owner only.

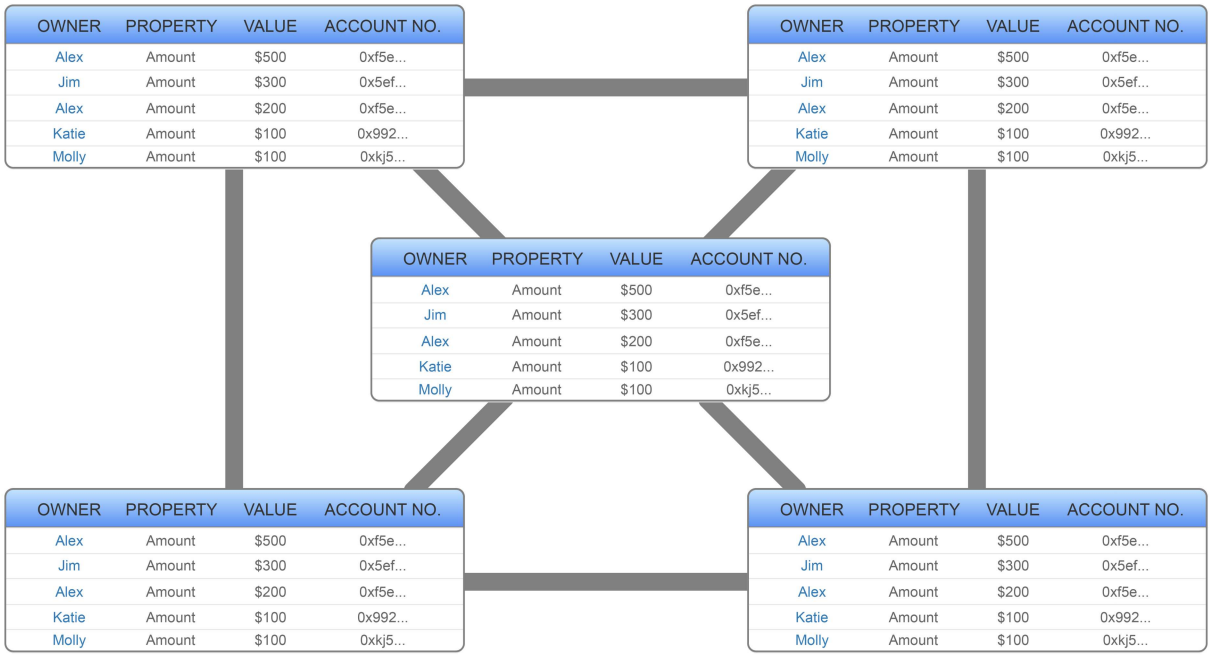


Identity + Transparency

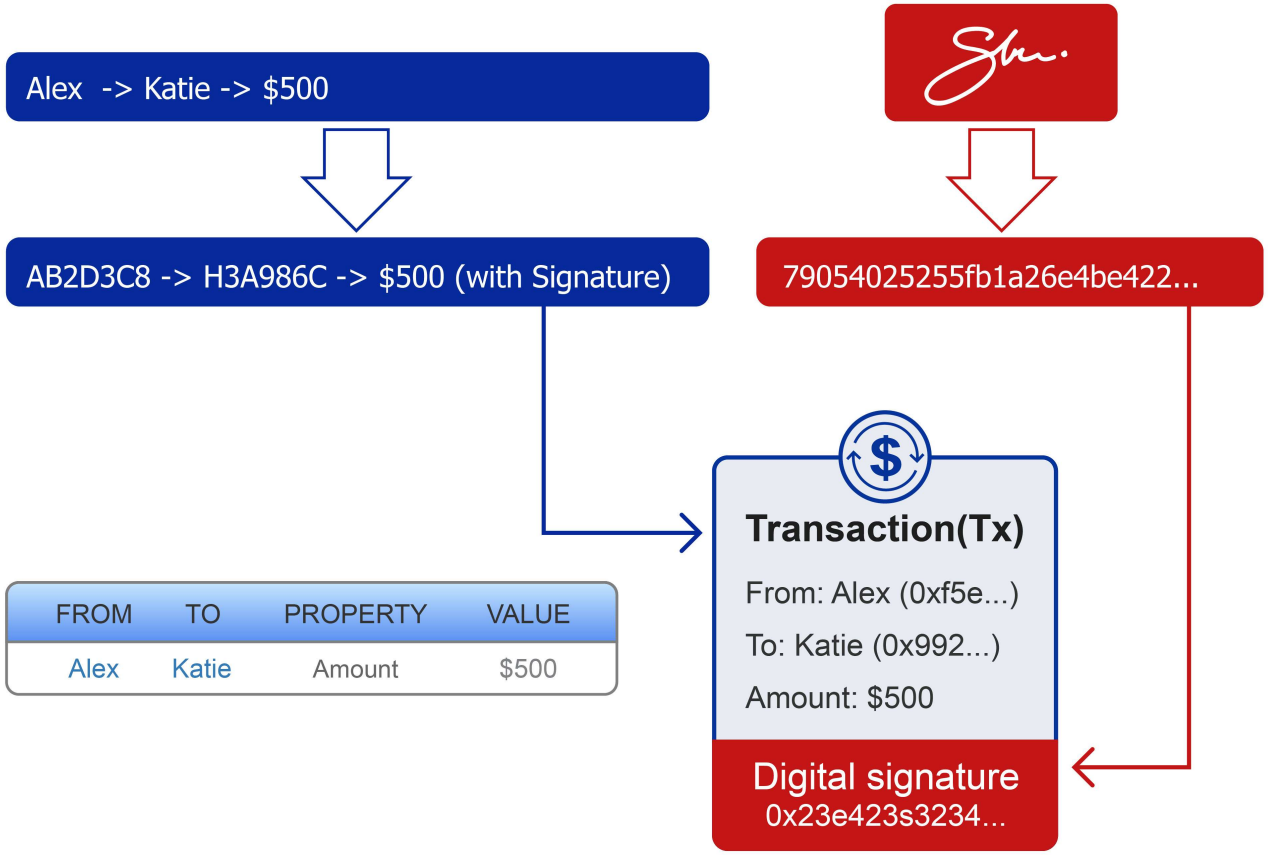


OWNER	PROPERTY	VALUE	ACCOUNT NO.
Alex	Amount	$500	0xf5e...
Jim	Amount	$300	0x5ef...
Alex	Amount	$200	0xf5e...
Katie	Amount	$100	0x992...
Molly	Amount	$100	0xkj5...

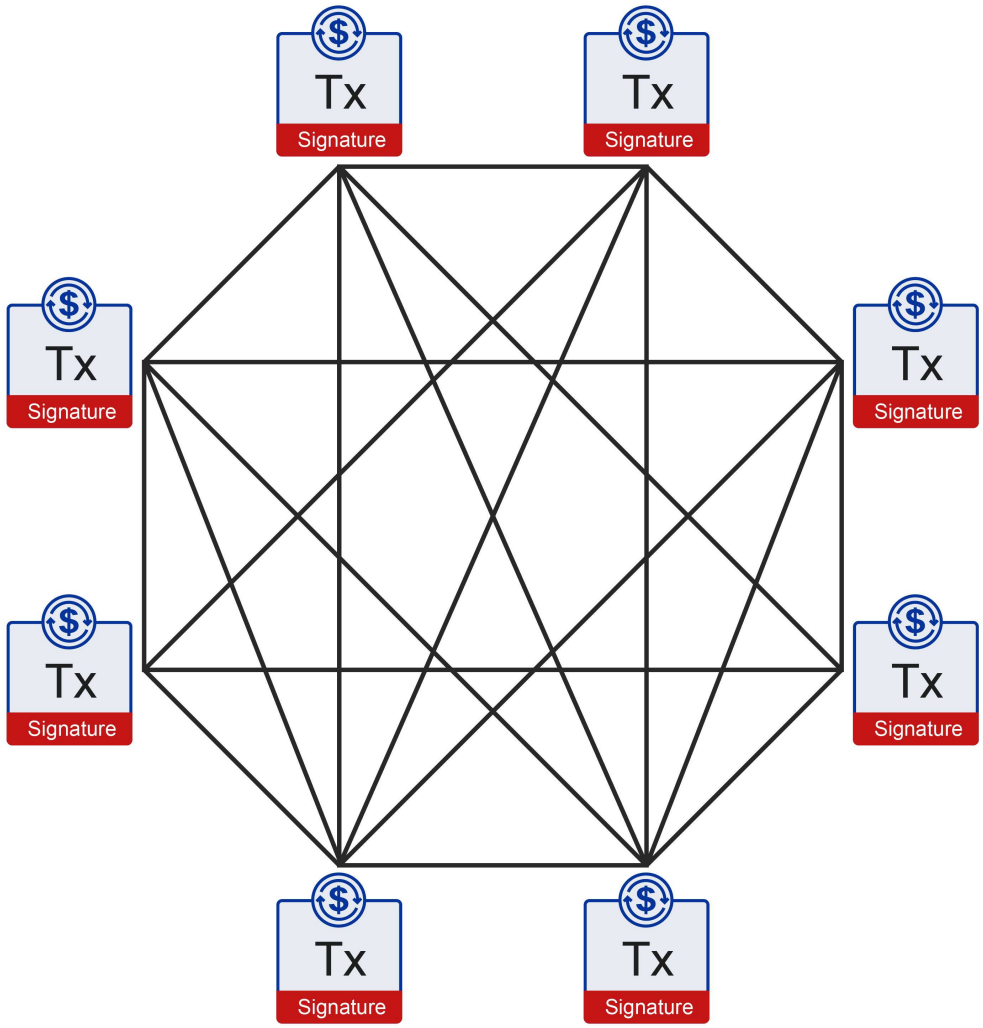
Distributed Ledger



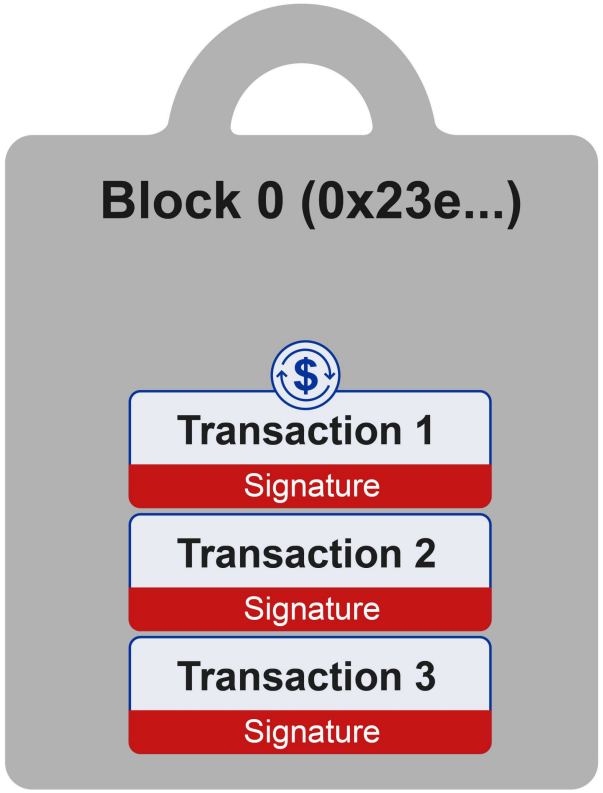
Transaction



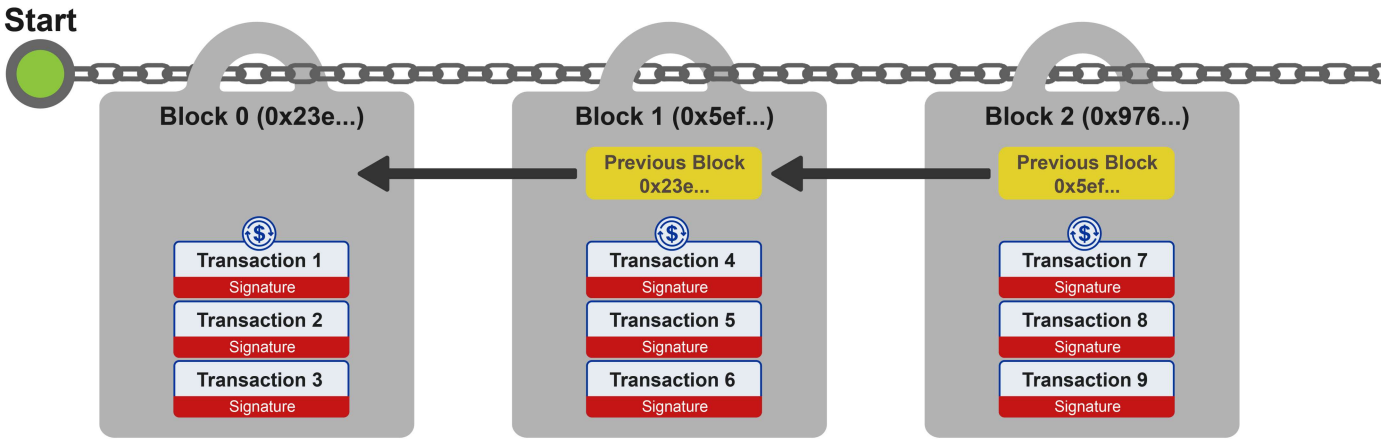
Transactions



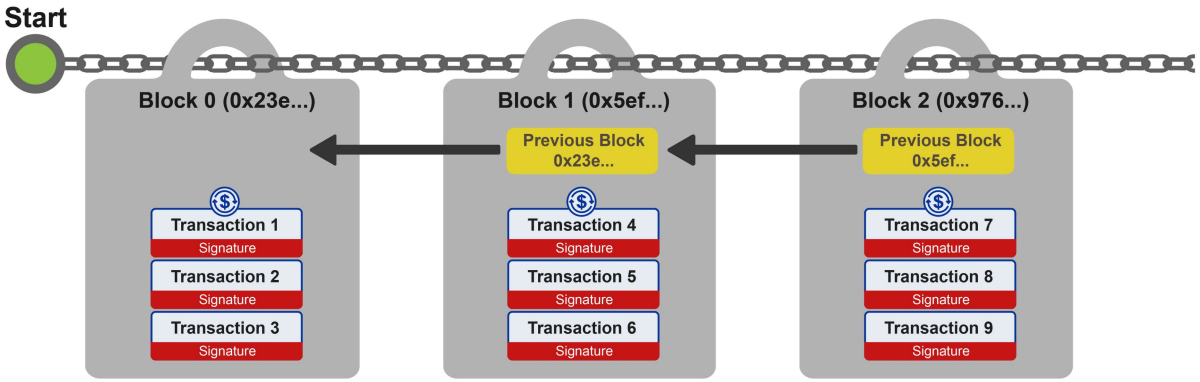
A Block of Transactions



Chain of Blocks



Chain of Blocks as a Ledger

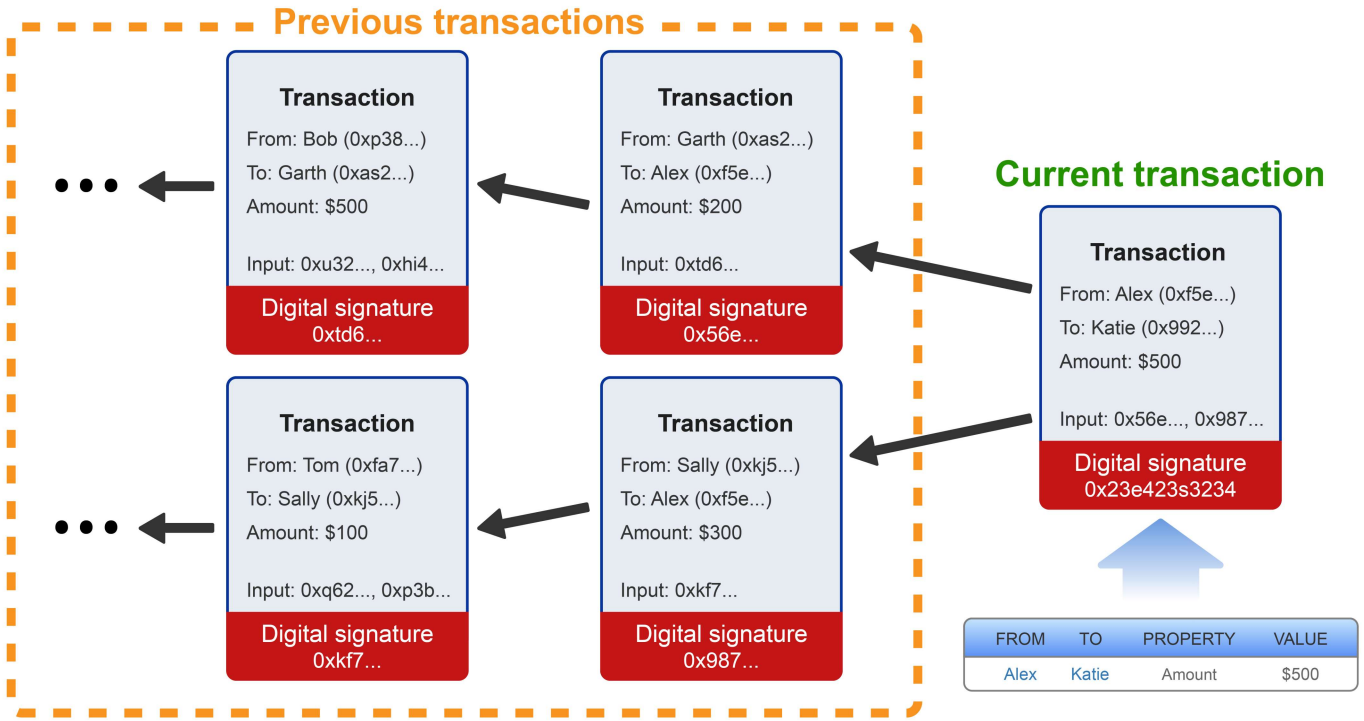


OWNER	PROPERTY	VALUE	ACCOUNT NO.
Alex	Amount	$500	0xf5e...
Jim	Amount	$300	0x5ef...
Alex	Amount	$200	0xf5e...
Katie	Amount	$100	0x992...
Molly	Amount	$100	0xkj5...

Distributed Ledger

Tracability

Blockchains create a transaction chain that maintains the history of ownership of an asset



Blockchain Summary

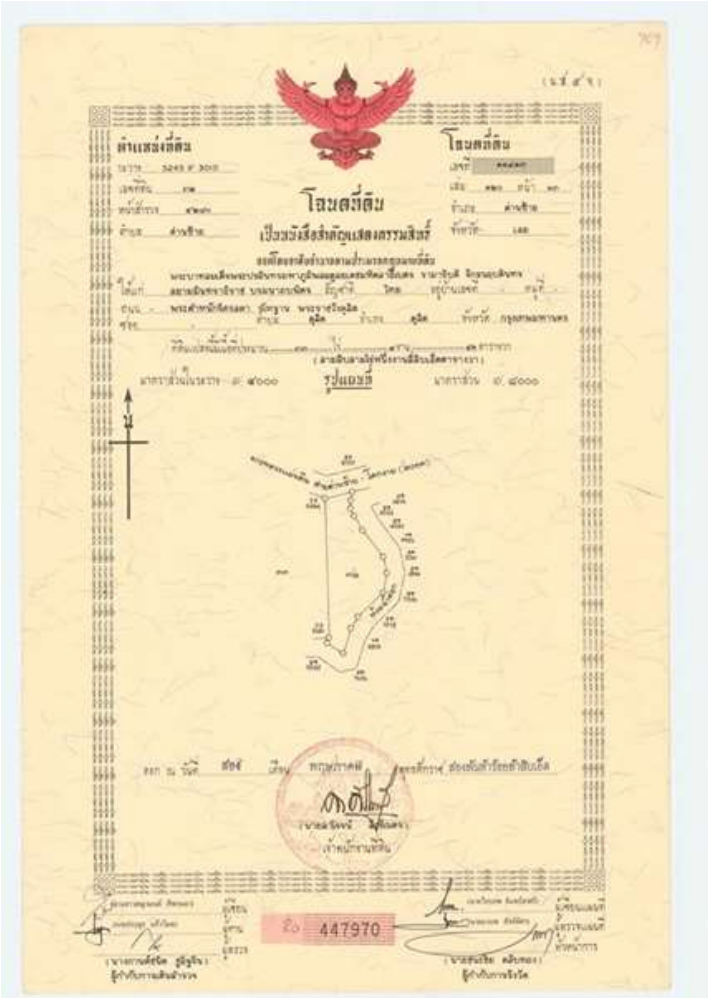
- Replaces `Authority` with `Cryptography`
- From `Centralized System` to `Distributed System`
- Cryptography as a proof of identity
- Distributed Ledger (with Pseudo-Anonymous)
- Tracable Transactions
- Impossible to change historical records

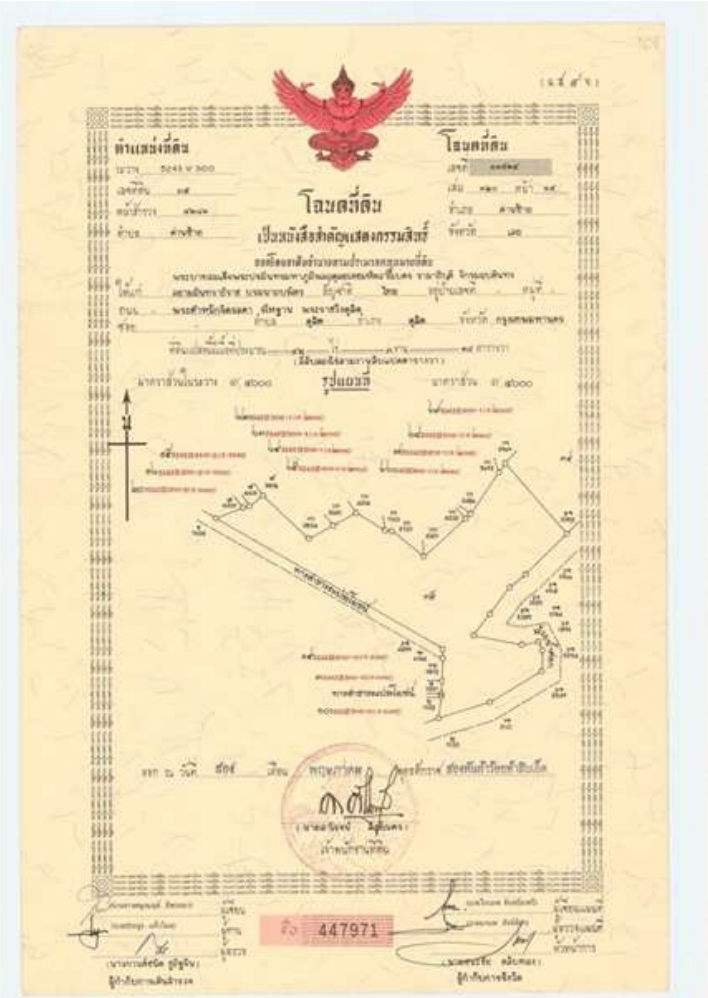
The Potential of Blockchain

Cross-Border Transfer

Stock Exchange

Title Deed





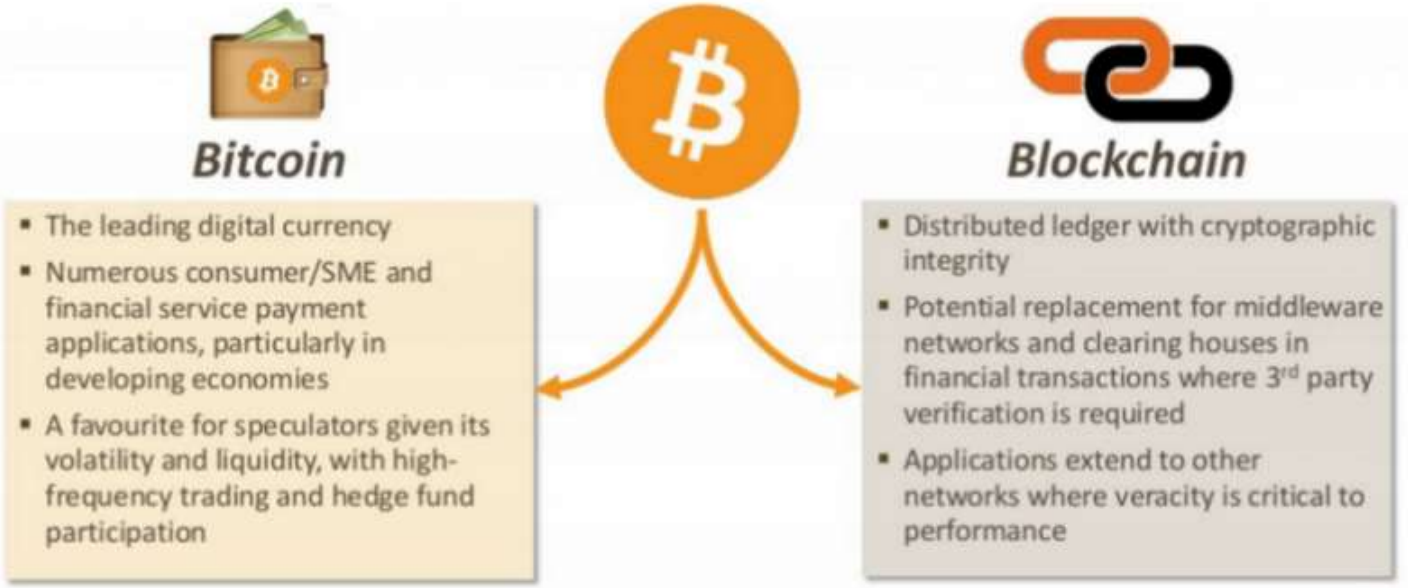
Supply Chain

Benefits

Decentralization has great benefits & changes fundamental processes & models

- Eliminates Intermediaries
  - Allows industries to redefine or create new business models.
- Reduces Fraud
  - Highly secure and transparent, making it nearly impossible to change historical records.
- Increases Efficiency and Speed
  - Simplifies transactions and enables T+Zero settlement time.
- Increases Revenue and Savings
  - Potential savings and new revenue opportunities through more efficient processes and reduced costs.

Bitcoin & Blockchain

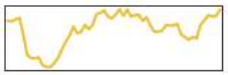


Beyond Bitcoin

Digital-Currencies

There're 649 currencies listed in the coin market.

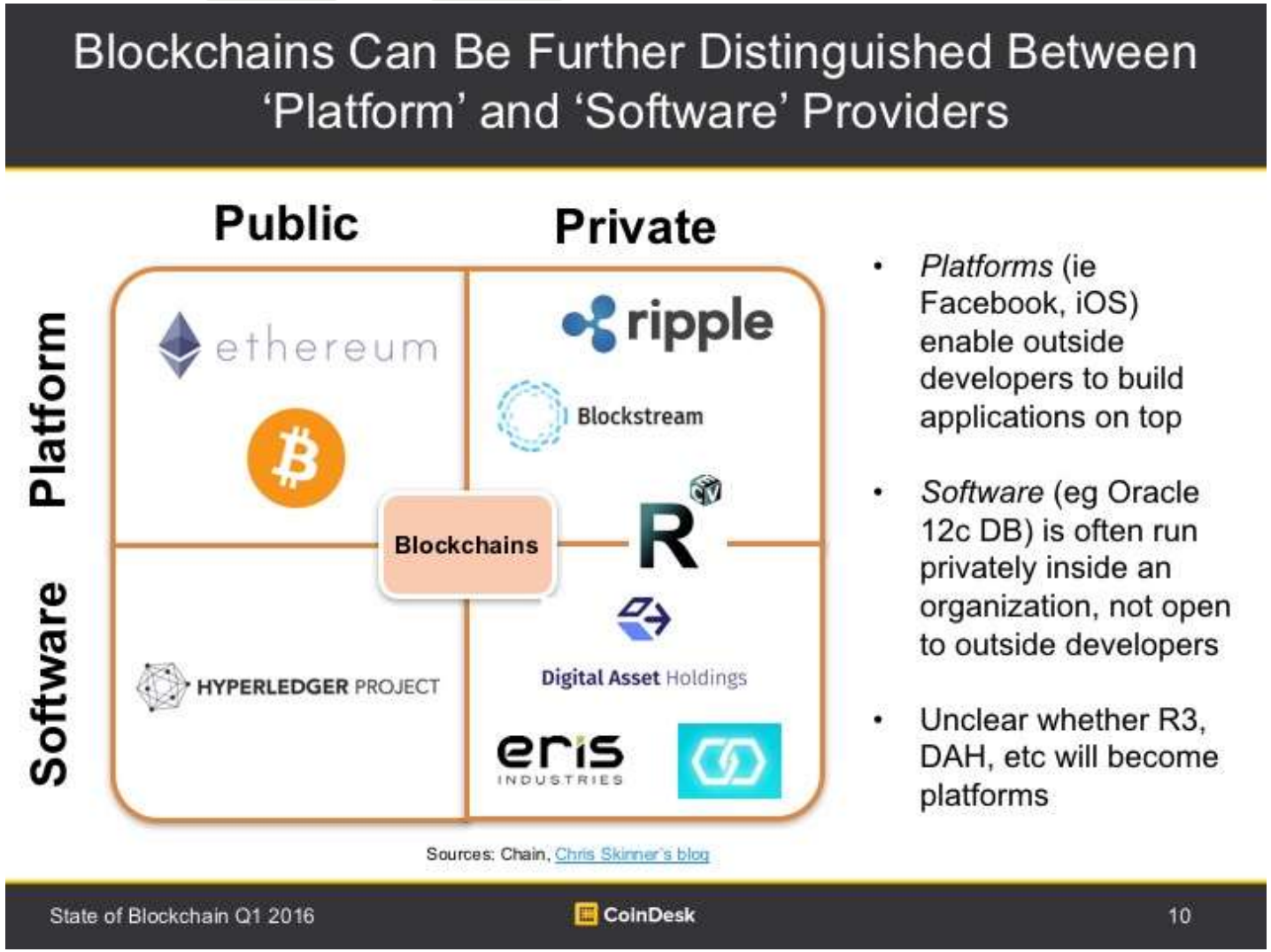
All ▾ | Currencies ▾ | Assets ▾ | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$14,624,547,622	$907.87	16,108,725 BTC	$154,428,000	9.27%	
2	Ethereum	$905,498,457	$10.29	87,997,906 ETH	$16,982,600	6.77%	
3	Ripple	$249,143,729	$0.006775	36,771,322,652 XRP *	$1,841,090	0.07%	
4	Litecoin	$194,472,960	$3.94	49,381,681 LTC	$4,745,600	0.98%	
5	Monero	$168,603,038	$12.24	13,771,045 XMR	$4,393,130	14.75%	
6	Ethereum Classic	$107,588,107	$1.22	87,956,987 ETC	$1,428,620	4.01%	
7	Dash	$100,655,172	$14.31	7,033,806 DASH	$1,858,830	10.81%	
8	MaidSafeCoin	$52,540,430	$0.116098	452,552,412 MAID *	$776,288	2.31%	
9	Augur	$48,458,190	$4.41	11,000,000 REP *	$137,927	9.60%	
10	Steem	$38,705,106	$0.167473	231,112,515 STEEM	$421,521	-8.62%	

Blockchains

Blockchain Providers

Blockchain `Platform` and `Software` Providers



- *Platforms* (ie Facebook, iOS) enable outside developers to build applications on top
- *Software* (eg Oracle 12c DB) is often run privately inside an organization, not open to outside developers
- Unclear whether R3, DAH, etc will become platforms

Review

1. Financial Services Landscape
2. Bitcoin
3. Blockchain
4. Beyond Bitcoin