ITLATTE
PRESENTS

Blockchain: A Sneak Peek

- ITLatte.wordpress.com
- Facebook.com/YourITLatte

The Russian Government is Testing Blockchain for Document Storage

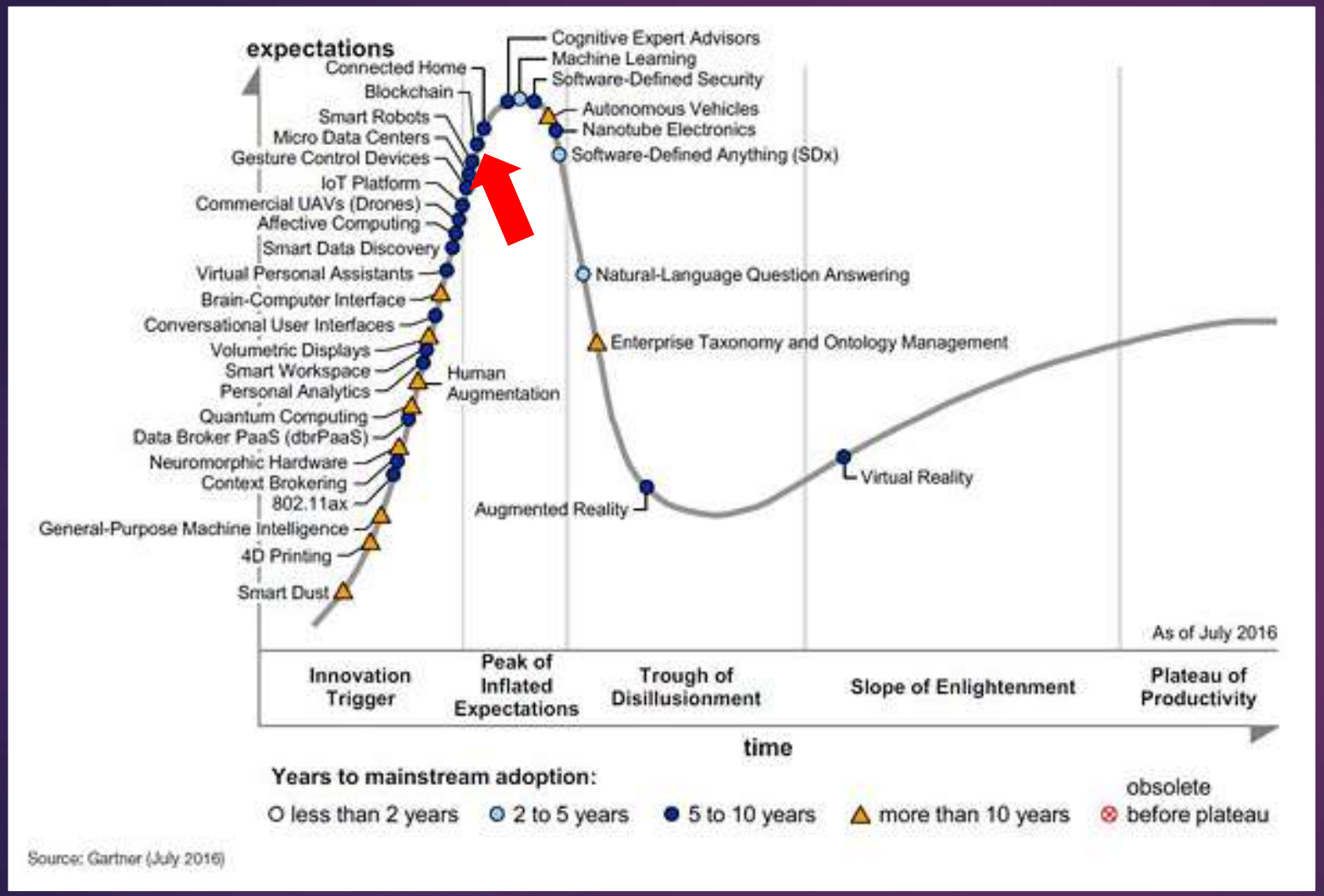
Microsoft Partners Bank of America on Blockchain to "Transform" Trade Finance

ANZ and US Bank Wells Fargo are building a distributed ledger platform for correspondent banking using Blockchain

Abu Dhabi Securities Exchange Announces Blockchain e-Voting Service

ICICI Bank executes India's first banking transactions on blockchain in partnership with Emirates NBD

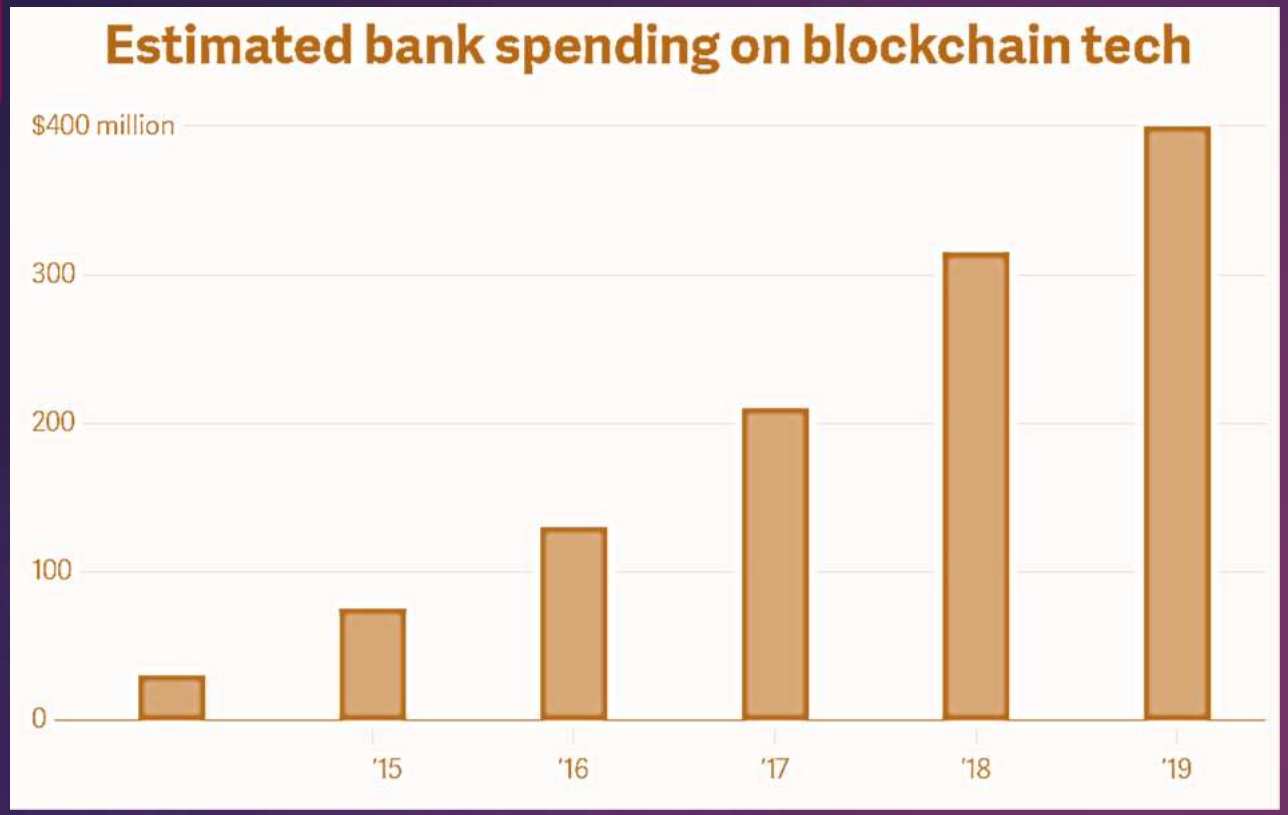
Everyone is talking about it……



"Gartner clients in industries beyond financial services are asking whether it is too late to join in the contagion of 'blockchain fever' that has struck the financial services sector"

– **Ray Valdes, Gartner.**

….and Spending fortunes on it…..



JPMorgan, **The London Stock Exchange Group**, **Wells Fargo**, and **State Street** recently announced they joined a consortium with IBM, Intel, and Cisco and blockchain startup Hyperledger (now owned by Digital Assets Holdings) to develop blockchain technology.

Banks will invest an estimated **$400 million** into the Blockchain technology by 2019, according to new estimates from financial services research firm Aite Group.

R3, a blockchain startup, partnered with 30 major banks like **HSBC**, **Citi**, and **Bank of America** earlier this year to build a blockchain system that would allow the banks to more easily transfer funds with one another.

Among firms stating their organizations have some blockchain initiatives underway, **32%** have an annual budget in excess of **$5 million per year**, and a further **15%** have budgets in excess of **$2 million**. Projected across the entire financial services industry, that level of spending will likely top **$1 billion in 2016**

WHY IS THE WORLD GOING CRAZY OVER BLOCKCHAIN?

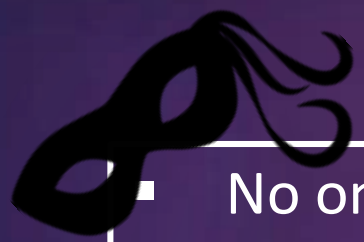
BlockChain what?

BLOCKCHAIN Is Like

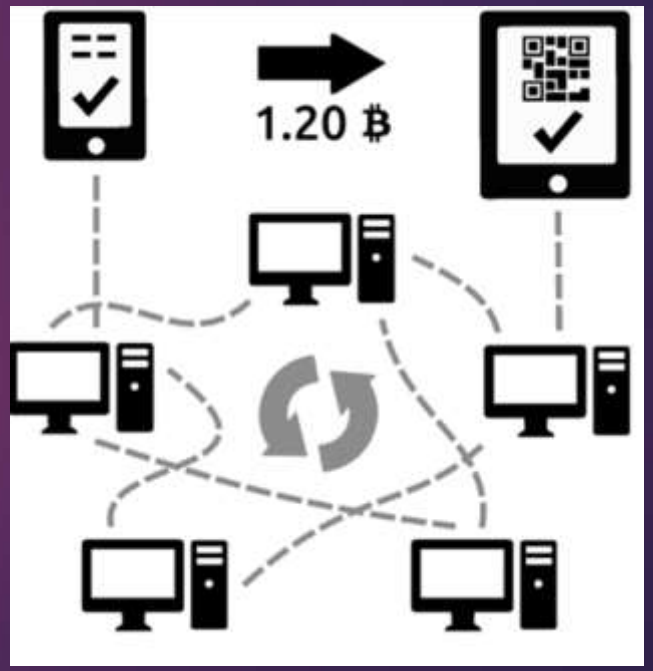
LEDGER

WORLD WIDE ~~WEB~~

"The blockchain is a simple digital platform for recording and verifying transactions so that other people can't erase them later -- and anyone can see them." - GIZMODO



- No one knows who invented blockchain.
- The idea for it came from a paper published online eight years ago
- The author, Satoshi Nakamoto, is thought to be using a pseudonym.



The Basics

- A type of distributed ledger
- comprises of unchangeable, digitally recorded data in packages called blocks.
- These digitally recorded "blocks" of data is stored in a linear chain.
- Each block in the chain contains transaction data
- Is cryptographically hashed.
- The blocks of hashed data draw upon the previous-block in the chain,
- This ensures all data in the overall "blockchain" has not been tampered with and remains unchanged.

The blockchain represents a "golden record" of transactions, a complete, historical record that technically cannot be interfered with or undone.

Key Concepts

Encryption

Public Key: (a long, randomly-generated string of numbers) is a users' address on the blockchain. Transactions (money sent from) get recorded as belonging to that address.
Private Key: Gives its owner access to their digital assets. Store your data on the blockchain and it is incorruptible.

Replication

Replication: Every node in a decentralized system has a copy of the blockchain. No centralized "official" copy exists and no user is "trusted" more than any other. Transactions are broadcast to the network using software applications.
Mining nodes: They validate transactions, add them to the block they're creating and then broadcast the completed block to other nodes. Blockchains use various timestamping schemes, such as proof-of-work to serialize changes.

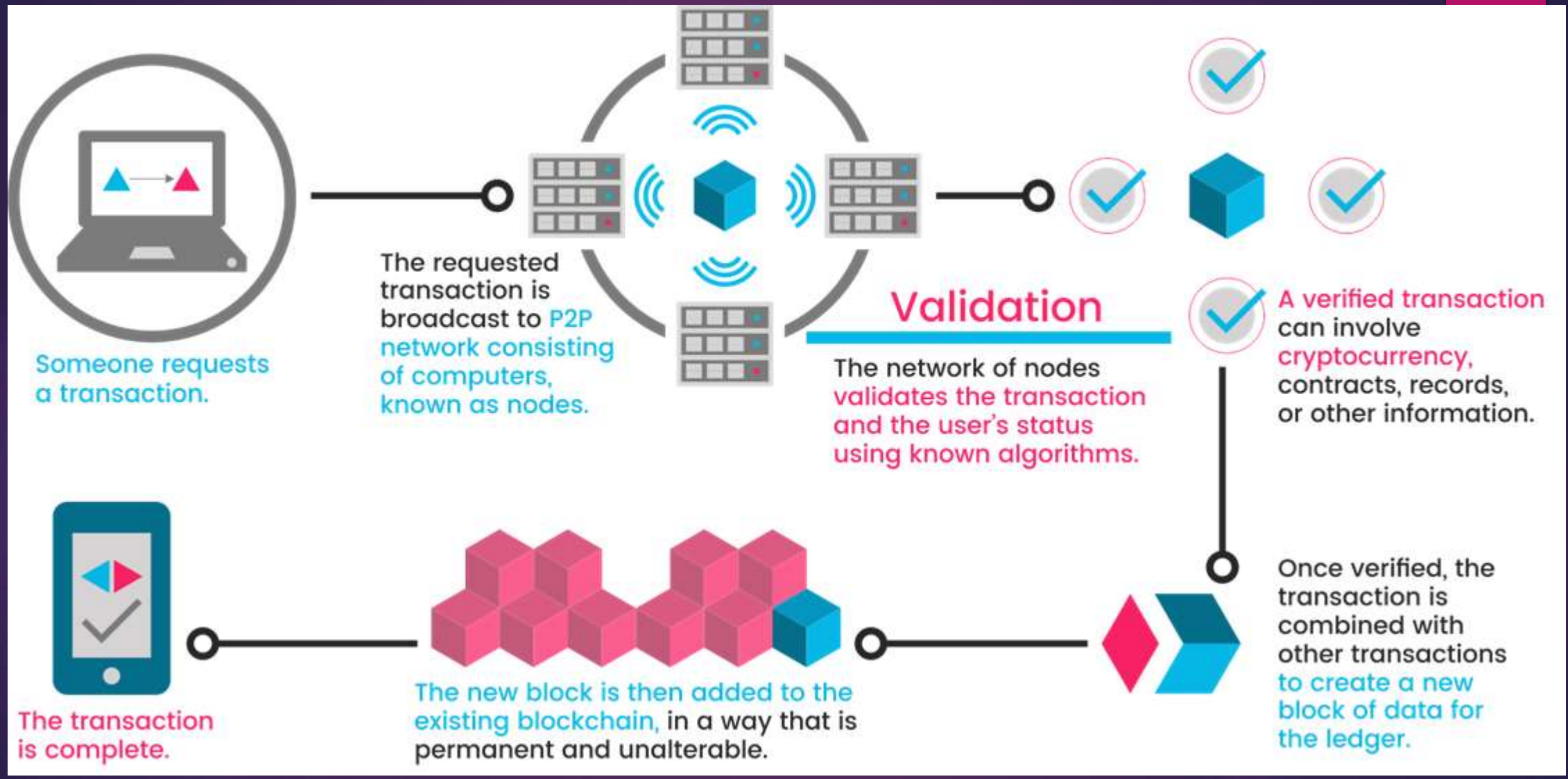
Integrity

Peers keep the highest scoring version of the database that they currently know of. Whenever a peer receives a higher scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers.

Mining

When miners try to compute a block, they pick all transactions that they want to be added in the block, plus one coinbase (generation) transaction to their address.
For a block to be accepted by the network it needs to contain only valid transactions: inputs that are not yet spent, inputs that have the valid amount, signature that verifies ok and etc...

How does it work?



Source: http://blockgeeks.com/

Public vs. Private Blockchains

PUBLIC BLOCKCHAIN

Permissionless Ledgers

Also called ***unpermissioned ledgers***, allow anyone to contribute data to the ledger with all participants possessing an identical copy of the ledger. Since there is no single owner of the ledger, this methodology is more suitable for censorship resistant applications (e.g. Bitcoin). Here the whole network, independent miners and practically everyone who is part of the network, is responsible for the integrity of the Blockchain.

PRIVATE BLOCKCHAIN

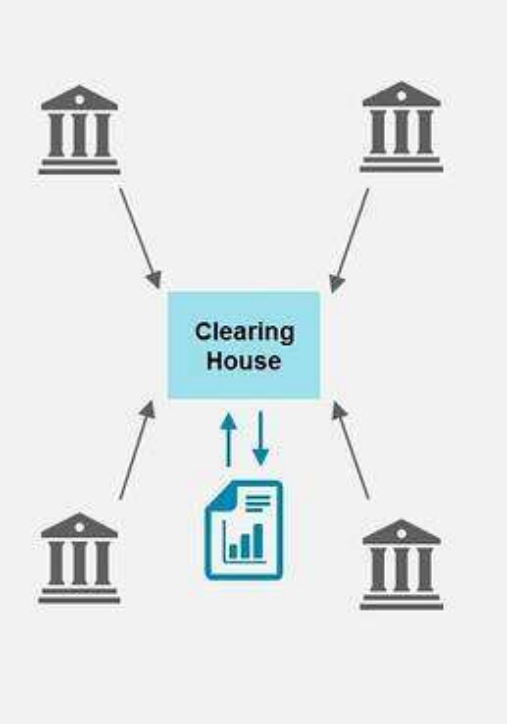
Permissioned Ledgers

Sometimes called ***private blockchains***, allow for distributed identical copies of a ledger, but only to a limited amount of trusted participants only. As the network may have an owner(s), this methodology is better suited for applications requiring simplicty, speed, and greater transparency. Classic example might be interbank transaction.

BLOCKCHAIN IN ACTION

Banking the Blockchain Way

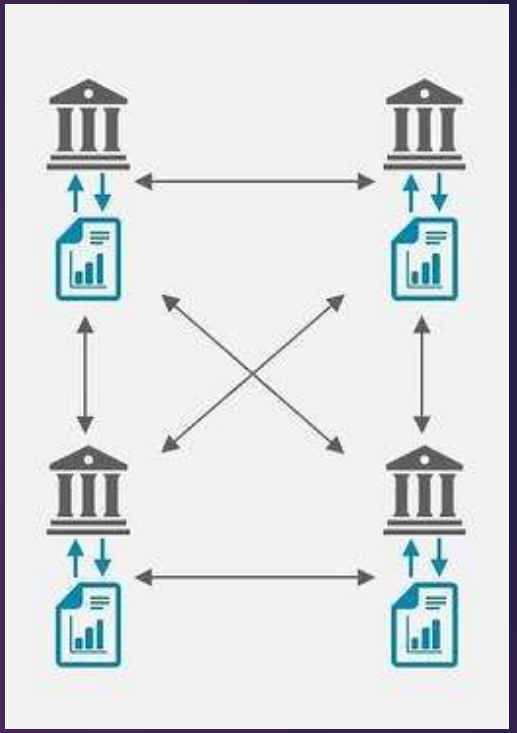
NON BLOCKCHAIN WAY



You transfer a fund to your friend via check, you balance your own check book and your friend does the same when they deposit it.

BLOCKCHAIN WAY

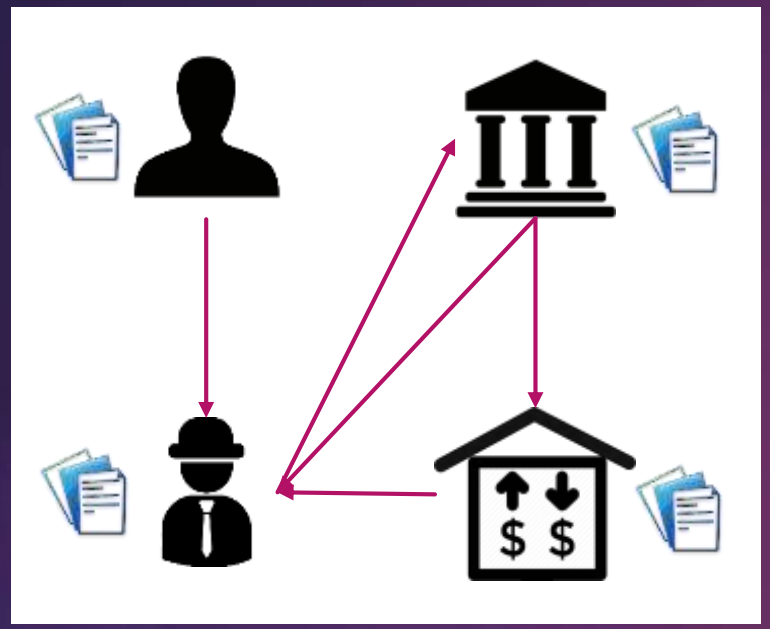
Instead of two separate check books with two records of debits and credits, you'd both look at the same ledger of transactions. It's encrypted, and decentralized, so neither of you controls the ledger.



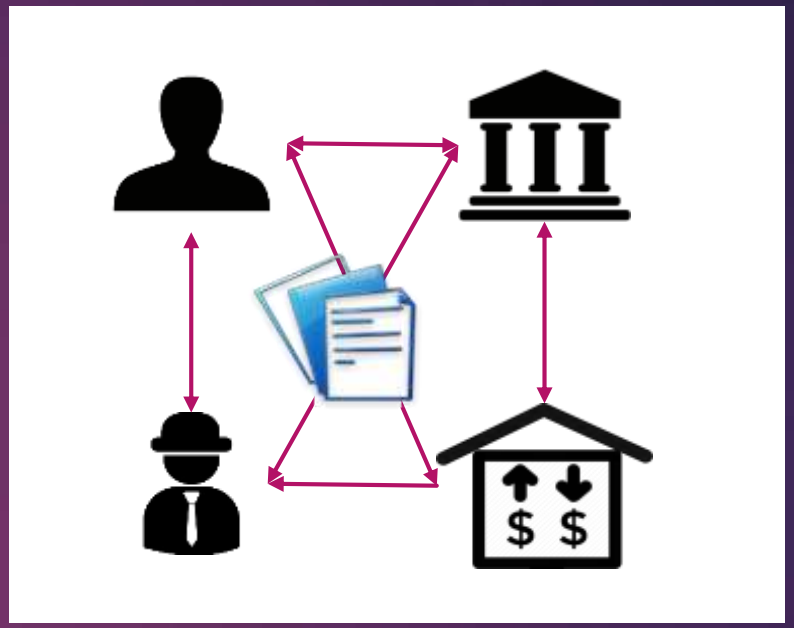
This "distributed ledger" operates on **consensus**. Both of you can look at the ledger. Each transaction gets put into a block. If you both say that block is valid and correct, it's added to a **chain**. And that chain is protected by sophisticated **cryptography**: No one can change the chain after the fact.

Taking Stock of the Future: Trading and Beyond ?

Imagine buying a share.....



Right now, the customer, the bank, the brokerage, the stock exchange, and the company being bought all have separate, private ledgers of transactions. They can't see each other's ledgers. Nor can they verify that everything is accurate among all involved.



With Blockchain, all the entities will be looking at the same ledger since exactly when the order is placed, the transaction of the money being debited, the order being laced, the stocks being blocked etc, will all be broadcasted among the stakeholders. All the transaction that ever happened thus get added into the blockchain, doubling up as a global, immutable history of transactions.

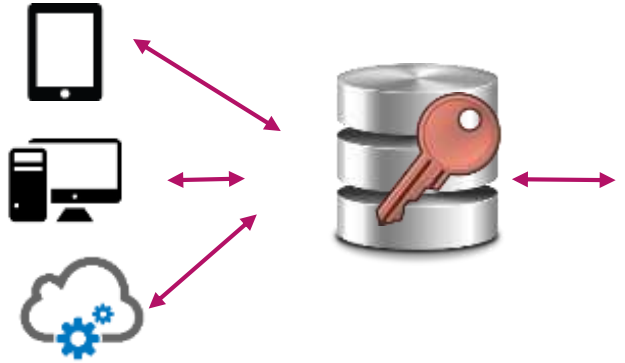
Food for Thought: What happens if we extrapolate the idea to all trading, for example, **real-estate**?

Future of Security?

TRADITIONAL APPROACH

Internal Security Transactions Systems

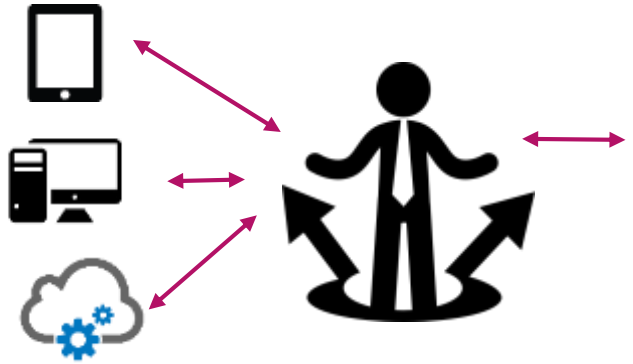
Architecture: Centralized internal database



YOUR APP

Security Clearinghouses

Architecture: Third party authentication Service

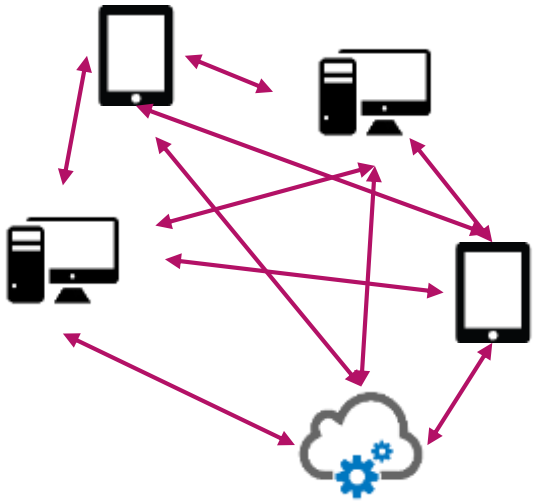


YOUR APP

BLOCKCHAIN

Blockchain

Architecture: Distributed ledger with cryptographic integrity



YOUR APP

Leading Blockchain Consortiums and Collaborative Projec

HYPERLEDGER PROJECT

R3CEV

DOMUS TOWER

INTERLEDGER

CHINALEDGER

Post-Trade Distributed Ledger Group

The very nascent Blockchain market is already seeing massive consolidation with around four major mining service companies gaining prominence globally over independent miners and smaller companies. Future years might see multiple interoperable blockchains coming into existence.

They Said it.....

The first generation of the digital revolution brought us the Internet of information. The second generation — powered by blockchain technology — is bringing us the Internet of value: a new platform to reshape the world of business and transform the old order of human affairs for the better.

- Don Tapscott, world's leading authority on innovation

"I'm reasonably confident … that the blockchain will change a great deal of financial practice and exchange," he said Tuesday from the Consensus 2016 event in midtown Manhattan, adding that his bet on the future of finance would see "40 years from now, blockchain and all that followed from it will figure more prominently in that story than will bitcoin."

- Larry Summers, US Former Treasury Secretary

"Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate."

- Marc Andreesen, inventor of the first browser, thought leader and top VC.

BLOCKCHAIN : ‘TRUST’ through mass collaboration

THANK YOU.